GOOD INVOLUTIONS OF LINEAR QUANDLES: A CONJECTURE OF TA, AND A COMPLETE COUNT WHEN $4 \nmid N$

KOREA SUPERINTELLIGENCE LABS

Abstract. For a positive integer N and a unit k of $\mathbb{Z}/N$, the *linear quandle* $\Lambda_{N,k}$ is the Alexander quandle of $\mathbb{Z}/N$ with $\varphi_k(x) = kx$; it is the dihedral quandle R_N when $k = -1$ and the trivial quandle when $k = 1$. Ta tabulated the number $|\operatorname{Good}\Lambda_{N,k}|$ of good involutions of every nontrivial linear quandle of order at most 29, all but two entries by a computer search, and closed his paper with the conjecture that $|\operatorname{Good}\Lambda_{4n,2n-1}| = 10$ for every odd $n \geq 3$, having confirmed $n = 3, 5, 7$. We prove that conjecture, for every odd $n \geq 1$.

The proof runs through a reduction which is uniform in N: if $k^2 = 1$ and the ideal of $\mathbb{Z}/N$ generated by $k - 1$ is generated by a divisor g of N, then the good involutions of $\Lambda_{N,k}$ correspond bijectively to the maps $D\colon \mathbb{Z}/g \to \mathbb{Z}/g$ satisfying $D(u) + D(u + cD(u)) = 0$, where $c \equiv N/g \pmod{g}$. For the conjectured family $g = \gcd(4n, 2n - 2) = 4$ for *every* odd n, so two searches over 4^4 maps settle every n at once, whereas the search reported in the source is run one order at a time over a space that grows with n.

We then determine $|\operatorname{Good}\Lambda_{N,k}|$ for *every* modulus N not divisible by 4 and every k: it is 0 unless $k^2 = 1$, and otherwise it is the number of involutions of a set with $\gcd(N, k-1)$ elements, the corresponding term of OEIS A000085. The mechanism is a dichotomy: if $k^2 = 1$ and $g = \gcd(N, k - 1)$, then $\gcd(N/g, g)$ divides 2, and the value 2 forces $4 \mid N$. Consequences are a closed form for Ta's per-order sums, OEIS A387317, at every such modulus, twenty-three terms of that sequence beyond its published range, and eight individual counts beyond every published table, the largest being $|\operatorname{Good}\Lambda_{48,17}| = 46\,206\,736$. A two-case classification valid for every modulus, whose second case is the square of a term of OEIS A000898, is proved here in the ordinary way; that second case is the one part of the paper that is not machine-checked. Every other statement below has been verified with a proof assistant, apart from those attributed to the literature and the few marked in the text as computed but unproved.

1. Introduction

A *quandle* is a set X together with a map $x \mapsto s_x$ from X into the symmetric group S_X satisfying

$$s_x s_y = s_{s_x(y)}\, s_x, \qquad s_x(x) = x \qquad (x, y \in X);$$

it is *involutory*, or a *kei*, if in addition $s_x^2 = \mathrm{id}$ for every x. Following Kamada [2], a *good involution* of a quandle $Q = (X, s)$ is an involution $\rho \in S_X$ with

$$\rho s_x = s_x \rho, \qquad s_{\rho(x)} = s_x^{-1} \qquad (x \in X), \tag{1}$$

and the pair (Q, ρ) is then a *symmetric quandle*. We write $\operatorname{Good} Q$ for the set of good involutions of Q. Symmetric quandles are the coefficient objects for colouring and cocycle invariants of links and surface-links that need not be oriented or orientable [2, 3]; for the wider range of applications see the introduction of [9]. The

classification problem symmetric quandles pose — given Q, determine all ρ making (Q,ρ) symmetric — is one of two problems posed by Taniguchi [12] and recorded as [9, Problem 1.2].

This paper is about the case where Q is a *linear quandle*. For an abelian group A and $\varphi \in \operatorname{Aut} A$, the *Alexander quandle* $\operatorname{Alex}(A,\varphi)$ is A with $s_a(b) := \varphi(b-a)+a$; for a positive integer N and a unit k of $\mathbb{Z}/N$, the linear quandle is

$$\Lambda_{N,k} := \operatorname{Alex}(\mathbb{Z}/N, \varphi_k), \qquad \varphi_k(x) := kx,$$

so that $s_y(x) = kx + (1-k)y$; as a $\mathbb{Z}[t^{\pm 1}]$-module it is $\mathbb{Z}[t^{\pm 1}]/(N, t-k)$ [7, 1]. Thus $\Lambda_{N,-1}$ is the dihedral quandle R_N, and $\Lambda_{N,k}$ is trivial exactly when $k \equiv 1$. Section 2 extends the notation to every $k \in \mathbb{Z}/N$, which is what lets the counts below be quantified over k and which changes no count. Throughout we write N for the order of a linear quandle; the source writes $\Lambda_{n,k}$, and we reserve n for the parameter of the conjectured family.

What the source proves, and what it leaves open. Ta [9] classifies the good involutions of every subquandle of a twisted conjugation quandle, and in the abelian case obtains the following sharpening of a theorem of Taniguchi [12]: for $Q = \operatorname{Alex}(A,\varphi)$, the set $\operatorname{Good} Q$ is nonempty if and only if Q is a kei, and in that case ρ is a good involution if and only if $\rho(a) = \psi(a) - \varphi(a)$ for some $\psi\colon A \to \operatorname{Fix}\varphi$ with $\psi s_a = \psi = \psi\rho$ for all a [9, Thm. 4.2]. Specialised to a linear quandle, $\operatorname{Fix}\varphi_k = \langle N/d\rangle \cong \mathbb{Z}/d$ with $d = \gcd(N, k-1)$ [9, Obs. 5.5]. From these two facts [9] runs a GAP search and tabulates $|\operatorname{Good}\Lambda_{N,k}|$ for all 47 nontrivial linear quandles of order $N \le 29$ that admit good involutions [9, Table 1], together with the per-order sums [9, Table 2], which are the published terms of sequence A387317 of [8]. Two subfamilies are given in closed form: the dihedral counts $|\operatorname{Good} R_N| \in \{1,2,4\}$, an alternative proof of a theorem of Kamada and Oshiro [3, Thm. 3.2], and

$$|\operatorname{Good}\Lambda_{4n,2n+1}| = \Big(\sum_{i=0}^{\lfloor n/2\rfloor} \frac{n!}{(n-2i)!\,i!}\,2^{n-2i}\Big)^2, \tag{2}$$

sequence A202828 of [8], verified by the author's program for $n \le 5$ [9, Thm. 5.11]; the two entries $(24,13)$ and $(28,15)$ of [9, Table 1] are obtained from (2) rather than from the search. The paper then closes with:

> **Conjecture 5.13** [9]. *Let $n \ge 3$ be an odd integer, and let $k := 2n-1$. Then $|\operatorname{Good}\Lambda_{4n,k}| = 10$.*

introduced by "We conclude with the following conjecture, which our GAP program confirmed for $n = 3, 5, 7$" [9]. Those three values are the entries $(12,5)$, $(20,9)$ and $(28,13)$ of [9, Table 1]. The obstruction to going further is plain: the search uses the two facts above, but it is run one order at a time, over a space of candidate functions ψ that grows with n; a footnote to [9, Thm. 5.11] records that the author's machine could not finish the neighbouring family at $n = 6, 7$.

Results. Our results are the following. Good involutions of a linear quandle exist only when $k^2 = 1$, by [9, Lem. 4.1 and Thm. 4.2] after [12], and again by Proposition 6.1 below — which is what lets the last five items be stated with no hypothesis on k at all.

- **The conjecture, uniformly in n** (Theorem 4.1). For every odd $n \ge 1$, $|\operatorname{Good}\Lambda_{4n,2n-1}| = 10$. In particular Conjecture 5.13 of [9] holds as stated,

and for instance $|\operatorname{Good}\Lambda_{36,17}| = |\operatorname{Good}\Lambda_{164,81}| = 10$, the first of these being the first member of the family beyond the author's computation.

- **A reduction independent of** N (Theorem 3.1). If $N = gm$, $k^2 = 1$, and the ideal $(k-1)$ of $\mathbb{Z}/N$ equals the ideal (g), then

$$|\operatorname{Good}\Lambda_{N,k}| = \#\{\, D\colon \mathbb{Z}/g \to \mathbb{Z}/g \;:\; D(u) + D(u + cD(u)) = 0 \text{ for all } u \,\}$$

  with $c \equiv m \pmod g$, by an explicit bijection. The parameter g is $\gcd(N, k-1)$, so the search space has size g^g however large N is. For the conjectured family $g = 4$ for every odd n, and c depends on n only through $n \bmod 4 \in \{1, 3\}$; two searches over 256 maps therefore settle every n at once. We claim no novelty for this reduction: it is the specialisation to linear quandles of [9, Thm. 4.2 and Obs. 5.5], and [9] performs the same specialisation inside its GAP program. What it buys is that the specialised statement can be quantified over n.
- **A closed count in the coprime case** (Theorem 5.1). If in addition $\gcd(m, g) = 1$, then $D \mapsto \big(u \mapsto u + cD(u)\big)$ is a bijection onto the involutions of $\mathbb{Z}/g$, so

$$|\operatorname{Good}\Lambda_{N,k}| = I(g),$$

  where $I(g)$ is the number of involutions of a g-element set, sequence A000085 of [8]. This is where the conjectured value comes from: $I(4) = 10$. It also reaches the entries $(21, 8)$ and $(24, 17)$ of [9, Table 1], whose values $232 = I(7)$ and $764 = I(8)$ are out of range for a search over maps.
- **The even companion** (Proposition 4.3). When n is even the count is 4 and not 10. This is Remark 5.14 of [9], deduced there from an isomorphism $\Lambda_{4n,2n-1} \cong R_{4n}$; we obtain it from the same reduction, at $g = 2$. It shows that the parity hypothesis of Conjecture 5.13 does real work.
- **Published values recomputed** (Section 10). Thirty-one of the forty-seven entries of [9, Table 1] are recomputed here as individual numbers: twenty-seven through the reduction, three by an unrestricted search over all N^N self-maps of the carrier, and $(24, 17)$ by Corollary 7.2(1). The three unrestricted searches, together with the good involutions of the trivial quandles $\Lambda_{4,1}$ and $\Lambda_{5,1}$, are what certifies that the formalised predicate is (1) and not a near miss.
- **A dichotomy** (Theorem 6.3). If $k^2 = 1$, $g = \gcd(N, k-1)$ and $m = N/g$, then $\gcd(m, g)$ divides 2; and the value 2 forces $4 \mid N$ (Corollary 6.4). So the coprime hypothesis of Theorem 5.1 is not one case among many but one of exactly two, and every modulus not divisible by 4 lies in it. The statement is elementary and we claim no novelty for it; what it is, is the mechanism.
- **A complete count when** $4 \nmid N$ (Theorem 7.4). For every such N — asymptotically three quarters of all moduli — and every k, the count $|\operatorname{Good}\Lambda_{N,k}|$ is $I(\gcd(N, k-1))$ if $k^2 = 1$ and 0 otherwise. Nothing in [9] is quantified over the modulus: its counting is either a single family or a table. The evaluation of I that this needs is Theorem 7.1, the recurrence of A000085 proved from the definition of an involution; with it $|\operatorname{Good}\Lambda_{24,17}| = 764$ becomes a theorem where the first version of this paper could only quote the value.

- **Values beyond every published table** (Theorem 7.6). Eight counts with $9 \le g \le 16$, from $|\operatorname{Good}\Lambda_{45,19}| = 2620$ to $|\operatorname{Good}\Lambda_{48,17}| = 46\,206\,736$, at orders up to 105 against 29 for [9, Table 1].
- **The per-order sums** (Theorems 8.1 and 8.2). A closed form for sequence A387317 of [8] at every N with $4 \nmid N$, as a sum indexed by the square roots of 1 modulo N, together with its twenty-three values in $[30, 60]$, all beyond the published range of that sequence.
- **A two-case classification** (Theorem 9.1). For every N and k the count is $I(g)$ or $J(g/2)^2$ according as $\gcd(m, g)$ is 1 or 2, where J is sequence A000898 of [8]. This one is proved in the ordinary way and is *not* machine-checked: its first case is Theorems 5.1 and 7.1 above, which contain Theorem 7.4; its second case is verified only numerically.

An honest assessment. The mathematics here is elementary. A reader who already knows that $\Lambda_{4n,2n-1} \cong T_4 \times R_n$ for odd n, where T_4 is the trivial quandle on four elements (Remark 4.4), and who knows that $\operatorname{Good} T_4$ consists of all 10 involutions of a 4-element set [3, Prop. 3.1], could reconstruct the argument below in about a page. What is new is the statement and not its difficulty: Conjecture 5.13 was open in the record we could consult, and the two closed counts of Theorems 4.1 and 5.1 are not in [9], whose only closed forms are the dihedral values and (2). It is worth saying exactly how those two relate to Theorem 5.1: the dihedral quandle R_N has $g = \gcd(N, N-2) = \gcd(N, 2)$, so its coprime instances are the subcase $g \le 2$ of Theorem 5.1, giving $I(1) = 1$ for odd N and $I(2) = 2$ for $N \equiv 2 \pmod 4$; while the family of (2) has $g = 2n$ and $m = 2$, hence $\gcd(m, g) = 2$ throughout, so it lies entirely outside the coprime regime — which is why its values are squares of $A000085$-like sums rather than $A000085$ values. The regime $g \ge 3$ with $\gcd(N/g, g) = 1$, where the conjecture lives, meets neither.

The same reading applies to the material added in Sections 6–9. Theorem 6.3 is four lines of elementary arithmetic and Theorem 7.1 is classical; what we take to be new is the statement of Theorem 7.4, a count quantified over the modulus, and what follows from it. The reason such a statement was available to us and not to [9] is Theorem 3.1: it makes the problem g symbols wide, and the search of [9] grows with N.

Related work. Nakajima and Yamaguchi [6] study how Good behaves under two constructions. Their first theorem states that if D is the maximal trivial component of a quandle Q and both D and $Q \setminus D$ are nonempty, then $\operatorname{Good} Q \cong \operatorname{Good}(Q \setminus D) \times \operatorname{Inv}(D)$; their second states that $\operatorname{Good}\big(\prod_\lambda Q_\lambda\big) \cong \prod_\lambda \operatorname{Good} Q_\lambda$ for a finite family of *nontrivial connected* quandles [6, Thms. 1.1 and 1.4]. Neither theorem applies to the family of Conjecture 5.13. The first does not, because for $n \ge 2$ the maximal trivial component of $\Lambda_{4n,2n-1}$ is empty: $s_y(x) = x$ for every y forces $(k-1)(x-y) = 0$ for every y and hence $k = 1$, while $k = 2n-1 \ne 1$ in $\mathbb{Z}/4n$ once $n \ge 2$. The second does not, because in the decomposition $T_4 \times R_n$ of Remark 4.4 the factor T_4 is trivial, and [6, Ex. 6.3] shows, by a product of two trivial quandles, that the conclusion can fail when a factor is trivial. (For odd n the product formula does happen to return the right number here, since $|\operatorname{Good} T_4| = 10$ [3, Prop. 3.1] and $|\operatorname{Good} R_n| = 1$ [9, Prop. 5.9]; what fails is the applicability of the theorem, not its conclusion.) Theorem 5.1 may be read as the analogue for a trivial factor of their product theorem, and the mechanism (a coordinate of ρ depends only on the

corresponding coordinate of its argument) is close to theirs; we claim independence for the statement about linear quandles, not for the technique.

One point deserves emphasis, because the abstract of [6] invites a confusion. The conjecture that [6] refutes is Conjecture 11.8 of a *different* paper of Ta [10], namely that a connected noninvolutory quandle has at most one good involution. It is unrelated to Conjecture 5.13 of [9], which is the subject here. Indeed no linear quandle is involved in the two questions at once: by [9, Thm. 4.2] a linear quandle with a good involution is a kei, hence involutory. The same remark separates this paper from a companion manuscript [5], which answers Problem 1.7 of [10] — at which orders does a connected noninvolutory symmetric quandle exist? — for every order below 48. The quandles counted there are noninvolutory, so by [9, Thm. 4.2] none of them is a linear quandle: the two papers count disjoint sets of objects. Work of ours in progress, on markings of a graph realising a kei or a symmetric quandle, extends Table 1 of [11]; its objects are graph quandles, not Alexander quandles.

Organisation. Section 2 fixes notation, Section 3 proves the reduction, Section 4 the conjecture and its even companion, and Section 5 the coprime count. Section 6 removes the hypotheses of those counts and proves the dichotomy; Section 7 counts involutions and proves the classification for $4 \nmid N$; Section 8 treats the per-order sums; Section 9 gives the two-case classification covering the remaining branch, the one statement here that is not machine-checked. Section 10 recomputes published values and records the controls that show each hypothesis is load-bearing; Section 11 says what is *not* settled here; Section 12 describes the machine verification.

This is a revised and extended version. Sections 1–5 keep the numbering of the first version, the added material is Sections 6–9, and the three closing sections are renumbered accordingly.

2. Preliminaries

Throughout, N, g, m denote positive integers and k an element of $\mathbb{Z}/N$. We write the linear quandle operation as

$$s_y(x) := kx + (1-k)y = k(x-y) + y \qquad (x, y \in \mathbb{Z}/N), \tag{3}$$

which is the Alexander quandle operation of $\varphi_k(x) = kx$ [9, Ex. 2.9, Def. 5.1]. The source's Definition 5.1 asks k to be a unit, and (3) defines a quandle exactly then (Proposition 2.1(3)); we allow every $k \in \mathbb{Z}/N$ in (3), so that the counts below can be quantified over k with no side condition. That costs nothing, because a non-unit k has $k^2 \neq 1$ and so $\operatorname{Good}\Lambda_{N,k} = \emptyset$ by Proposition 6.1. We record the basic facts in the form in which they are used; none is new, and the proofs are one-line computations in $\mathbb{Z}/N$.

Proposition 2.1. *Let $k \in \mathbb{Z}/N$. With s as in* (3)*:*

1. *$s_x(x) = x$ for all x;*
2. *$s_x\big(s_y(z)\big) = s_{s_x(y)}\big(s_x(z)\big)$ for all x, y, z;*
3. *if k is a unit then every s_y is a bijection, so $\Lambda_{N,k}$ is a quandle;*
4. *if $k^2 = 1$ then $s_y \circ s_y = \mathrm{id}$ for every y, so $\Lambda_{N,k}$ is a kei, and $\mathrm{id} \in \operatorname{Good}\Lambda_{N,k}$.*

Proof. (1) and (2) are polynomial identities in $\mathbb{Z}/N$ and hold for every k, unit or not. For (3), if $lk = 1$ then $z \mapsto lz - l(1-k)y$ inverts s_y. For (4), $s_y(s_y(x)) = k^2x + (1-k^2)y = x$, so $s_y = s_y^{-1}$, and $\rho = \mathrm{id}$ satisfies both clauses of (1). □

Part (4) is the "if" half of [9, Lem. 4.1 and Thm. 4.2] for linear quandles; the converse, that $\operatorname{Good}\Lambda_{N,k} = \emptyset$ when $k^2 \neq 1$, we use only through [9], except at $(N,k) = (5,2)$ where it is verified directly (Proposition 10.3).

It is convenient to spell the second clause of (1) as a two-sided inverse condition, since $s_{\rho(y)}$ and s_y are maps of a finite set:

$$\rho\rho = \mathrm{id}, \quad \rho s_y = s_y \rho, \quad s_{\rho(y)} s_y = \mathrm{id}, \quad s_y s_{\rho(y)} = \mathrm{id} \qquad (y \in \mathbb{Z}/N). \tag{4}$$

This is the form used in the formalisation. It is equivalent to (1) verbatim.

Finally, we write $\operatorname{Inv}(Y)$ for the set of involutions of a set Y — maps F with $F \circ F = \mathrm{id}$, the identity included — and

$$I(g) := \big|\operatorname{Inv}(\{1,\dots,g\})\big| = \sum_{i=0}^{\lfloor g/2 \rfloor} \frac{g!}{(g-2i)!\, i!\, 2^i},$$

sequence A000085 of [8], whose first values are

$$I(0), I(1), \dots, I(8) \;=\; 1,\ 1,\ 2,\ 4,\ 10,\ 26,\ 76,\ 232,\ 764.$$

3. The reduction

The whole paper rests on the following statement, whose point is that its right-hand side does not mention N.

Theorem 3.1. *Let $N = gm$ with $g, m \geq 1$ and let $k \in \mathbb{Z}/N$ satisfy $k^2 = 1$. Assume that the ideal of $\mathbb{Z}/N$ generated by $k-1$ is the ideal generated by g, that is, that there exist $j, a \in \mathbb{Z}/N$ with*

$$k - 1 = gj \qquad \text{and} \qquad (k-1)a = g. \tag{5}$$

Write $c \in \mathbb{Z}/g$ for the residue of m and let

$$\mathcal{D}_{g,c} := \{\, D\colon \mathbb{Z}/g \to \mathbb{Z}/g \;:\; D(u) + D\big(u + cD(u)\big) = 0 \text{ for all } u \in \mathbb{Z}/g \,\}.$$

Then $D \mapsto \rho_D$, where

$$\rho_D(x) := x + m\,\widetilde{D(\bar{x})} \pmod N$$

with $\bar{x} \in \mathbb{Z}/g$ the residue of x and $\widetilde{v} \in \{0,1,\dots,g-1\}$ the least representative of $v \in \mathbb{Z}/g$, is a bijection from $\mathcal{D}_{g,c}$ onto $\operatorname{Good}\Lambda_{N,k}$. In particular

$$|\operatorname{Good}\Lambda_{N,k}| = |\mathcal{D}_{g,c}|.$$

The hypothesis (5) is not a restriction, only a way of naming g:

Remark 3.2. For $g = \gcd(N, k-1)$ the two conditions (5) always hold: $g \mid k-1$ in $\mathbb{Z}$ gives the first, and Bézout gives a, b with $(k-1)a + Nb = g$, which reduces mod N to the second. We keep (5) as a hypothesis because it is what the proof uses and is a finite check for a concrete pair; that the identification of g with the gcd always works is Lemma 6.2 below, and it is what makes the statements of Section 7 possible.

Proof of Theorem 3.1. Write $d(x) := \rho(x) - x$ for a candidate ρ, and let $\tau\colon \mathbb{Z}/g \to \mathbb{Z}/N$, $\tau(v) := m\widetilde{v}$; since $N = gm$, the map τ is an injective homomorphism whose image is $\{z : gz = 0\}$, and $g\tau(v) = 0$ for all v. Let $\pi\colon \mathbb{Z}/N \to \mathbb{Z}/g$ be reduction mod g. The proof is in four steps.

Step 1. Let $\rho \in \operatorname{Good}\Lambda_{N,k}$. Since $k^2 = 1$, every s_y is an involution by Proposition 2.1(4), so the third clause of (4) reads $s_{\rho(y)} = s_y^{-1} = s_y$; comparing the two affine maps and using (3) gives

$$(k-1)\,d(y) = 0 \qquad (y \in \mathbb{Z}/N). \tag{6}$$

Step 2. From (3), $s_y(x) = x + (k-1)(x-y)$, and the commutation clause gives $\rho(s_y(x)) = s_y(\rho(x)) = s_y(x) + k\,d(x)$. By (6), $k\,d(x) = d(x) + (k-1)d(x) = d(x)$, so

$$d\big(s_y(x)\big) = d(x) \qquad (x, y \in \mathbb{Z}/N). \tag{7}$$

As y ranges over $\mathbb{Z}/N$ the point $s_y(x) = x + (k-1)(x-y)$ ranges over the whole coset $x + (k-1)\mathbb{Z}/N$, which by (5) is $x + g\mathbb{Z}/N$. Hence d is constant on the fibres of π: there is a unique $E\colon \mathbb{Z}/g \to \mathbb{Z}/N$ with $d = E \circ \pi$.

Step 3. Multiplying (6) by a and using $(k-1)a = g$ gives $g\,d(y) = 0$, so d takes values in $\{z : gz = 0\} = \tau(\mathbb{Z}/g)$. Therefore $E = \tau \circ D$ for a unique $D\colon \mathbb{Z}/g \to \mathbb{Z}/g$, that is, $\rho = \rho_D$.

Step 4. For $\rho = \rho_D$ one computes $\pi(\rho_D(x)) = \pi(x) + cD(\pi(x))$, so

$$\rho_D\big(\rho_D(x)\big) = x + \tau\big(D(\pi x)\big) + \tau\big(D(\pi x + cD(\pi x))\big) = x + \tau\big(D(\pi x) + D(\pi x + cD(\pi x))\big),$$

using that τ is additive. Since τ is injective, ρ_D is an involution if and only if $D \in \mathcal{D}_{g,c}$. Conversely, let $D \in \mathcal{D}_{g,c}$. The displayed computation makes ρ_D an involution. Its displacement $\tau(D(\pi x))$ is killed by $k-1$, because $k - 1 = gj$ and $g\tau(v) = 0$; this gives both remaining clauses of (4), since $s_{\rho_D(y)}$ and s_y then agree as maps and $s_y s_y = \mathrm{id}$, and it also gives the commutation clause after observing that $\pi(s_y(x)) = \pi(x)$, again by (5). So $\rho_D \in \operatorname{Good}\Lambda_{N,k}$.

Steps 1–3 show the assignment is onto, and injectivity is the injectivity of τ together with $\pi \circ \iota = \mathrm{id}$ for the section ι of π by least representatives. □

Remark 3.3. Mathematically, Theorem 3.1 is [9, Thm. 4.2] — $\rho(a) = \psi(a) - \varphi_k(a)$ with ψ valued in $\operatorname{Fix}\varphi_k \cong \mathbb{Z}/\gcd(N, k-1)$ and constant on components and on ρ-orbits — specialised to linear quandles, and [9] makes the same specialisation inside its GAP program. We prove it from the definition rather than quote it, so that the formal development does not depend on the source, and state it as one equation on g symbols, the form that can be quantified over a family.

4. The conjecture

Theorem 4.1. *For every odd $n \geq 1$,*

$$|\operatorname{Good}\Lambda_{4n,\,2n-1}| = 10.$$

In particular Conjecture 5.13 of [9] *holds for every odd $n \geq 3$.*

Proof. Put $N = 4n$ and $k = 2n - 1$ in $\mathbb{Z}/N$. First, $k^2 = 4n^2 - 4n + 1 = 1$, because $4n = 0$ in $\mathbb{Z}/4n$. Next we check (5) with $g = 4$ and $m = n$. Since n is odd, $k - 1 = 2n - 2 = 4 \cdot \frac{n-1}{2}$, which is the first condition; and $(k-1)\cdot(-2) = -4n + 4 = 4$ in $\mathbb{Z}/4n$, which is the second — note that the second holds for every n, odd or not, and it is the first that uses the parity. So $g = 4$ for every odd n, however large n is.

By Theorem 3.1, $|\operatorname{Good}\Lambda_{4n,2n-1}| = |\mathcal{D}_{4,c}|$ with c the residue of n modulo 4. As n is odd, $c \in \{1, 3\}$. Both cases are finite: each is a search over the $4^4 = 256$ maps $D\colon \mathbb{Z}/4 \to \mathbb{Z}/4$, testing the four instances of $D(u) + D(u + cD(u)) = 0$. Both searches return 10. □

The two searches are the only exhaustive computations in the proof, and they are the same two computations for every n; nothing in them grows with n. For comparison, the search carried out in [9] starts from the same two facts but is run one order at a time, over a space of candidate functions that grows with n.

Theorem 4.1 includes the degenerate member $n = 1$: there $k = 1$, the quandle $\Lambda_{4,1}$ is trivial, and 10 is the count of *all* involutions of a 4-element set [3, Prop. 3.1], which Proposition 10.1 obtains again by an unrestricted search.

Corollary 4.2. $|\operatorname{Good}\Lambda_{36,17}| = 10$ *and* $|\operatorname{Good}\Lambda_{164,81}| = 10$.

The first of these, $n = 9$, is the first member of the family beyond the values $n = 3, 5, 7$ reported in [9]; those three are recovered as instances of Theorem 4.1, and are also computed independently in Proposition 10.2 below.

Proposition 4.3. *For every even* $n \geq 1$, $|\operatorname{Good}\Lambda_{4n,\,2n-1}| = 4$.

Proof. Again $k^2 = 1$. Take $g = 2$ and $m = 2n$. Then $k - 1 = 2(n - 1)$ gives the first condition of (5), and $(k-1)\cdot(-(n+1)) = 2 - 2n^2 = 2$ in $\mathbb{Z}/4n$, since $2n^2 = 0$ when n is even. Now c is the residue of $2n$ modulo 2, that is $c = 0$, so $\mathcal{D}_{2,0}$ consists of all D with $2D(u) = 0$ in $\mathbb{Z}/2$: all $2^2 = 4$ maps $\mathbb{Z}/2 \to \mathbb{Z}/2$ qualify. □

Proposition 4.3 is Remark 5.14 of [9], which obtains it from the isomorphism $\Lambda_{4n,2n-1} \cong R_{4n}$ for even n [7, Cor. 2.2] together with the dihedral count. We claim nothing new for the statement; we include it because it comes out of the same reduction with $g = 2$ instead of $g = 4$, and because it shows that the parity hypothesis of Conjecture 5.13 is doing work and is not decoration: the two cases differ, and they differ precisely in the value of $\gcd(4n, 2n - 2)$.

Remark 4.4. For odd n there is a structural reading of the number 4. Since $\gcd(4, n) = 1$, the Chinese remainder theorem gives a ring isomorphism $\mathbb{Z}/4n \cong \mathbb{Z}/4 \times \mathbb{Z}/n$ carrying $k = 2n - 1$ to $(1, -1)$, and an Alexander quandle of a product is the product of the Alexander quandles, so

$$\Lambda_{4n,\,2n-1} \;\cong\; \Lambda_{4,1} \times \Lambda_{n,-1} \;=\; T_4 \times R_n,$$

with T_4 the trivial quandle on four elements. The quantity $g = 4$ of the proof of Theorem 4.1 is the order of the trivial factor, and $10 = I(4)$ is $|\operatorname{Good} T_4|$ [3, Prop. 3.1]. This isomorphism is not used anywhere below and is not part of the formalised material; we record it because it is the shortest way to see why the answer is what it is, and because it locates the family relative to [6] as explained in Section 1.

5. The coprime case, and where the ten comes from

Theorem 4.1 produces the number 10 from a search, which explains nothing. The following identification explains it, and covers an infinite family of linear quandles that [9] does not treat in closed form.

Theorem 5.1. *Let* $g \geq 1$ *and let* $c \in \mathbb{Z}/g$ *be a unit. Then*

$$D \;\longmapsto\; F_D, \qquad F_D(u) := u + cD(u),$$

is a bijection from $\mathcal{D}_{g,c}$ *onto* $\operatorname{Inv}(\mathbb{Z}/g)$. *Consequently, if* $N = gm$, $k^2 = 1$, *the ideal condition* (5) *holds, and* $\gcd(m, g) = 1$, *then*

$$|\operatorname{Good}\Lambda_{N,k}| \;=\; |\operatorname{Inv}(\mathbb{Z}/g)| \;=\; I(g).$$

Proof. Let $e \in \mathbb{Z}/g$ with $ec = 1$. If $D \in \mathcal{D}_{g,c}$ then

$$F_D(F_D(u)) = u + cD(u) + cD\big(u + cD(u)\big) = u + c\big(D(u) + D(u + cD(u))\big) = u,$$

so $F_D \in \mathrm{Inv}(\mathbb{Z}/g)$. The map is injective because $cD = cD'$ forces $D = D'$ after multiplying by e. It is onto: given $F \in \mathrm{Inv}(\mathbb{Z}/g)$, set $D(u) := e\big(F(u) - u\big)$. Then $u + cD(u) = F(u)$, so $D(u) + D(u + cD(u)) = e(F(u) - u) + e(F(F(u)) - F(u)) = e(F(F(u)) - u) = 0$, i.e. $D \in \mathcal{D}_{g,c}$, and $F_D = F$.

For the second assertion, $\gcd(m, g) = 1$ makes the residue c of m a unit of $\mathbb{Z}/g$, and Theorem 3.1 identifies $|\operatorname{Good}\Lambda_{N,k}|$ with $|\mathcal{D}_{g,c}|$. □

Outside the formal development, the identity of Theorem 5.1 was compared against direct enumeration for 158 pairs (N, k) with $N < 120$ and $g \leq 10$, and agreed in every case.

The hypothesis $\gcd(m, g) = 1$ says, with $g = \gcd(N, k - 1)$ and $m = N/g$, that the two factors of $N = gm$ are coprime.

Corollary 5.2. *For every odd $n \geq 1$ the set $\operatorname{Good}\Lambda_{4n,2n-1}$ is in bijection with the set of involutions of a 4-element set. Since $I(4) = 10$, this is a second and structural proof of Theorem 4.1.*

Proof. Take $g = 4$, $m = n$ in Theorem 5.1; the hypotheses (5) were checked in the proof of Theorem 4.1, and $\gcd(n, 4) = 1$ because n is odd. The evaluation $I(4) = 10$ is a search over the 4^4 self-maps of a 4-element set. □

The same theorem reaches entries of [9, Table 1] beyond the range of a search over self-maps.

Corollary 5.3. (1) $|\operatorname{Good}\Lambda_{15,11}| = I(5) = 26$ *($g = 5$, $m = 3$);*
(2) $|\operatorname{Good}\Lambda_{21,8}| = I(7) = 232$ *($g = 7$, $m = 3$);*
(3) $|\operatorname{Good}\Lambda_{24,17}| = I(8)$ *($g = 8$, $m = 3$).*

Proof. In each case one checks $k^2 = 1$ and the two conditions (5) for the stated g, and $\gcd(m, g) = 1$; these are finitely many identities in $\mathbb{Z}/N$. For (1) the evaluation $I(5) = 26$ is a search over the $5^5 = 3125$ self-maps of a 5-element set. For (2) that route is not available — $7^7 = 823\,543$ — and instead $I(7)$ is computed as the number of $\sigma \in S_7$ with $\sigma^2 = 1$, a search over $7! = 5040$ permutations, using that an involutive self-map of a finite set is a permutation, so that $\mathrm{Inv}(Y)$ and $\{\sigma \in S_Y : \sigma^2 = 1\}$ correspond; this returns 232. □

The published values for these three entries are 26, 232 and 764 [9, Table 1], matching $I(5), I(7), I(8)$; so (1) and (2) confirm two of them outright. In (3) the identification $|\operatorname{Good}\Lambda_{24,17}| = I(8)$ is proved, but the evaluation of $I(8)$ is beyond the reach of either search: the permutation search at $g = 8$ ranges over $8! = 40\,320$ objects and exceeds the budget we allow a single verified computation, and the search over self-maps is worse. Section 7 removes the obstruction by proving the standard recurrence $I(g) = I(g - 1) + (g - 1)I(g - 2)$ instead of searching, and Corollary 7.2(1) records $|\operatorname{Good}\Lambda_{24,17}| = 764$ as a theorem.

6. Emptiness, and a dichotomy for the reduction parameter

Everything above is conditional: Theorem 3.1 assumes $k^2 = 1$ and the ideal condition (5), and Theorem 5.1 assumes $\gcd(m, g) = 1$ on top of that. This section disposes of all three — the first because it is forced, the second because it holds

automatically at the canonical choice of g, and the third because the only alternative to it is a single further case.

For $k \in \mathbb{Z}/N$ we write $\gcd(N, k-1)$ for the greatest common divisor of N and an integer representative of $k-1$; it does not depend on the representative chosen.

Proposition 6.1. *Let $N \geq 1$ and $k \in \mathbb{Z}/N$. If $\operatorname{Good}\Lambda_{N,k} \neq \emptyset$ then $k^2 = 1$. Consequently $|\operatorname{Good}\Lambda_{N,k}| = 0$ for every k with $k^2 \neq 1$.*

Proof. Let ρ be a good involution. Since $s_0(x) = kx$ and $s_{\rho(0)}(z) = kz + (1-k)\rho(0)$, the third clause of (4) at $y = 0$ reads

$$k^2 x + (1-k)\rho(0) = x \qquad (x \in \mathbb{Z}/N).$$

At $x = 0$ this gives $(1-k)\rho(0) = 0$, and at $x = 1$ it gives $k^2 + (1-k)\rho(0) = 1$. Subtracting the first from the second leaves $k^2 = 1$. □

Proposition 6.1 is not new. It is the "only if" half of [9, Thm. 4.2], which is the abelian sharpening of Taniguchi's theorem that a good involution of the generalised Alexander quandle $\operatorname{GAlex}(G, \varphi)$ of a group G exists if and only if that quandle is a kei [12, Thm. 1.3], combined with [9, Lem. 4.1]: for a linear quandle, being a kei is exactly $k^2 = 1$, whose converse half is Proposition 2.1(4). We give the two-line direct proof because it makes every count below *total* in k — no hypothesis $k^2 = 1$ survives into the final statements — and because it keeps the verification of this paper independent of [9].

Lemma 6.2. *Let $N \geq 1$, $k \in \mathbb{Z}/N$, and put $g := \gcd(N, k-1)$. Then $g \mid N$ and both conditions of (5) hold, that is, there are $j, a \in \mathbb{Z}/N$ with $k - 1 = gj$ and $(k-1)a = g$.*

Proof. Let $v \in \{0, 1, \ldots, N-1\}$ represent $k-1$, so $g = \gcd(N, v)$. From $g \mid v$ in $\mathbb{Z}$ we get $v = gj_0$ and hence $k - 1 = gj$ in $\mathbb{Z}/N$ with j the class of j_0. Bézout gives integers x, y with $g = xN + yv$; reducing modulo N kills xN and leaves $g = (k-1)a$ with a the class of y. □

Lemma 6.2 is Remark 3.2 made into a statement, and it is what allows a theorem to be quantified over N: with it, the pair (N, k) alone determines g, and nothing has to be checked case by case. The next statement is the arithmetic fact that makes the whole problem finite in a second, stronger sense.

Theorem 6.3. *Let $N \geq 1$ and let $k \in \mathbb{Z}/N$ satisfy $k^2 = 1$. Put $g := \gcd(N, k-1)$ and $m := N/g$. Then*

$$\gcd(m, g) \quad \textit{divides} \quad 2.$$

Proof. Everything happens in $\mathbb{Z}$. Let $a \in \{0, 1, \ldots, N-1\}$ represent $k-1$, so that $k = a + 1$ and the hypothesis $k^2 = 1$ says exactly

$$N \mid a(a+2),$$

both factors being non-negative integers. Write $N = gm$ and $a = gj$, possible because $g = \gcd(N, a)$. Then $g \gcd(m, j) = \gcd(gm, gj) = \gcd(N, a) = g$, so $\gcd(m, j) = 1$. Cancelling g in $gm \mid gj(a+2)$ gives $m \mid j(a+2)$, whence $m \mid a+2$ because m and j are coprime. Now $\gcd(m, g)$ divides $a + 2$ through m and divides a through g, so it divides $(a+2) - a = 2$. □

We claim no novelty for Theorem 6.3: it is a repackaging of the folklore identity $\gcd(N, K-1)\gcd(N, K+1) \in \{N, 2N\}$ for $K^2 \equiv 1 \pmod N$, and the proof is four lines. What matters is its effect — the parameter $\gcd(m, g)$, which one would expect to range over the divisors of g, takes only the values 1 and 2. Outside the formal development the conclusion was checked for all 131 950 pairs (N, k) with $k^2 \equiv 1 \pmod N$ and $N \le 20\,000$, of which 39 315 realise the value 2; there were no exceptions.

Corollary 6.4. *In the situation of Theorem 6.3, if moreover* $4 \nmid N$ *then* $\gcd(m, g) = 1$.

Proof. The value is 1 or 2, and if it is 2 then $2 \mid m$ and $2 \mid g$, so $4 \mid gm = N$. □

So the branch a pair (N, k) falls into is decided by the modulus alone, in one direction: a modulus not divisible by 4 can only be in the coprime branch. The converse fails, and Theorem 7.6 exhibits two witnesses, $(N, k) = (48, 17)$ and $(60, 49)$, where $4 \mid N$ and $\gcd(m, g) = 1$ all the same.

7. A complete count for every modulus not divisible by four

Theorem 5.1 identifies $\operatorname{Good}\Lambda_{N,k}$ with the involutions of a g-element set but leaves their number to be found. A search over the g^g self-maps of that set stops at $g = 5$, and the cheaper search over its $g!$ permutations stops at $g = 7$ (Corollary 5.3). The classical recurrence for I stops nowhere; the following theorem is that recurrence, proved from the definition of an involution.

Theorem 7.1. *Define* $\widehat{I}\colon \mathbb{N} \to \mathbb{N}$ *by*

$$\widehat{I}(0) = \widehat{I}(1) = 1, \qquad \widehat{I}(n+2) = \widehat{I}(n+1) + (n+1)\,\widehat{I}(n).$$

Then $|\operatorname{Inv}(Y)| = \widehat{I}(|Y|)$ *for every finite set* Y. *In particular* $\widehat{I} = I$, *so* $I(g) = I(g-1) + (g-1)I(g-2)$ *for* $g \ge 2$.

Proof sketch. For a finite set Y and a subset $S \subseteq Y$ let $\operatorname{Inv}(Y, S)$ be the set of involutions of Y that fix every point outside S. Localising in this way is the point of the argument: the ambient set, and with it the type of the objects being counted, does not change as S shrinks. We prove $|\operatorname{Inv}(Y, S)| = \widehat{I}(|S|)$ by induction on $|S|$; the theorem is the case $S = Y$.

For $S = \emptyset$ both sides are 1. Otherwise fix $u_0 \in S$ and split $\operatorname{Inv}(Y, S)$ according to the value $F(u_0)$, which lies in S: if it did not, then $F(F(u_0)) = F(u_0)$ would contradict $F(F(u_0)) = u_0 \in S$. The part with $F(u_0) = u_0$ is exactly $\operatorname{Inv}(Y, S \setminus \{u_0\})$, and contributes $\widehat{I}(|S|-1)$. For $v \in S \setminus \{u_0\}$, precomposition with the transposition $(u_0\, v)$ carries the part with $F(u_0) = v$ bijectively onto $\operatorname{Inv}(Y, S \setminus \{u_0, v\})$: it lands there because an involution mapping $\{u_0, v\}$ into itself commutes with $(u_0\, v)$, and it is a bijection because it is its own inverse. Each of the $|S|-1$ choices of v contributes $\widehat{I}(|S|-2)$. Adding the two contributions gives the recurrence. □

Nothing here is new mathematics. The recurrence is the one recorded for sequence A000085 of [8], whose reference for it is [4, §5.1.4]; and the explicit sum quoted in Section 2 is the sum over i of [9, Lem. 5.10], which counts the involutions of an n-set having exactly i transpositions. We state and prove it because it is the step that was missing in the count below, and because it replaces every remaining exhaustive search in this paper by an evaluation.

Corollary 7.2. (1) $|\operatorname{Good}\Lambda_{24,17}| = I(8) = 764$*, completing Corollary 5.3(3);*
(2) $|\operatorname{Good}\Lambda_{21,8}| = I(7) = 232$*, with no search over* S_7*;*
(3) $|\operatorname{Good}\Lambda_{N,1}| = I(N)$ *for every* $N \geq 1$*; for instance* $|\operatorname{Good}\Lambda_{20,1}| = 23\,758\,664\,096$*;*
(4) $|\operatorname{Good}\Lambda_{4n,2n-1}| = I(4) = 10$ *for every odd* $n \geq 1$*, with no finite search at all.*

Proof. (1) and (2) are Corollary 5.3(3) and (2) followed by Theorem 7.1. For (3), the quandle $\Lambda_{N,1}$ is trivial and $k-1=0$, so $g=\gcd(N,0)=N$ and $m=1$; Lemma 6.2 supplies (5) and $\gcd(1,N)=1$, so Theorem 5.1 applies with the whole of $\mathbb{Z}/N$ as the reduced problem. (The value also follows from [9, Ex. 2.23], after [3, Prop. 3.1]; we derive it here because it is the sharpest available check on Theorem 7.1, the same two numbers $I(4)=10$ and $I(5)=26$ being obtained by unrestricted search in Proposition 10.1.) (4) is Corollary 5.2 with $I(4)$ evaluated from the recurrence instead of by a search over the 4^4 self-maps of a four-element set. □

Remark 7.3. A remark about the cost of the two routes, not about the mathematics; it is recorded because it is the reason Corollary 5.3(3) could be stated but not evaluated in the earlier version of this paper. Evaluating $I(8)$ as a verified count over the $8! = 40\,320$ permutations of an eight-element set was attempted and abandoned: the computation was stopped by a memory watchdog after 188 seconds at 11.78 GB of resident memory, still unfinished. The neighbouring $I(7)=232$, where the same search does terminate, cost 1 minute 47 seconds at 8.81 GB. Through Theorem 7.1 both values are immediate, and so is $I(20) = 23\,758\,664\,096$, whose corresponding search space has about 10^{26} points.

Theorem 7.4. *Let* $N \geq 1$ *with* $4 \nmid N$*, let* $k \in \mathbb{Z}/N$*, and put* $g := \gcd(N, k-1)$*. Then*

$$|\operatorname{Good}\Lambda_{N,k}| = \begin{cases} I(g) & \text{if } k^2 = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. If $k^2 \neq 1$ this is Proposition 6.1. If $k^2 = 1$, then k is a unit, Lemma 6.2 supplies (5) for this g, and Corollary 6.4 gives $\gcd(m,g)=1$ with $m = N/g$; so Theorem 5.1 gives $|\operatorname{Good}\Lambda_{N,k}| = |\operatorname{Inv}(\mathbb{Z}/g)|$, which is $I(g)$ by Theorem 7.1. □

Two remarks on the shape of this statement. It is quantified over both N and k, which no statement in [9] is: the counting there is either a single family ([9, Prop. 5.9, Thm. 5.11]) or a table. And the hypothesis $4 \nmid N$ is load-bearing rather than technical: at $(N,k) = (16,9)$ one has $4 \mid 16$, $k^2 = 1$ and $g = 8$, and the right-hand side would read $I(8) = 764$ against the true value 5776 [9, Table 1].

Corollary 7.5. *For every odd* $N \geq 1$ *and every* $k \in \mathbb{Z}/N$ *with* $k^2 = 1$, $|\operatorname{Good}\Lambda_{N,k}| = I\big(\gcd(N, k-1)\big)$*; for every other* k *the set* $\operatorname{Good}\Lambda_{N,k}$ *is empty.*

Twenty-four of the forty-seven entries of [9, Table 1] have $4 \nmid N$, and Theorem 7.4 returns all of them at once and without computation — among them the nine dihedral entries at $N = 7, 17, 18, 19, 22, 23, 25, 26, 27$, where $g = \gcd(N,2)$ and the values $I(1)=1$, $I(2)=2$ are those of [9, Prop. 5.9]. It also covers infinitely many moduli no table can; the next statement records what that buys at the low end.

Theorem 7.6. *The eight counts of Table 1 hold; each of them lies outside the range of every published table. In each row* $k^2 = 1$ *in* $\mathbb{Z}/N$*,* $g = \gcd(N, k-1)$*,* $N = gm$ *and* $\gcd(m,g) = 1$*.*

(N,k)	g	m	$\lvert\operatorname{Good}\Lambda_{N,k}\rvert$	(N,k)	g	m	$\lvert\operatorname{Good}\Lambda_{N,k}\rvert$
$(45,19)$	9	5	2 620	$(39,14)$	13	3	568 504
$(30,11)$	10	3	9 496	$(42,29)$	14	3	2 390 480
$(33,23)$	11	3	35 696	$(105,76)$	15	7	10 349 536
$(60,49)$	12	5	140 152	$(48,17)$	16	3	46 206 736

TABLE 1. Counts beyond [9, Table 1], which stops at $N = 29$. Each value is $I(g)$.

Proof sketch. For each row the conditions $k^2 = 1$, $\gcd(N, k-1) = g$, $N = gm$, $\gcd(m, g) = 1$ are finitely many identities and are checked rather than assumed; Theorem 5.1 then gives $\lvert\operatorname{Inv}(\mathbb{Z}/g)\rvert$ and Theorem 7.1 evaluates it. No exhaustive search occurs, which is what makes the rows reachable: the corresponding searches over $\mathcal{D}_{g,c}$ would range over g^g maps, that is over 10^{10} for $(30,11)$ and over $16^{16} \approx 1.8 \cdot 10^{19}$ for $(48,17)$. □

Six of the eight rows have $4 \nmid N$ and are equally instances of Theorem 7.4. The other two, $(60,49)$ and $(48,17)$, are the promised witnesses that the converse of Corollary 6.4 fails: $4 \mid N$ does not by itself put a pair into the second branch. The largest order reached by the search of [9] is 29; the row $(105,76)$ is more than three times that.

8. The per-order sums, and sequence A387317

For $N \geq 1$ put

$$T(N) := \sum_{k \in \mathbb{Z}/N,\ k \neq 1} \lvert\operatorname{Good}\Lambda_{N,k}\rvert,$$

the number of good involutions of all nontrivial linear quandles of order N taken together. Summing over every $k \neq 1$ rather than over units only is harmless: a non-unit k has $k^2 \neq 1$ and contributes 0 by Proposition 6.1. For $3 \leq N \leq 29$ the values of T are the second table of [9], and they are the published terms of sequence A387317 of [8] — an entry of the author of [9] which, as consulted on 29 August 2026, carries the keyword `more`, stops at $N = 29$, and records in its formula field only two special cases, those of [9, Prop. 5.9] and [9, Thm. 5.11].

Theorem 8.1. *For every $N \geq 1$ with $4 \nmid N$,*

$$T(N) = \sum_{\substack{k \in \mathbb{Z}/N,\ k \neq 1 \\ k^2 = 1}} I\big(\gcd(N, k-1)\big),$$

a sum indexed by the square roots of 1 modulo N.

Proof. Apply Theorem 7.4 to each summand. □

Theorem 8.2. *The values of T at the twenty-three integers N with $30 \leq N \leq 60$ and $4 \nmid N$ are those of Table 2.*

Proof sketch. Each value is the finite sum of Theorem 8.1: at most $N - 1$ terms, each of them either 0 or a value of I at a divisor of N, and the whole sum is evaluated exactly. As a control the same evaluation returns the published entries $T(21) = 237$ and $T(27) = 1$ of [9, Table 2]. □

N	$T(N)$	N	$T(N)$	N	$T(N)$	N	$T(N)$
30	9 574	38	2	46	2	54	2
31	1	39	568 509	47	1	55	35 723
33	35 701	41	1	49	1	57	4 809 701 445
34	2	42	2 390 558	50	2	58	2
35	259	43	1	51	211 799 317	59	1
37	1	45	2 647	53	1		

TABLE 2. The per-order sums $T(N)$ for $30 \le N \le 60$, $4 \nmid N$; all twenty-three lie beyond the published range of A387317, which stops at $N = 29$.

One caveat, since it changes what these numbers are good for. Each of the twenty-three values is a theorem, but as an *extension of the published sequence* only $T(30) = 9574$ and $T(31) = 1$ are usable: a sequence is extended contiguously, and the next value $T(32)$ is not settled here, lying in the branch of Section 9. Its dominant term is $|\operatorname{Good}\Lambda_{32,17}| = 1\,049\,760\,000$, which is [9, Thm. 5.11] at $n = 8$; the total $T(32) = 1\,049\,760\,008$ is computed but not proved here. The eight gaps $N = 32, 36, 40, 44, 48, 52, 56, 60$ in Table 2 are exactly the moduli in $[30, 60]$ at which the second branch can occur, so the shape of the table is a picture of the classification.

9. The remaining branch, and a two-case classification

Theorem 6.3 leaves exactly one case open, $\gcd(m, g) = 2$, which by Corollary 6.4 occurs only when $4 \mid N$. We can say what happens there, but not with the standing of the rest of the paper: the following theorem is proved in the ordinary way and has *not* been machine-checked, and neither has anything derived from it below. We mark it as such wherever it is used.

A second classical sequence enters. Let $J\colon \mathbb{N} \to \mathbb{N}$ be given by $J(0) = 1$, $J(1) = 2$ and $J(n+2) = 2J(n+1) + 2(n+1)J(n)$; this recurrence is what defines sequence A000898 of [8], whose first values are

$$J(0), J(1), \ldots, J(8) \;=\; 1,\ 2,\ 6,\ 20,\ 76,\ 312,\ 1384,\ 6512,\ 32400.$$

Equivalently, $J(n)$ counts the elements of order at most 2 in the hyperoctahedral group $\mathbb{Z}/2 \wr S_n$: such an element is a pair (σ, ε) with σ an involution of $\{1, \ldots, n\}$ and $\varepsilon\colon \{1, \ldots, n\} \to \mathbb{Z}/2$ constant on the orbits of σ, so by [9, Lem. 5.10] their number is

$$\sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n!}{(n-2i)!\, i!\, 2^i}\, 2^{\,n-i},$$

which is the sum that [9, Thm. 5.11] writes down before simplifying it. That last reading is ours: what [8] records for A000898 is the recurrence, together with a description of $J(n)$, for $n \ge 1$, as the sum of the degrees of the irreducible representations of the group of $n \times n$ signed permutation matrices.

Theorem 9.1 (not machine-checked)**.** *Let J be as above, and let $N \ge 1$ and $k \in \mathbb{Z}/N$. If $k^2 \ne 1$ then $\operatorname{Good}\Lambda_{N,k} = \emptyset$. If $k^2 = 1$, put $g := \gcd(N, k-1)$,*

$m := N/g$ and $d := \gcd(m, g)$; then $d \in \{1, 2\}$ and

$$|\operatorname{Good}\Lambda_{N,k}| = \begin{cases} I(g) & \text{if } d = 1, \\ J(g/2)^2 & \text{if } d = 2. \end{cases}$$

Proof sketch. The first assertion is Proposition 6.1 and $d \in \{1, 2\}$ is Theorem 6.3, both proved above. For the value, use Theorem 3.1, legitimate by Lemma 6.2, to replace $|\operatorname{Good}\Lambda_{N,k}|$ by $|\mathcal{D}_{g,c}|$ with c the residue of m modulo g. Let $K := \{x \in \mathbb{Z}/g : cx = 0\}$ and $h := |K|$, let $A := \{x \in K : 2x = 0\}$ and $a := |A|$, and let $C := c\,\mathbb{Z}/g$, a subgroup of index h, so that $\mathbb{Z}/g$ is the union of h cosets of C, each of size g/h. Define $W(0) = 1$, $W(1) = a$ and $W(n+2) = aW(n+1) + h(n+1)W(n)$.

For $S \subseteq \mathbb{Z}/g$ let $\operatorname{Cnt}(S)$ be the number of maps $D\colon \mathbb{Z}/g \to \mathbb{Z}/g$ that vanish outside S, satisfy $u + cD(u) \in S$ for $u \in S$, and satisfy $D(u) + D(u + cD(u)) = 0$ for $u \in S$. We claim

$$\operatorname{Cnt}(S) = \prod_r W\big(|S \cap r|\big),$$

the product being over the cosets r of C; at $S = \mathbb{Z}/g$ this is $|\mathcal{D}_{g,c}| = W(g/h)^h$. The claim is proved by induction on $|S|$, the empty set giving 1. Fix $u_0 \in S$, lying in the coset r_0, write $n_r := |S \cap r|$, and split according to $v := u_0 + cD(u_0)$, which lies in $S \cap r_0$. If $v = u_0$ then $cD(u_0) = 0$ and the equation at u_0 reads $2D(u_0) = 0$, so $D(u_0)$ ranges over A: that is a choices, and deleting u_0 is a bijection onto the maps counted by $\operatorname{Cnt}(S \setminus \{u_0\})$. If $v \neq u_0$ then, v being given, $cD(u_0) = v - u_0$ has exactly h solutions and $D(v) = -D(u_0)$ is forced, so deleting both u_0 and v is an h-to-one map onto the maps counted by $\operatorname{Cnt}(S \setminus \{u_0, v\})$. In both cases no third point of S is involved, because $u \mapsto u + cD(u)$ is an involution of $\mathbb{Z}/g$ — the same computation as in the proof of Theorem 5.1, which does not use that c is a unit. Summing the two cases and applying the induction hypothesis gives

$$\operatorname{Cnt}(S) = \Big(a\,W(n_{r_0} - 1) + h\,(n_{r_0} - 1)\,W(n_{r_0} - 2)\Big) \prod_{r \neq r_0} W(n_r),$$

and the bracket is $W(n_{r_0})$ by the recurrence.

Finally, only two cases occur. If $d = 1$ then c is a unit, so $K = \{0\}$, $h = a = 1$, there is one coset, and $W = I$. If $d = 2$ then g is even and $c = 2c_0$ with c_0 invertible modulo $g/2$, so $K = \{0, g/2\}$ and $h = 2$; both elements of K are killed by 2, so $a = 2$; C is the set of even residues, of index 2; and $W = J$. Hence $|\mathcal{D}_{g,c}| = I(g)$ or $J(g/2)^2$ according to d. □

The case $d = 1$ of Theorem 9.1 is Theorem 5.1 with Theorem 7.1, and is machine-checked; the case $d = 2$ is not, and is the only part of this paper in that position. It contains [9, Prop. 5.9], the dihedral count, as the case $g \leq 2$; Conjecture 5.13 of [9] as the case $d = 1$, $g = 4$; and [9, Thm. 5.11], where $N = 4n$, $k = 2n + 1$, $g = 2n$, $m = 2$, so that $d = 2$ and the value is $J(n)^2$ — the identity $J(n)^2 = A202828(n)$ being the first formula recorded in the entry A202828 of [8], where it predates [9], so that we claim neither it nor the value but only the reading of the value as one instance of one classification. It also returns the seven entries of [9, Table 1] that Section 10 leaves untouched: $J(3)^2 = 400$ at $(12, 7)$, $(24, 7)$, $(24, 19)$; $J(4)^2 = 5776$ at $(16, 9)$; $J(5)^2 = 97\,344$ at $(20, 11)$; and $J(6)^2$, $J(7)^2$ at $(24, 13)$, $(28, 15)$. All seven of those lie in the case $d = 2$, so they rest on Theorem 9.1 alone and are not machine-checked; they agree with the published values of [9, Table 1].

Two further comments. First, the conjectural closed form of the first version of this paper, in the parameters $h = \gcd(c, g)$, $g' = g/h$ and $a = \gcd(h, \gcd(2, g))$, is correct but is the wrong statement: $a = \gcd(2, h)$ always, and by Theorem 6.3 $h \in \{1, 2\}$ and $h = a$, so the parameters collapse to the two cases above. Second, the evidence. Before Theorem 9.1 was written down, its right-hand side was compared with a direct count of $\mathcal{D}_{g,c}$ over all g^g maps for every c and every $g \le 9$ — that is 387 420 489 maps for each of the nine values of c at $g = 9$ — with a count over involutions of $\mathbb{Z}/g$ with prescribed fixed points and transpositions for every $g \le 12$, and with a backtracking count on the defining equation for every $g \le 15$; with all 47 entries of [9, Table 1]; with all 27 published terms of A387317; and with [9, Thm. 5.11] for $n \le 8$. There were no discrepancies. That is evidence, not proof, and the difference is exactly what the label on Theorem 9.1 records.

10. Published values, and the controls

Two kinds of check surround the results above. The first is that the formalised predicate is the definition (1) of [9, Def. 2.21] and not a near miss; the second is that the hypotheses of Theorem 3.1 and Theorem 5.1 are all load-bearing.

10.1. **The encoding, checked against known values.**

Proposition 10.1. *Testing every one of the N^N maps $\mathbb{Z}/N \to \mathbb{Z}/N$ against* (4)*, with no structural assumption whatever, gives*

$$|\operatorname{Good}\Lambda_{3,2}| = 1, \qquad |\operatorname{Good}\Lambda_{4,3}| = 4, \qquad |\operatorname{Good}\Lambda_{5,4}| = 1,$$
$$|\operatorname{Good}\Lambda_{4,1}| = 10, \qquad |\operatorname{Good}\Lambda_{5,1}| = 26.$$

The first three are the entries $(3, -1)$, $(4, -1)$, $(5, -1)$ of [9, Table 1]. The last two are the trivial quandles, for which [3, Prop. 3.1] — quoted as Example 2.23 of [9] — forces Good to be the full set of involutions of the carrier, i.e. $I(4) = 10$ and $I(5) = 26$. Passing this check is what makes the counts below meaningful, since every theorem in the paper is a count of the same predicate. The method stops here: at $N = 6$ the space of $6^6 = 46\,656$ maps was beyond the budget for a single verified search.

10.2. **Table 1 through the reduction.**

Proposition 10.2. *The twenty-seven values tabulated below agree with the corresponding entries of* [9, Table 1]*.*

Proof sketch. For each row the hypotheses of Theorem 3.1 — $k^2 = 1$ and the two conditions (5) for the tabulated g — are finitely many identities in $\mathbb{Z}/N$, and are checked rather than assumed; the count is then a search over at most $5^5 = 3125$ maps. □

Together with Proposition 10.1 and Corollary 7.2(1), thirty-one of the forty-seven entries of [9, Table 1] are recomputed here as individual numbers. Of the sixteen that are not, seven have $g \ge 6$ — namely $(12, 7)$, $(24, 7)$, $(24, 19)$, $(16, 9)$, $(20, 11)$, $(24, 13)$, $(28, 15)$, with g running up to 14 — and these seven are exactly the entries of [9, Table 1] that lie in the second branch of Theorem 6.3 at a g too large for a direct search, so Theorem 9.1 — which is not machine-checked — is the only statement here that reaches them. The other nine are the dihedral entries at $N = 7, 17, 18, 19, 22, 23, 25, 26, 27$, which the reduction handles at $g \le 2$ but which

(N,k)	g	m	value	(N,k)	g	m	value	(N,k)	g	m	value
$(6,5)$	2	3	2	$(13,12)$	1	13	1	$(21,8)$	7	3	232
$(8,3)$	2	4	4	$(14,13)$	2	7	2	$(21,13)$	3	7	4
$(8,5)$	4	2	36	$(15,4)$	3	5	4	$(21,20)$	1	21	1
$(8,7)$	2	4	4	$(15,11)$	5	3	26	$(24,5)$	4	6	36
$(9,8)$	1	9	1	$(15,14)$	1	15	1	$(24,11)$	2	12	4
$(10,9)$	2	5	2	$(16,7)$	2	8	4	$(24,23)$	2	12	4
$(11,10)$	1	11	1	$(16,15)$	2	8	4	$(28,13)$	4	7	10
$(12,5)$	4	3	10	$(20,9)$	4	5	10	$(28,27)$	2	14	4
$(12,11)$	2	6	4	$(20,19)$	2	10	4	$(29,28)$	1	29	1

TABLE 3. Entries of [9, Table 1] recomputed through Theorem 3.1, with their reduction data $N = gm$. All rows but $(21,8)$ are obtained by a search over the g^g maps $\mathbb{Z}/g \to \mathbb{Z}/g$; the row $(21,8)$ comes from Theorem 5.1, as in Corollary 5.3.

we do not run individually; all nine have $4 \nmid N$ and are instances of Theorem 7.4. Outside the formal development, all 47 entries were recomputed from the definitions in an auxiliary program: 44 of them by direct enumeration through the reduction, and all 47 by the closed form discussed in Section 11; the per-order sums agree with all 27 terms of A387317 published as of August 2026, and (2) is reproduced for $n = 1, \dots, 8$, giving the first eight terms of A202828.

10.3. **The hypotheses are load-bearing.**

Proposition 10.3. (1) $|\operatorname{Good}\Lambda_{N,k}| \le 10$ *is false in general:* $|\operatorname{Good}\Lambda_{8,5}| = 36$.

(2) $|\operatorname{Good}\Lambda_{N,k}| \ge 1$ *is false in general:* $\operatorname{Good}\Lambda_{5,2} = \emptyset$*, by a search over all* 5^5 *maps.*

(3) *The hypothesis* $k^2 = 1$ *of Theorem 3.1 cannot be dropped: at* $(N,k) = (16,5)$ *both conditions* (5) *hold with* $g = 4$ *and* $|\mathcal{D}_{4,0}| = 16$*, but* $5^2 = 9 \ne 1$ *in* $\mathbb{Z}/16$.

(4) *The second condition of* (5) *cannot be dropped: at* $(N,k) = (8,5)$ *with* $g = 2$ *the first holds and the second fails, and* $|\mathcal{D}_{2,0}| = 4$*, against the true value* 36.

(5) *The hypothesis* $\gcd(m,g) = 1$ *of Theorem 5.1 cannot be dropped: at* $(N,k) = (16,9)$ *with* $g = 8$*,* $m = 2$ *everything else holds, and the true value is* 5776 [9, Table 1]*, not* $I(8) = 764$.

(6) *The hypothesis* $k^2 = 1$ *of Theorem 6.3 cannot be dropped: at* $(N,k) = (16,5)$*, where* $5^2 = 9 \ne 1$ *in* $\mathbb{Z}/16$*, one has* $g = \gcd(16,4) = 4$*,* $m = 4$ *and* $\gcd(m,g) = 4$*, which does not divide* 2.

(7) *Theorem 6.3 cannot be sharpened to* $\gcd(m,g) = 1$*: the value* 2 *is attained, at* $(N,k) = (16,9)$ *with* $g = 8$ *and* $m = 2$*. Both branches are non-empty, the first being realised at* $(24,17)$ *with* $g = 8$ *and* $m = 3$.

(8) *The hypothesis* $4 \nmid N$ *of Theorem 7.4 cannot be dropped: at* $(N,k) = (16,9)$ *one has* $4 \mid 16$ *and* $k^2 = 1$*, and the right-hand side would read* $I(8) = 764$ *against the true value* 5776 [9, Table 1].

Item (1) refutes a too-large reading of Theorem 4.1 — the value 10 is not a bound over all linear quandles — and Proposition 4.3 refutes it in the parameter direction. Item (2) refutes the too-small reading that a linear quandle always has

a good involution, and verifies at one pair the "only if" half of [9, Thm. 4.2]. Items (3)–(5) and (8) each name a concrete pair (N, k) at which dropping one hypothesis leaves a well-formed but wrong count, and items (6) and (7) do the same for the dichotomy, which is a statement about gcd alone and would be false without its hypothesis.

11. What is not settled here

Theorem 9.1 says what the count is in every case. What is not settled here is its second case as a *verified* statement, and with it the seven entries of [9, Table 1] listed in Section 10, the contiguous extension of A387317 past $T(32)$, and the reading of [9, Thm. 5.11] as a sub-case of one classification.

What stands in the way is labour, not computation: no exhaustive search occurs anywhere in Theorem 9.1, and the obstacle is the length of a formal proof of its induction when $h = 2$. Two features of that case are absent when $h = 1$. The induction must carry a product over the two cosets of the even residues rather than a single cardinality, because the partner v of the chosen point u_0 must lie in the coset of u_0; and each orbit contributes a factor 2, so the count is weighted, which is an awkward shape for a formal argument. The weights can be removed: since $a = h = 2$, the weight of a configuration is $2^{\#\mathrm{orbits}}$, and $2^{\#\mathrm{orbits}(F)}$ is the number of maps ε from the carrier to a two-element set with $\varepsilon \circ F = \varepsilon$, so the weighted count becomes a plain count of pairs (F, ε) — which is the reading of J as counting the elements of order at most 2 in $\mathbb{Z}/2 \wr S_{g/2}$ recorded in Section 9. The deletion induction of Theorem 7.1 then transfers with one change, a factor 2 per fibre. The step that does not transfer, and where we expect the difficulty to sit, is the passage from $D \in \mathcal{D}_{g,c}$ to such a pair: reconstructing D from (F, ε) requires choosing, for each u, a solution x of $cx = F(u) - u$, and no canonical choice is antisymmetric under $u \mapsto F(u)$, so the value of ε at $F(u)$ is determined by its value at u only up to a correction.

Two questions seem worth asking beyond that. Is there a description of $\mathrm{Good}\,\Lambda_{N,k}$ in the second branch that does not pass through the coset decomposition — one, say, that makes the square in $J(g/2)^2$ visible as a product of two quandles, in the manner of Remark 4.4? And does the trivial-factor analogue of [6, Thm. 1.4] suggested by Theorem 5.1 hold for a product of a trivial quandle with an arbitrary quandle?

12. Formal verification

Every statement of this paper other than those attributed to the literature, other than Theorem 9.1 and the claims explicitly derived from it, and other than the numerical claims marked in the text as computed but unproved — in Sections 8, 9 and 11 and in Remarks 4.4 and 7.3 — has been formalised and machine-checked in Lean 4 with Mathlib.

The quandle operation (3) and the good-involution predicate (4) are transcribed from [9, Def. 2.1, 2.21, 5.1]; Proposition 10.1 is the transcription check, since it recovers published values with no structural assumption at all. The reasoning layer — Theorem 3.1 in both directions, Theorem 5.1 in both directions, the passage from involutions as self-maps to involutions as permutations used in Corollary 5.3(2), Proposition 6.1, Lemma 6.2, Theorem 6.3 with Corollary 6.4, and the deletion induction behind Theorem 7.1 — is proved from the definitions. At the version of

the library we build on — Mathlib at the revision our build pins, for Lean 4 toolchain `v4.32.0` — there is no count of involutions of a finite set in it at all: searching that revision for a statement relating the cardinality of a finite type to an involution of it returns only `FixedPointFree.odd_card_of_involutive`, the parity fact that a finite group admitting a fixed-point-free involutive automorphism has odd order. So Theorem 7.1 is proved from nothing. That is a statement about the pinned revision, checked on 29 August 2026, and not about the library, which grows.

Every finite computation in the paper is decided by the proof assistant's kernel: the 4^4 and 2^2 searches behind Theorem 4.1 and Proposition 4.3, the N^N searches with $N \leq 5$ behind Proposition 10.1 and Proposition 10.3(2), the g^g searches with $g \leq 5$ behind Section 10, the 7! permutation search behind $I(7) = 232$, and the evaluations of the sums of Theorem 8.1 at the twenty-three moduli of Table 2 and at the two control moduli $N = 21, 27$. The results of Sections 6 and 7 — the dichotomy, the involution count and the classification — involve no exhaustive computation whatever, which is why they reach values such as $|\operatorname{Good}\Lambda_{48,17}| = 46\,206\,736$, whose direct verification would range over 16^{16} objects. No compiled evaluation is used anywhere; the axiom set of every statement is the standard one of the ambient logic, with nothing added; and the development contains no incomplete proof. Repository reference to be added at submission.

Acknowledgements

The tabulated values we recompute are those of [9], whose author also maintains the GAP program and raw data that produced them [13].

References

[1] X.-d. Hou, *Finite modules over* $\mathbb{Z}[t, t^{-1}]$, J. Knot Theory Ramifications **21** (2012), no. 8, 1250079, 28 pp.

[2] S. Kamada, *Quandles with good involutions, their homologies and knot invariants*, Intelligence of Low Dimensional Topology 2006, Ser. Knots Everything **40**, World Sci., Hackensack, NJ, 2007, pp. 101–108.

[3] S. Kamada, K. Oshiro, *Homology groups of symmetric quandles and cocycle invariants of links and surface-links*, Trans. Amer. Math. Soc. **362** (2010), no. 10, 5501–5527; arXiv:0902.4277. The items cited above, Proposition 3.1 (good involutions of trivial quandles) and Theorem 3.2 (the dihedral count), carry those numbers in arXiv:0902.4277v1, the only version, whose journal reference is the article above.

[4] D. E. Knuth, *The Art of Computer Programming, Vol. 3: Sorting and Searching*, 2nd ed., Addison-Wesley, Reading, MA, 1998, §5.1.4. The pointer to §5.1.4 is the reference that [8] records for A000085, in the form "Vol. 3, Section 5.1.4, p. 65"; we reproduce the section number only. The book itself was not consulted, and no page is asserted here.

[5] Korea Superintelligence Labs, *Connected noninvolutory symmetric quandles of order less than* 48, companion manuscript, 2026.

[6] Y. Nakajima, K. Yamaguchi, *Decompositions of good involutions on quandles*, arXiv:2608.19951v1 (2026). The items cited above, namely Theorems 1.1 and 1.4 and Example 6.3, are numbered as in v1, which is the only version so far.

[7] S. Nelson, *Classification of finite Alexander quandles*, Topology Proc. **27** (2003), no. 1, 245–258; arXiv:math/0202281. Corollary 2.2 — the isomorphism criterion for $\mathbb{Z}[t^{\pm 1}]/(n, t-a)$ that [9, Rmk. 5.14] invokes, and the only item of this paper cited above — carries that number in arXiv:math/0202281v2 as well.

[8] The On-Line Encyclopedia of Integer Sequences, sequences A000085, A000898, A202828 and A387317, `https://oeis.org`. The statements made above about the content of these entries refer to those entries as fetched on 29 August 2026. On that date A387317 carried the keyword `nonn,more`; its data field held exactly the twenty-seven terms $n = 3, \ldots, 29$; its last edit was dated 3 September 2025; and its formula field held only two special cases, those of [9, Ex. 5.8,

Prop. 5.9] and [9, Thm. 5.11]. So Table 2 lies entirely beyond its published range. A202828 records $A202828(n) = A000898(n)^2$ as the first line of its formula field; that entry was created in December 2011, long before [9], whose only trace in it is a comment dated 26 August 2025. The recurrences quoted above for A000085 and A000898 are the ones those two entries record.

[9] L. Ta, *Good involutions of twisted conjugation subquandles and Alexander quandles*, arXiv:2508.16772v1 (2025); Comm. Algebra, published online 30 April 2026, DOI 10.1080/00927872.2026.2643415. Every numbered item cited above — Problem 1.2, Definitions 2.1, 2.21 and 5.1, Examples 2.9 and 2.23, Lemmas 4.1 and 5.10, Theorems 4.2 and 5.11, Observation 5.5, Proposition 5.9, Conjecture 5.13, Remark 5.14 and Tables 1 and 2 — was read from the LaTeX source of arXiv v1 of 22 August 2025, the only version, and carries that number in the document that source compiles to. The published version could not be obtained on any route we tried, the last of them on 29 August 2026: the publisher's site answers HTTP 403 on every path, the only open-access copy registered anywhere is the arXiv preprint, zbMATH Open holds a preprint record with no review, and MathSciNet has not indexed the article. The publisher's own deposited metadata records 42 references and pages 1–18, and the arXiv version has 42 bibliography entries and states 18 pages, so we take the numbering to be unchanged. That is an inference and not a verification: a remark added in production would change neither the reference count nor the pagination, and would not be visible to the check just described.

[10] L. Ta, *Good involutions of conjugation subquandles*, arXiv:2505.08090v5 (2025). Problem 1.7 and Conjecture 11.8 are numbered as in v5.

[11] L. Ta, *Graph quandles: generalized Cayley graphs of racks and right quasigroups*, Journal of Non-Associative Structures **1** (2026), no. 1, DOI 10.46298/jonas.17215; arXiv:2506.04437.

[12] Y. Taniguchi, *Good involutions of generalized Alexander quandles*, J. Knot Theory Ramifications **32** (2023), no. 12, Paper No. 2350081, 7 pp.; arXiv:2302.11138. Theorem 1.3, the only item cited above, carries that number in arXiv:2302.11138v1, the only version.

[13] L. Ta, *Symmetric linear quandles*, GAP program and data, `https://github.com/luc-ta/Symmetric-Linear-Quandles` (2025).