Connected quandles that refute Hayashi's conjecture

P. Graham
https://orcid.org/0009-0007-8493-1505

November 7, 2026

Abstract

We construct connected quandles of orders 1890 and 5670 whose right translations $x \mapsto x * y$ have cycles of lengths 60, 84, 140 and 210. Since 60, 84 and 140 do not divide 210, this disproves the conjecture of Hayashi (2013) that in a finite connected quandle the longest cycle length of a right translation is a multiple of all the others. A quandle is a set with a self-distributive operation modeled on conjugation in a group, and quandles give invariants of knots. The conjecture was known for profiles with at most five cycles (Lages and Lopes), for orders up to 47 (Watanabe) and for affine quandles (Kajiwara and Nakayama). Filipi showed that for conjugation quandles it is equivalent to a group-theoretic conjecture, that a power of an element of a finite generating conjugacy class C is central as soon as it commutes with a suitable element of C. Our quandles are conjugacy classes of affine maps, so they refute that conjecture too. The four long cycle lengths are each twice the product of three of the primes 2, 3, 5 and 7, while each right translation has order 420. The construction gives an infinite family, including latin counterexamples (every left translation is also a bijection), and no counterexample from it has order below 1890. The proofs are by hand. Independent programs recompute both quandles, and one checks every quandle axiom on the full operation table.

This work has not yet been reviewed by experts. The proofs, the checking programs and the text were produced by AI models (from OpenAI and Anthropic), working under the author's direction.

MSC 2020: 20N02, 57K12, 20D45. **Keywords:** quandle, profile, Hayashi's conjecture, conjugacy class, cycle type.

1 Introduction

A *quandle* is a set Q with a binary operation $*$ such that $x * x = x$, every right translation $R_y \colon x \mapsto x * y$ is a bijection, and $(x * y) * z = (x * z) * (y * z)$ for all $x, y, z \in Q$. It is *connected* if the group generated by the right translations acts transitively on Q, *faithful* if $y \mapsto R_y$ is injective, and *latin* if every left translation $x \mapsto y * x$ is a bijection. The basic example is a subset C of a group that is closed under conjugation by its elements and their inverses, with $x * y = yxy^{-1}$; then R_y is conjugation by y. This is a *conjugation quandle*.

Since $R_{x*y} = R_y R_x R_y^{-1}$, in a connected quandle all right translations are conjugate, so they share a cycle type. Following Lages and Lopes [8], the *profile* of a finite connected quandle is this cycle type, written $(\ell_1, \dots, \ell_r)$ with $1 = \ell_1 \le \cdots \le \ell_r$ and repeats allowed; we also write a^m for m cycles of length a, so that $(1, 2, 2, 6)$ is $1\,2^2\,6$. Hayashi posed the following as [3, Conjecture 1.1] (arXiv 2011, published 2013); we state it as in [8, Conjecture 1.6], with r for the number of cycles.

Hayashi's conjecture. *Let $(X, *)$ be a connected quandle of order n with profile $(\ell_1, \dots, \ell_r)$, where $1 = \ell_1 \le \cdots \le \ell_r$. Then ℓ_r is a multiple of ℓ_i for every $i \in \{1, \dots, r\}$.*

1.1 Main results

Theorem 1.1. *There are connected, faithful quandles of orders* 1890 *and* 5670*, with profiles*

$$1^2\,2^{104}\,60^7\,84^5\,140^3\,210^2 \qquad \textit{and} \qquad 1^2\,2^{314}\,60^{21}\,84^{15}\,140^9\,210^6,$$

respectively. Since 60*,* 84 *and* 140 *do not divide* 210*, Hayashi's conjecture is false. Both quandles are conjugation quandles: each is a single finite conjugacy class of the group it generates.*

The two quandles are given in Section 4 and Appendix A. Their profiles have 123 and 367 cycles, and both orders exceed 47. Both meet the necessary condition of [8, Corollary 2.6] for a counterexample: 210 divides $\operatorname{lcm}(60, 84, 140) = 420$. The quandle of order 1890 is the smallest the construction can give (Proposition 1.4), and it has the profile of the case $p = 3$, $\{q_j\} = \{2, 3, 5, 7\}$ of Theorem 1.3 below. The quandle of order 5670 differs only at the prime 3, where it uses the regular module $\mathbb{F}_3[x]/(x^3 - 1)$; it shows that the module changes the order but not the cycle lengths.

Filipi [2] calls a finite conjugacy class C of a group *good* when every $c \in C$ admits some $z \in C$ with $\langle c\rangle \cap C_G(z) \le Z(\langle C\rangle)$ [2, Definition 4.1]. Filipi proved that Hayashi's conjecture holds for all connected conjugation quandles if and only if every finite conjugacy class C with $\langle C\rangle = G$ is good [2, Theorem 4.1], a work that "completes Kayacan's ideas that first appeared in an arXiv paper [8] in 2021" [2, §1], with reference to [7]. The condition is stated as [2, Conjecture 4.1]: "Let G be a group and C its finite conjugacy class such that $\langle C\rangle = G$. Then for any $c \in C$, there exists some $z \in C$ such that for all $k \in \mathbb{Z}$, the element c^k is central if and only if it commutes with z."

Corollary 1.2. *Filipi's Conjecture 4.1 is false: for each quandle C of Theorem 1.1 and $H = \langle C\rangle$, the conclusion fails at every $c \in C$.*

The construction uses the group $\mathbb{F}_3^2$, whose four subgroups of order 3 each switch off one of the primes 2, 3, 5, 7 in the cycle lengths. Replacing it by $\mathbb{F}_p^2$, with its $p + 1$ subgroups of order p and $p + 1$ primes, gives:

Theorem 1.3. *Let p be an odd prime and $q_0, \dots, q_p$ distinct primes. There is a connected, faithful quandle of order $p^{2+\varepsilon} \prod_{q_j \ne p} q_j^{(p-1)/2}$, where $\varepsilon = 1$ if $p \in \{q_0, \dots, q_p\}$ and $\varepsilon = 0$ otherwise, whose profile consists of the lengths* 1*,* 2 *and $\ell_j = 2\prod_{i\ne j} q_i$ for $0 \le j \le p$. Exactly p of the $p + 1$ distinct lengths ℓ_j fail to divide the longest one. If all q_j are odd, the quandle is latin.*

So the number of cycle lengths that fail to divide the longest one is unbounded. The smallest latin case, $p = 3$ and $\{q_j\} = \{3, 5, 7, 11\}$, has order 10395 and profile $1\,2^{577}\,210^{11}\,330^7\,462^5\,770^3$.

Proposition 1.4. *Let C be the conjugation quandle of Section 3, built from any group A of odd order acting on a sum of vector spaces over distinct prime fields, any involution P with $PaP = a^{-1}$ for $a \in A$, and any g_0. If some cycle length of C does not divide the longest, then $|C| \ge 1890$, and $|C| \ge 10395$ if C is latin. Both bounds are attained.*

The proof is in Appendix B.

1.2 Prior work

Lages and Lopes proved the conjecture for profiles with three, four or five cycles [8, Theorem 1.7]. Watanabe proved it for profiles $\{1, \ell_1, \ell_2\}$ [12, Proposition 2.2] and, using a list of connected quandles, "In the case where the order of Q is less than or equal to 47" [12, Proposition 3.1]. Kajiwara and Nakayama proved the affine case first. Their summary reads "We prove that the affine case

of a conjecture by C. Hayashi [...] that any connected finite quandle has a large orbit" (zbMATH 1398.20081, for [5]), and Kayacan writes that "Kajiwara and Nakayama's result shows that Hayashi's Conjecture holds for connected affine quandles" [7, §1]. Rehman's thesis also states that "The Hayashi's conjecture is true for any connected affine quandle" [10, Observations 1.4.7(4)], as does [9, §4, the second Case 4]. Both use a theorem of Horŏsevskiĭ [4], which Bors states as "every automorphism α of a finite nilpotent group has a cycle whose length coincides with $\operatorname{ord}(\alpha)$" [1, Abstract]. Filipi records that a review of [5] pointed out that Horŏsevskiĭ's results "also contribute" [2, §1]. Bors also showed that "the least order of a group where this property is violated for an appropriate automorphism is 120" [1, Abstract], so outside nilpotent groups an automorphism can have no cycle as long as its order; our right translations are of this kind. Kayacan proved the conjecture for racks on which the inner automorphism group acts primitively [7, Theorem 6].

For conjugation quandles, Filipi records that "this conjecture still remains open" [2, §1], and writes after Conjecture 4.1 that it was "verified for all finite nilpotent groups, for the groups S_n, A_n, D_{2n}, for all group of order ≤ 500, and for all simple groups of order $\leq 3.500.000$" [2, §4]. Kaur, Sharma and Singh proved that for "all finite irreducible Coxeter groups G with a conjugation closed subset C, the conjugation quandle $\operatorname{Conj}(G, C)$ satisfies the Hayashi property" [6, Abstract]. Spaggiari's thesis, in a chapter based on a joint project with Bonatto, shows that the conjecture holds for all finite connected quandles if it holds for the faithful ones [11, Theorem 6.4.1]. The quandles of Theorem 1.1 are faithful, so they also refute that reduced form, and they generate groups of order greater than 500, beyond the range Filipi checked. The joint paper of Spaggiari and Bonatto, announced in [11] as work in progress, had not been posted by November 5, 2026.

1.3 What is new

The counterexamples, the family and the bound of Proposition 1.4 are new. A right translation R fails Hayashi's condition exactly when no cycle of R has length equal to its order. By the theorem of Horŏsevskiĭ this cannot happen for an automorphism of a finite nilpotent group, which is how the affine case is settled. Our quandles live in groups of affine maps that are not nilpotent. The step that needed a new idea is to make every cycle of R too short while keeping the quandle connected. The cycle lengths of R are governed by vectors d_b attached to the linear parts. Connectedness comes from the translations by vectors fixed by P: they commute with c_0, so adding them to the group generated by C does not change the class, and with them that group fills the whole affine group (Lemma 3.4). It remains open whether some connected quandle of order between 48 and 1889 refutes the conjecture; by Proposition 1.4 it would not come from our construction. The proofs below are complete by hand; Section 6 describes the computer checks of Theorem 1.1 and Corollary 1.2.

2 Proof overview

Let B be a direct sum of vector spaces V_q over $\mathbb{F}_q$ for distinct primes q, let $A \cong \mathbb{F}_3^2$ act on B, and let P be an involution with $PaP = a^{-1}$ for $a \in A$. The quandle is the class C of the affine map $c_0 \colon w \mapsto P(w + g_0)$ under conjugation by the affine maps with linear part in A. Every element of C has linear part bP for some $b \in A$; the *fiber* of b is the set of elements of C with linear part bP. The map $R = R_{c_0}$ swaps the fibers of b and b^{-1}. On the fiber of $b \neq 1$, the square R^2 is a translation by a vector d_b, so the cycles there have length $2\operatorname{ord}(d_b)$, where $\operatorname{ord}(d_b)$ is the product of the primes q at which d_b has a nonzero component.

We choose the data so that d_b has no component at $q = 2, 3, 5, 7$ respectively when b lies on the first, second, third or fourth of the four lines through 0 (subgroups of order 3) of $\mathbb{F}_3^2$. Every

$b \neq 1$ lies on exactly one line, so the cycle lengths outside the fiber $b = 1$ are 210, 140, 84 and 60, and none equals $\mathrm{ord}(R) = 420$. Connectedness and faithfulness follow from a short computation in the group (Lemmas 3.4 and 3.5). Proposition 1.4 rests on the fact that a group is never a union of three proper subgroups of index at least 3.

3 The construction

Data. Let $B = \bigoplus_q V_q$, where q runs over a finite set of distinct primes and V_q is a finite-dimensional $\mathbb{F}_q$-vector space; write v_q for the V_q-component of $v \in B$. All linear maps below map each V_q to itself. Let A be a group of such invertible linear maps, of odd order, let P be such a linear map with $P^2 = 1$ and $PaP = a^{-1}$ for all $a \in A$, and let $g_0 \in B$.

The group A is abelian, because $a \mapsto PaP = a^{-1}$ is a homomorphism. Each $b \in A$ has a unique square root $a = b^{(|A|+1)/2}$, and then $aPa^{-1} = a(Pa^{-1}P)P = a^2P = bP$, so $(bP)^2 = 1$.

Write (Y, u) for the affine map $w \mapsto Yw + u$ of B, so that $(Y, u)(Y', v) = (YY', Yv + u)$ and $(Y, u)^{-1} = (Y^{-1}, -Y^{-1}u)$. Let

$$G = \{(a, v) : a \in A,\ v \in B\}, \qquad c_0 = (P, Pg_0), \qquad C = \{gc_0g^{-1} : g \in G\},$$

with $x * y = yxy^{-1}$ on C. For a subgroup or element X of $A\langle P\rangle$ and a subspace V, let $C_V(X)$ be the vectors of V fixed by X, and let $[V, A]$ be the span of the vectors $(1 - a)v$. Put

$$h = (1 + P)g_0, \qquad d_b = (1 - b)h \quad (b \in A), \qquad U_b = (1 - bP)B.$$

Multiplying out gives two formulas, used throughout. For $g = (a, v) \in G$ and $b \in A$,

$$gc_0g^{-1} = (a^2P,\ (1 - a^2P)v + aPg_0), \tag{1}$$

$$c_0(a, u)c_0^{-1} = (a^{-1},\ Pu + P(1 - a)g_0), \qquad c_0(bP, u)c_0^{-1} = (b^{-1}P,\ Pu + Pg_0 - b^{-1}g_0). \tag{2}$$

For (2), $c_0^{-1} = (P, -g_0)$ and $c_0(Y, u)c_0^{-1} = (PYP,\ -PYg_0 + Pu + Pg_0)$; put $Y = a$, or $Y = bP$ and use $Pb = b^{-1}P$.

Lemma 3.1 (closure)**.** *Conjugation by c_0 maps G onto G, and C is invariant under conjugation by every element of $\hat{G} = G\langle c_0\rangle \supseteq C$. So C is a conjugation quandle, and all its right translations are conjugate, as permutations of C, to $R = R_{c_0}$.*

Proof. By (2), $c_0Gc_0^{-1} \subseteq G$, with equality since G is finite. Hence $c_0(gc_0g^{-1})c_0^{-1} = g'c_0g'^{-1}$ with $g' = c_0gc_0^{-1} \in G$, and C is invariant under G and c_0, hence also under c_0^{-1}, since conjugation by c_0 is injective and C is finite. For $y = kc_0k^{-1}$ with $k \in G$ we have $R_y = \varphi R\varphi^{-1}$, where φ is conjugation by k. □

Lemma 3.2 (the elements)**.** *$C = \{(bP, u) : b \in A,\ u \in U_b + aPg_0\}$, where a is the square root of b, and $|C| = |A|\,|U_1| = |A|\,|B|/|C_B(P)|$.*

Proof. In (1), $b = a^2$ runs over A and v over B. Since $bP = aPa^{-1}$, we have $U_b = aU_1$, and $|U_1| = |B|/|\ker(1 - P)|$. □

Lemma 3.3 (the cycles of R)**.** *Let $x = (bP, u) \in C$.*

1. *$R(x) = (b^{-1}P,\ Pu + Pg_0 - b^{-1}g_0)$ and $R^2(x) = (bP,\ u + d_b)$.*
2. *If $b \neq 1$, the cycle of x has length $2\prod\{q : (d_b)_q \neq 0\}$.*

3. *If $b = 1$, write $u = Pg_0 + w$ with $w \in U_1$. Then $R(x) = (P, Pg_0 - w)$, so R fixes the $|U_1 \cap V_2|$ points with $2w = 0$ (one point if 2 is not among the primes) and swaps the others in pairs.*

Proof. (1) The first formula is (2). Applying it twice, with $Pb^{-1} = bP$, gives $u \mapsto u + g_0 - bPg_0 + Pg_0 - bg_0 = u + (1-b)(1+P)g_0$. (2) Since $|A|$ is odd, $b^{-1} \neq b$; odd powers of R move x to the fiber of b^{-1}, and $R^{2m}(x) = (bP, u + md_b)$. The additive order of d_b is the product of the primes at which it is nonzero. (3) Since $P(1-P) = P-1$, we have $Pw = -w$ for $w \in U_1$, so $Pu + Pg_0 - g_0 = Pg_0 - w$. The elements of order at most 2 in B are those of V_2. □

Lemma 3.4 (connectedness)**.** *If 2 is not among the primes, or some $a \in A$ fixes no nonzero vector of V_2, then C is connected.*

Proof. First, $[B, A] + (1-P)B + C_B(P) = B$. For odd q every $v \in V_q$ is $\frac{1}{2}(1-P)v + \frac{1}{2}(1+P)v$, and $(1+P)v$ is fixed by P; on V_2, if a fixes no nonzero vector then $1-a$ is invertible and $[V_2, A] = V_2$.

Let $\alpha(g) = c_0 g c_0^{-1}$, an automorphism of G, and let N be the subgroup generated by the elements $g\alpha(g)^{-1} = (gc_0g^{-1})c_0^{-1}$, $g \in G$. Then $N \leq H = \langle C \rangle$, and N is normal in G because $k\, g\alpha(g)^{-1}k^{-1} = (kg)\alpha(kg)^{-1} \cdot (k\alpha(k)^{-1})^{-1}$. The linear part of $(a, v)\alpha((a, v))^{-1}$ is a^2, so the linear parts of N are all of A. For $n = (a, r) \in N$ and $t \in B$, the commutator $(1, t)n(1, t)^{-1}n^{-1} = (1, (1-a)t)$ lies in N, so N contains the translations by $[B, A]$. It also contains $(1, v)\alpha((1, v))^{-1} = (1, (1-P)v)$. The translations by $C_B(P)$ form a group T that commutes with c_0. By the first paragraph NT contains every translation, and it has every linear part, so $NT = G$. Hence every gc_0g^{-1} equals nc_0n^{-1} for some $n \in N \subseteq H$, and conjugation by an element of H is a product of maps $R_y^{\pm 1}$ with $y \in C$. □

Lemma 3.5 (faithfulness)**.** *If $C_{V_2}(A) \cap C_{V_2}(P) = 0$, or 2 is not among the primes, then C is faithful.*

Proof. Suppose $R_x = R_y$ with $x = (bP, u)$ and $y = (b'P, u')$. Then $z = y^{-1}x$ commutes with every element of C, and $z \in G$ has linear part $b'b^{-1}$. As z commutes with c_0, (2) shows its linear part equals its inverse, so it is 1; thus $b = b'$ and $z = (1, s)$. From $x = yz = (bP, u' + bPs)$ we get $bPs = u - u' \in U_b$. Conjugating $(1, s)$ by $(b''P, u'') \in C$ gives $(1, b''Ps)$, so $b''Ps = s$ for all $b'' \in A$; hence $s \in C_B(P) \cap C_B(A)$ and $s = bPs \in U_b$. On U_b the map bP acts as -1, so $s = -s$ and $s_q = 0$ for odd q, while $s_2 \in C_{V_2}(A) \cap C_{V_2}(P) = 0$. Hence $s = 0$, so $z = 1$ and $x = y$. □

4 The counterexamples

Proof of Theorem 1.1. Take $A = \langle a_1, a_2 \rangle \cong \mathbb{F}_3^2$ acting on $B = V_2 \oplus V_3 \oplus V_5 \oplus V_7$, with P and g_0 as in Appendix A, where the hypotheses of Section 3 are checked by hand. For $q \in \{2, 3, 5, 7\}$ let $K_q = \{b \in A : (d_b)_q = 0\}$, a subgroup of A since it is the stabilizer of h_q. Appendix A shows that K_2, K_3, K_5, K_7 are the four distinct lines of $\mathbb{F}_3^2$. Every $b \neq 1$ lies on exactly one line, so by Lemma 3.3(2) its fiber consists of cycles of length $2 \cdot 210/q$, where q is the prime of its line: 210, 140, 84 or 60 for $q = 2, 3, 5, 7$. Lemma 3.3(3) gives the cycles of lengths 1 and 2 on the fiber $b = 1$. The counts in the profiles follow from Lemma 3.2 and the sizes computed in the appendix: in the quandle of order 1890 each fiber has 210 points, and in that of order 5670 each has 630. Connectedness and faithfulness follow from Lemmas 3.4 and 3.5, because a_1 fixes no nonzero vector of V_2. By Lemmas 3.1 and 3.4, C is a single conjugacy class of $\langle C \rangle$. □

Proof of Corollary 1.2. By Lemmas 3.1 and 3.4, C is a finite conjugacy class of $H = \langle C \rangle$. Fix $c, z \in C$, let ℓ be the length of the cycle of R_c through z, and let m be the order of R_c, the least common multiple of its cycle lengths. Since $c^k z c^{-k} = R_c^k(z)$, the power c^ℓ commutes with z. It is central in H if and only if it commutes with every element of C, that is, if and only if $m \mid \ell$. Every

right translation has the profile of Theorem 1.1, so $m = 420$ and $\ell \le 210$. Thus c^ℓ commutes with z without being central, and no z satisfies the conclusion of the conjecture. □

The same argument shows that every quandle of Theorem 1.3 refutes Filipi's conjecture, since there the order $2\prod_j q_j$ of R exceeds every ℓ_j. The argument is the equivalence of [2, Theorem 4.1], applied to a single class.

5 The family and latin examples

Proof of Theorem 1.3. Let $A = \mathbb{F}_p^2$, with its $p+1$ subgroups of order p (the lines) $L_0, \dots, L_p$, and choose surjective homomorphisms $\chi_j \colon A \to \mathbb{Z}/p$ with kernel L_j. Let $\Pi = 1 + x + \cdots + x^{p-1}$. For each j take the block V_{q_j} over $\mathbb{F}_{q_j}$, together with the actions of $a \in A$ and of P and the component of g_0, as follows:

- if $q_j \ne p$: $V_{q_j} = \mathbb{F}_{q_j}[x]/(\Pi)$, a acts as multiplication by $x^{\chi_j(a)}$, $Pf(x) = f(x^{-1})$, and g_0 has component x; P is well defined because $\Pi(x^{-1}) = x^{1-p}\Pi(x)$;
- if $q_j = p$: $V_p = \mathbb{F}_p^2$, a acts as $J^{\chi_j(a)}$ with $J = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $P = \mathrm{diag}(-1, 1)$, and g_0 has component $(0, 1)$.

In both cases $P^2 = 1$ and $PaP = a^{-1}$, and A acts faithfully because $\bigcap_j L_j = 1$.

If $q_j \ne p$, then $h_{q_j} = x + x^{-1} = x + x^{p-1}$ is nonzero in V_{q_j}, since for $p \ge 3$ it has two nonzero coefficients and is not a multiple of Π, which has p. For $p \nmid k$, the polynomial $1 - x^k$ is a unit modulo Π, since $\gcd(x^k - 1, x^p - 1) = x - 1$ and $\Pi(1) = p \ne 0$ in $\mathbb{F}_{q_j}$. So $(d_b)_{q_j} = (1-b)h_{q_j}$ is nonzero exactly when $b \notin L_j$. If $q_j = p$, then $h_p = (0, 2)$ and $(1 - J^k)h_p = (-2k, 0)$, again nonzero exactly when $p \nmid k$. Hence for $b \ne 1$ on L_j, d_b is nonzero exactly at the primes q_i with $i \ne j$, and Lemma 3.3 gives cycles of length ℓ_j. The remaining lengths are 1 and 2.

If some $q_j = 2$, then $V_2 = \mathbb{F}_2[x]/(\Pi)$ and every $a \notin L_j$ acts on it without nonzero fixed vectors, since $1 - x^k$ is a unit; so Lemmas 3.4 and 3.5 apply, as they do when no q_j is 2. For the order, $|C| = p^2 \prod_j |(1-P)V_{q_j}|$ by Lemma 3.2. If $q_j = p$, then $1 - P = \mathrm{diag}(2, 0)$ has rank 1. If $q_j \ne p$, the image of $1 - P$ on $\mathbb{F}_{q_j}[x]/(x^p - 1)$ is spanned by the $(p-1)/2$ elements $x^k - x^{-k}$, $1 \le k \le (p-1)/2$, which have disjoint supports; their span meets the kernel $\mathbb{F}_{q_j}\Pi$ of the map to V_{q_j} only in 0, since its elements have constant term 0. So $(1 - P)V_{q_j}$ has dimension $(p-1)/2$.

For $j \ne k$, ℓ_j does not divide ℓ_k: if q_k is odd, q_k divides ℓ_j but not ℓ_k; if $q_k = 2$, then 4 divides ℓ_j but not ℓ_k. So the ℓ_j are distinct, and none of the other p divides the longest.

Suppose finally that all q_j are odd, and let $y = (bP, u) \in C$. Then $yc_0y^{-1} = (b^2P, (1 - b^2P)u + bg_0)$. If y and $y' = (b'P, u')$ have the same image, then $b^2 = b'^2$, so $b = b'$, and $(1 - b^2P)v = 0$ for $v = u - u' \in U_b$. On U_b we have $bPv = -v$, so $(1 - b^2P)v = (1 + b)v$. If $(1 + b)v = 0$ then $v = b^{|A|}v = -v$, so $2v = 0$ and $v = 0$. Thus the left translation $y \mapsto yc_0y^{-1}$ is injective, hence bijective, on C. Every element of C is kc_0k^{-1} with $k \in G$, and its left translation is that of c_0 conjugated by k. So C is latin. □

6 Computational verification

Theorem 1.1 and Corollary 1.2 are also checked by computer for both quandles, from the data of Appendix A. The data are those of Section 4, not the bases of Theorem 1.3, whose latin examples rest on the proof above. Four checks are used; none of their programs imports another. The first three start from the input data, and the fourth reads the table built by the second.

- The first, in Python with exact arithmetic over $\mathbb{F}_q$, checks that c_0 normalizes G, computes the class C and the cycle type of R_{c_0}, and shows that the right translations by six elements of C already act transitively. It forms no operation table.
- The second is a Python program that rebuilds C and its full operation table, rejecting any product outside C, followed by a C program that checks the quandle axioms on the table: idempotence, bijectivity of every R_y, and right self-distributivity over all n^3 triples. It then checks connectedness, that all n right translations have the stated cycle type, and faithfulness.
- The third checks Filipi's statement in the group: it computes the powers of c_0, finds that only c_0^0 is central in $\langle C\rangle$, and for every $z \in C$ finds a $k \le 210$ with c_0^k commuting with z.
- The fourth reads the table and shows that, for every $c \in C$, no cycle of R_c has length equal to its order.

Each check rejects an altered input aimed at it. With the V_3-component of g_0 set to zero, the profile satisfies the conjecture, as Lemma 3.3 predicts (for order 5670 it becomes $1^2\,2^{314}\,20^{63}\,28^{45}\,70^{18}\,140^9$); the first, the C program and the third and fourth checks reject it. With an identity block on V_7 in P, c_0 no longer normalizes G, and the first check and the table builder reject it. With one table entry changed, the C program rejects the table. On an ordinary computer all checks take about three minutes, and the complete distributivity check for order 5670 about seven minutes more. The programs and commands are distributed with this paper.

Appendix A The data and their hand verification

Vectors are columns and matrices are given by rows. The quandle of order 5670 uses $V_2 = \mathbb{F}_2^2$, $V_3 = \mathbb{F}_3^3$, $V_5 = \mathbb{F}_5^2$, $V_7 = \mathbb{F}_7^2$ and

	a_1	a_2	P	g_0
$\mathbb{F}_2^2$	$E = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$	I	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$(0,1)$
$\mathbb{F}_3^3$	I	$\sigma = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$	$-\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$	$(0,1,0)$
$\mathbb{F}_5^2$	$M = \begin{pmatrix} 0 & 4 \\ 1 & 4 \end{pmatrix}$	M	$\begin{pmatrix} 1 & 4 \\ 0 & 4 \end{pmatrix}$	$(1,0)$
$\mathbb{F}_7^2$	$\mathrm{diag}(2,4)$	$\mathrm{diag}(4,2)$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$(1,0)$

The quandle of order 1890 changes only the $\mathbb{F}_3$-block, to $a_1 = I$, $a_2 = J \oplus 1$ with $J = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $P = \mathrm{diag}(2,1,1)$ and $g_0 = (0,1,0)$. Its third $\mathbb{F}_3$-coordinate is inert (A and P fix it and g_0 vanishes there); it keeps the block sizes of the order-5670 data.

$A \cong \mathbb{F}_3^2$. In each block a_1 and a_2 commute (one is I, or they are equal, or both are diagonal). Each has order 3: $E^3 = I$ over $\mathbb{F}_2$, σ is a 3-cycle of coordinates, $J^3 = I$ over $\mathbb{F}_3$, $M^3 = I$ over $\mathbb{F}_5$, and $2^3 = 4^3 = 1$ in $\mathbb{F}_7$. If $a_1^i a_2^k = 1$, the $\mathbb{F}_2$-block gives $3 \mid i$ and the $\mathbb{F}_3$-block gives $3 \mid k$. So $|A| = 9$.

$P^2 = 1$ **and** $Pa_iP = a_i^{-1}$**.** Over $\mathbb{F}_2$: $P^2 = I$ and $PEP = \left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right) = E^2$. Over $\mathbb{F}_3$: conjugating the 3-cycle σ by the transposition of the last two coordinates gives σ^{-1}; for the order-1890 data, $\operatorname{diag}(-1,1)J\operatorname{diag}(-1,1) = J^{-1}$. Over $\mathbb{F}_5$: $P^2 = I$ and $PMP = \left(\begin{smallmatrix}4&1\\4&0\end{smallmatrix}\right) = M^{-1}$. Over $\mathbb{F}_7$: swapping coordinates turns $\operatorname{diag}(2,4)$ into $\operatorname{diag}(4,2) = \operatorname{diag}(2,4)^{-1}$.

The lines K_q. The components of $h = (1+P)g_0$ are $h_2 = (1,0)$, $h_3 = (0,1,2)$ (order 5670) or $(0,2,0)$ (order 1890), $h_5 = (2,0)$ and $h_7 = (1,1)$. Let $b = a_1^i a_2^k \neq 1$.

- $q = 2$: b acts as E^i, which for $3 \nmid i$ fixes no nonzero vector, since $x^2 + x + 1$ has no root in $\mathbb{F}_2$. So $K_2 = \langle a_2 \rangle$.
- $q = 3$: for order 5670, b acts as σ^k, whose fixed vectors for $3 \nmid k$ are the constant vectors, and h_3 is not constant; for order 1890, $(1-b)h_3 = (k,0,0)$. So $K_3 = \langle a_1 \rangle$.
- $q = 5$: b acts as M^{i+k}, which for $i + k \not\equiv 0$ fixes no nonzero vector, since $x^2 + x + 1$ has no root in $\mathbb{F}_5$. So $K_5 = \langle a_1 a_2^2 \rangle$.
- $q = 7$: b acts as $\operatorname{diag}(2^{i+2k}, 2^{2i+k})$, and both coordinates of h_7 are nonzero, so $(d_b)_7 = 0$ needs $3 \mid i+2k$ and $3 \mid 2i+k$, since $2^j = 1$ exactly when $3 \mid j$. Both congruences say $i \equiv k \pmod 3$, so $K_7 = \langle a_1 a_2 \rangle$.

Counting. The fixed spaces of P are $\{(x,0)\}$ in $\mathbb{F}_2^2$, $\{(0,2z,z)\}$ in $\mathbb{F}_3^3$ (order 5670) or $\{(0,y,z)\}$ (order 1890), $\{(x,0)\}$ in $\mathbb{F}_5^2$ and the diagonal in $\mathbb{F}_7^2$. So $|C_B(P)|$ is $2\cdot3\cdot5\cdot7 = 210$ or $2\cdot9\cdot5\cdot7 = 630$, while $|B| = 4\cdot27\cdot25\cdot49 = 132300$. Hence $|U_1|$ is 630 or 210, and $|C| = 9|U_1|$ is 5670 or 1890. In both cases $U_1 \cap V_2 = (1-P)V_2$ has 2 elements, so the fiber $b = 1$ contributes $1^2\, 2^{(|U_1|-2)/2}$. Each line contributes two fibers of $|U_1|$ points, divided into cycles of the length of that line.

Appendix B Proof of Proposition 1.4

Proof of Proposition 1.4. Let $S(b)$ be the set of primes q with $(d_b)_q \neq 0$, and $S = \bigcup_b S(b)$. By Lemma 3.3 the cycle lengths of R are 1, possibly 2, and $2\prod S(b)$ for $b \neq 1$. If $S(b^*) = S$ for some $b^* \neq 1$, every length divides $2\prod S$, which is itself a length. So if some length fails, every $b \in A$ lies in one of the proper subgroups $K_q = \{b : (d_b)_q = 0\}$ with $q \in S$. A cyclic group is not a union of proper subgroups, and in a group of odd order a proper subgroup has at most $|A|/3$ elements, so three of them cover at most $|A| - 2$ elements. Hence $|S| \geq 4$ and A is non-cyclic of odd order, so $|A| \geq 9$ and $\prod S \geq 2\cdot3\cdot5\cdot7$.

For $q \in S$, pick b with $q \in S(b)$. Both u and $u + d_b$ lie in $U_b + aPg_0$ by Lemma 3.3(1), so $(d_b)_q$ is a nonzero element of $(1-bP)V_q$, which has the size of $(1-P)V_q$. So $|U_1| \geq \prod S \geq 210$ and $|C| = |A|\,|U_1| \geq 1890$.

In a latin quandle R_y fixes only y, since $x * y = x = x * x$ forces $x = y$. By Lemma 3.3(3), $U_1 \cap V_2 = (1-P)V_2$ is then 0, so $2 \notin S$, $\prod S \geq 3\cdot5\cdot7\cdot11$ and $|C| \geq 9\cdot1155 = 10395$. Theorem 1.1 and the case $p = 3$, $\{q_j\} = \{3,5,7,11\}$ of Theorem 1.3 attain the bounds. □

Appendix C Correction

November 7, 2026. The abstract of the first version said that each cycle length is twice the product of three of the primes 2, 3, 5 and 7. That holds only for the four long cycle lengths 60, 84, 140 and 210; the profiles also have cycles of lengths 1 and 2. The abstract now says so. No theorem, proof or check has changed.

References

[1] A. Bors, *On finite groups where the order of every automorphism is a cycle length*, arXiv:1412.8418v2 (2015).

[2] F. Filipi, *Hayashi property for conjugation quandles*, arXiv:2503.22377v1 (2025).

[3] C. Hayashi, *Canonical forms for operation tables of finite connected quandles*, Comm. Algebra 41 (2013), no. 9, 3340–3349, doi:10.1080/00927872.2012.685532; arXiv:1110.1849v1 (2011).

[4] M. V. Horŏsevskiĭ, *On automorphisms of finite groups*, Math. USSR-Sb. 22 (1974), no. 4, 584–594, doi:10.1070/SM1974v022n04ABEH001707.

[5] T. Kajiwara and C. Nakayama, *A large orbit in a finite affine quandle*, Yokohama Math. J. 62 (2016), 25–29; summary in zbMATH 1398.20081.

[6] D. Kaur, U. B. Sharma and P. Singh, *Hayashi property for conjugation quandles over finite Coxeter groups*, arXiv:2607.03922v1 (2026).

[7] S. Kayacan, *On a conjecture about profiles of finite connected racks*, Erzincan University Journal of Science and Technology 18 (2025), no. 3, 735–744, doi:10.18185/erzifbed.1591413; arXiv:2006.10327v3.

[8] A. Lages and P. Lopes, *On a conjecture by Hayashi on finite connected quandles*, Ars Math. Contemp. 26 (2026), no. 4, Paper No. P4.05, doi:10.26493/1855-3974.3529.4e5. Statement numbers are those of the published version; in arXiv:2405.11660v2 they are Conjecture 1.1, Theorem 1.3 and Corollary 2.1.

[9] N. Rehman, *On the cycle structure of finite racks and quandles*, arXiv:1912.05115v1 (2019).

[10] N. Rehman, *Quandles and Hurwitz orbits*, PhD thesis, Philipps-Universität Marburg, 2016, https://d-nb.info/1114394920/34.

[11] F. Spaggiari, *Non-associative algebraic structures*, PhD thesis, Charles University, Prague, 2025.

[12] T. Watanabe, *On the structure of the profile of finite connected quandles*, Math. J. Okayama Univ. 61 (2019), 85–98, doi:10.18926/mjou/56328, https://www.math.okayama-u.ac.jp/mjou/mjou61/_05_Watanabe.pdf.