THE ORDER OF A COUNTEREXAMPLE: TWO PROBLEMS OF KINYON AND PHILLIPS ON LOOPS WITH LEFT NUCLEAR SQUARES

KOREA SUPERINTELLIGENCE LABS

Abstract. Kinyon and Phillips study loops in which every square lies in two of the three nuclei, and leave three problems open; each of the three asks for a loop with left nuclear squares. We prove that two of them have no counterexample of prime order and none of order twice an odd prime. The theorem behind this is a statement about a single nucleus: a finite loop with left nuclear squares and endomorphic squaring whose order is a prime, or twice an odd prime, has middle nuclear squares and has the automorphic inverse property. Commuting squares, which one of the two problems assumes, is never used. The proof is arithmetic rather than a search: the squaring map is an endomorphism, so the order of the loop is the number of squares times the number of elements of square e; both factors are at least two for a counterexample; and at order $2p$ the two surviving factorizations are killed by a fixed-point-free involution and by the centrality of a two-element kernel. The exclusion is sharp in the sense that it cannot be widened to composite, or even to even, orders: the authors' own Example 5.10 has the hypotheses and fails middle nuclear squares at order $8 = 2{\cdot}4$. We also reproduce one direction of their Theorem 5.4, verify the property profiles of their six example loops, and record an exhaustive search that leaves no counterexample of order 5 or 6. Every theorem below is machine-checked in Lean 4.

1. Introduction

A *loop* $(Q, \cdot, e)$ is a set with a binary operation and a two-sided identity e in which every left translation $L_a\colon x \mapsto ax$ and every right translation $R_a\colon x \mapsto xa$ is a bijection. Associativity is not assumed, and the three *nuclei*

$$\mathrm{Nuc}_\ell(Q) = \{a : ax{\cdot}y = a{\cdot}xy\}, \qquad \mathrm{Nuc}_m(Q) = \{a : xa{\cdot}y = x{\cdot}ay\}, \qquad \mathrm{Nuc}_r(Q) = \{a : xy{\cdot}a = x{\cdot}ya\}$$

record where it does hold. Throughout, juxtaposition binds more tightly than the displayed $\cdot$, so that $xx \cdot yz$ means $(x \cdot x) \cdot (y \cdot z)$; this is the convention of [1], whose notation we follow.

Kinyon and Phillips [1] study the loops in which every *square* $x^2 = xx$ lies in a prescribed nucleus. The three conditions are Bol–Moufang identities:

$$xx \cdot yz = (xx \cdot y)z \qquad \text{left nuclear squares, (LNS),} \tag{1}$$

$$(x \cdot yy)z = x(yy \cdot z) \qquad \text{middle nuclear squares, (MNS),} \tag{2}$$

$$xy \cdot zz = x(y \cdot zz) \qquad \text{right nuclear squares, (RNS).} \tag{3}$$

Three further properties enter: *commuting squares* (CS), the identity $xx \cdot y = y \cdot xx$, which says that every square commutes with every element and not merely with other squares; *endomorphic squaring* (END), the identity $x^2y^2 = (xy)^2$, which says that $s\colon x \mapsto x^2$ is an endomorphism of Q; and the *automorphic inverse property* (AIP), the identity $(xy)^\rho = x^\rho y^\rho$, where x^ρ denotes the right inverse, the unique element with $x\,x^\rho = e$.

The main result of Section 5 of [1] is its Theorem 5.4: in a loop whose squares lie in *two* of the three nuclei, the AIP and endomorphic squaring are equivalent, and when they hold the squares are central. With two nuclei the properties therefore collapse into one another, and what remains open is the one-nucleus world. That is where the three problems of [1] sit; we quote them as Problems 5.6, 5.8 and 5.11 below. The examples that make them open were found with Mace4, and [1] introduces them by saying that they "show that the hypotheses of the theorem are reasonably close to optimal. There are a few unresolved cases we leave as open problems"; no bound on the search is stated.

Results. The main theorem is about a single nucleus and does not mention commuting squares.

Theorem 1.1 (Theorem 7.1 and Corollary 7.3 below)**.** *Let Q be a finite loop with left nuclear squares and endomorphic squaring. If $|Q|$ is a prime, or twice an odd prime, then Q has middle nuclear squares and Q has the automorphic inverse property.*

Since Problem 5.8 asks for a loop with left nuclear squares and endomorphic squaring failing the AIP, and Problem 5.11 asks for one with left nuclear and commuting squares, endomorphic squaring and the AIP failing middle nuclear squares, we obtain:

Corollary 1.2 (Corollary 7.4)**.** *No counterexample to Problem 5.8 or to Problem 5.11 has prime order or order twice an odd prime. In particular there is none of order*

$$10,\ 11,\ 13,\ 14,\ 17,\ 19,\ 22,\ 23,\ 26,\ 29,\ 31,\ 34,\ \ldots$$

Three features of this deserve emphasis. First, the hypotheses are strictly weaker than either problem's: commuting squares is never used, so Theorem 1.1 also settles, at these orders, the implication LNS $\wedge$ CS $\wedge$ END $\Rightarrow$ MNS, whose general validity would answer Problem 5.11 outright. Second, the excluded set is infinite and is produced by a proof, not by a search; the arithmetic ingredient is the identity $|\mathcal{S}| \cdot |\mathcal{K}| = |Q|$ of Section 5, where $\mathcal{S}$ is the set of squares and $\mathcal{K}$ the set of elements of square e. Third, the exclusion cannot be widened: the loop of Example 5.10 of [1] has left nuclear squares and endomorphic squaring, fails middle nuclear squares, and has order $8 = 2 \cdot 4$ (Proposition 8.1). So neither "composite" nor "even" can replace "prime or twice an odd prime", and nothing here answers either problem. Problem 5.6 is untouched by all of this, since it assumes that squaring is *not* an endomorphism.

The rest of the paper supports and delimits Theorem 1.1. Section 3 reproduces the direction of Theorem 5.4 of [1] that explains the shape of the three problems, and verifies the property profiles of the six example loops of [1]. Section 4 records that under LNS and END associativity holds modulo the kernel of squaring, so that a counterexample must have two distinct elements with the same square, and that a counterexample to Problem 5.11 has its squares in the left nucleus *only*. Sections 5–6 contain the counting identity and the two structural facts about elements of square e that drive the main theorem, Section 7 proves it, Section 8 collects the sharpness and non-vacuity checks, and Section 9 records an exhaustive search: no counterexample to any of the three problems has order 5 or 6.

We have not located the statement of Theorem 1.1 in [1] or elsewhere in the literature on nuclear-square loops, of which the closest published item is [3]; nor have we found any restriction on the order of a loop satisfying (1) alone, or (1) together with endomorphic squaring. That is a narrower claim than it may look. Restrictions of this shape are a familiar genre — Bol loops of order $2p$ and of order p^2 are groups [4], and automorphic loops of order p or p^2 are groups [5] — and they exist inside the nuclear-square world too, for the smaller variety of C-loops, whose squares lie in the nucleus and whose admissible orders are restricted in [2, Prop. 3.1]. The methods there — Bol identities, multiplication groups, the Lie ring of an automorphic loop, Steiner quotients — are not available for (1) alone. The searches behind the negative claim are recorded outside this paper: a full-text sweep of an arXiv mirror of some 865 000 papers, OpenAlex, Semantic Scholar, Crossref, zbMATH, and the GAP LOOPS documentation, all as of 28 August 2026. MathSciNet, the standard monographs and the pre-1990 literature were not searched.

2. Preliminaries

All loops here are finite. On a finite carrier the requirement that the translations be bijections is equivalent to two-sided cancellativity, and that is the form used in the formal development.

Definition 2.1. Let Q be a loop and write $x^2 = xx$. We say that Q has

- *left nuclear squares* (LNS) if $x^2 \in \mathrm{Nuc}_\ell(Q)$ for all x, equivalently (1);
- *middle nuclear squares* (MNS) if $x^2 \in \mathrm{Nuc}_m(Q)$ for all x, equivalently (2);

- *right nuclear squares* (RNS) if $x^2 \in \mathrm{Nuc}_r(Q)$ for all x, equivalently (3);
- *commuting squares* (CS) if $x^2y = yx^2$ for all x, y;
- *endomorphic squaring* (END) if $x^2y^2 = (xy)^2$ for all x, y;
- the *automorphic inverse property* (AIP) if $(xy)^\rho = x^\rho y^\rho$ for all x, y, where x^ρ is the unique element with $x\,x^\rho = e$.

Two distinctions are worth stating explicitly, because both are easy to misread and either misreading manufactures spurious counterexamples below. Commuting squares is not the condition that squares commute with one another: it asks that each square commute with *every* element. And the AIP is the *automorphic* inverse property, with no reversal; the antiautomorphic one, $(xy)^\rho = y^\rho x^\rho$ (AAIP), is a different property, and [1] notes that the AIP does not even force inverses to be two-sided. Proposition 8.4 below records concrete separations for both.

In the formal development the AIP is stated in a division-free form, so that it is a condition on the multiplication alone; the two forms agree.

Proposition 2.2. *In a loop Q the following are equivalent: $(xy)^\rho = x^\rho y^\rho$ for all x, y; and: for all x, y, a, b, if $xa = e$ and $yb = e$ then $(xy)(ab) = e$.*

Proof. If the first holds and $xa = e$, $yb = e$, then $a = x^\rho$ and $b = y^\rho$ by uniqueness of the right inverse, so $ab = x^\rho y^\rho = (xy)^\rho$ and $(xy)(ab) = e$. Conversely apply the second to $a = x^\rho$, $b = y^\rho$ and use uniqueness again. □

The three problems, quoted verbatim from [1], are the following; the numbering is that of the compiled source.

Problem 5.6 (Kinyon–Phillips [1])**.** Does there exist an AIP loop with left nuclear and commuting squares but without endomorphic squaring?

Problem 5.8 (Kinyon–Phillips [1])**.** Does there exist a left nuclear square loop with endomorphic squaring but not satisfying the AIP?

Problem 5.11 (Kinyon–Phillips [1])**.** Does there exist a loop with left nuclear and commuting squares, endomorphic squaring and the AIP, but without middle nuclear squares?

Remark 2.3 (normalization). A counterexample to any of the three problems is a single multiplication table. In the formal development a loop of order n is a table on $\{0, 1, \dots, n-1\}$ whose identity element is 0, and the theorems below are quantified over tables in that normal form. Every loop of order n is isomorphic to such a table, and each of the six properties of Definition 2.1 is equational, hence invariant under isomorphism, so no generality is lost. That relabelling argument is standard and is *not* part of the formal development; the machine-checked statements read "no loop table on $\{0, \dots, n-1\}$ with identity 0 is a counterexample".

3. Squares in two nuclei, and the source's examples

We first reproduce the implication from [1] that explains the shape of the three problems.

Theorem 3.1 ([1, Theorem 5.4])**.** *Let Q be a loop whose squares lie in two of the three nuclei. If squaring is an endomorphism, then every square commutes with every element of Q; that is, Q has commuting squares, and hence its squares are central.*

Proof sketch. Three cases, according to which pair of nuclei contains the squares; each is a chain of rewritings, and the chains are those of [1]. Write a for a square and let x be arbitrary.

Left and middle. Using $a, a^2 \in \mathrm{Nuc}_\ell(Q)$, then endomorphic squaring, then $a \in \mathrm{Nuc}_\ell(Q)$ and $a \in \mathrm{Nuc}_m(Q)$,

$$a\big((ax)x\big) = \big(a(ax)\big)x = (a^2x)x = a^2x^2 = (ax)(ax) = a\big(x(ax)\big) = a\big((xa)x\big);$$

cancelling a on the left and x on the right gives $ax = xa$.

Middle and right. Dually, using $a, a^2 \in \mathrm{Nuc}_r(Q)$, endomorphic squaring and $a \in \mathrm{Nuc}_m(Q)$,

$$\big(x(xa)\big)a = x\big((xa)a\big) = x(x \cdot a^2) = x^2a^2 = (xa)(xa) = \big((xa)x\big)a = \big(x(ax)\big)a,$$

and the same two cancellations give $ax = xa$. This is the case [1] calls dual to the preceding one and omits; it is written out in full in the formal development.

Left and right. Here one first shows that a commutes with every square s:

$$\big(a(sa)\big)s = \big((as)a\big)s = (as)(as) = a^2s^2 = a\big(a \cdot s^2\big) = a\big((as)s\big) = \big(a(as)\big)s,$$

whence $sa = as$; and then, with $a \cdot x^2 = x^2 \cdot a$ now available,

$$a\big(x(ax)\big) = (ax)(ax) = a^2x^2 = a(a \cdot x^2) = a(x^2 \cdot a) = a\big(x(xa)\big),$$

so $ax = xa$.

Finally, [1] characterizes the centre of a loop as the intersection of the commutant with any two distinct nuclei; the two-nuclei hypothesis supplies the nuclear half, and the conclusion just proved supplies the commuting half. The argument is uniform in the order of Q and involves no case enumeration. □

Remark 3.2. Theorem 3.1 is the reason each of Problems 5.6–5.11 either assumes commuting squares or works with a single nucleus: as soon as the squares lie in two nuclei and squaring is an endomorphism, commuting squares comes for free and the questions collapse. For Problem 5.11 the collapse is visible inside this paper — a counterexample fails middle nuclear squares by hypothesis and right nuclear squares by Proposition 4.3, so its squares lie in the left nucleus alone.

The examples of [1] mark the boundary of that world. We restate them as machine-checked data. Each table below is the table printed in [1], re-indexed so that the identity is the first element; nothing else is changed.

Proposition 3.3. *The six loops of* [1] *have the property profiles below. In each row the properties* [1] *claims for that loop are among those listed; the remaining entries are further properties of the same table, verified here and not asserted in* [1].

table	*order*	*source*	*verified profile*
E_0	5	*Example 2.2*	*AIP, not AAIP, inverses not two-sided*
E_1	6	*Example 5.5*	$LNS \wedge AIP \wedge \neg END \wedge \neg CS \wedge \neg MNS \wedge \neg RNS$
E_2	6	*Example 5.7*	$MNS \wedge AIP \wedge CS \wedge \neg END \wedge \neg LNS$
E_3	8	*Example 5.9*	$MNS \wedge CS \wedge END \wedge \neg AIP \wedge \neg LNS$
E_4	8	*Example 5.10*	$LNS \wedge END \wedge AIP \wedge \neg CS \wedge \neg MNS \wedge \neg RNS$
E_5	8	*Example 5.12*	$MNS \wedge END \wedge AIP \wedge CS \wedge \neg LNS$

Moreover each witness quoted in [1] *holds at the elements named there: in* E_0 *the left and right inverses of one element differ; in* E_1, $3^2 \cdot 1^2 \neq (3 \cdot 1)^2$ *and* $2^2 \cdot 3 \neq 3 \cdot 2^2$*; in* E_2, $1^2 \cdot 3^2 \neq (1 \cdot 3)^2$*; in* E_3, $(2 \cdot 4)^\rho \neq 2^\rho 4^\rho$*; in* E_4, $2^2 \cdot 2 \neq 2 \cdot 2^2$*; and in* E_5, $(2^2 \cdot 2) \cdot 2 \neq 2^2 \cdot (2 \cdot 2)$*. (Element names refer to the re-indexed tables.)*

Proof sketch. Each profile is a closed decidable proposition about a table of order at most 8 and is discharged by kernel evaluation; there is no appeal to compiled code. This is the load-bearing test that the formal renderings of Definition 2.1 are the notions of [1] and not lookalikes: were any of the six definitions subtly wrong, at least one profile would disagree with the paper. □

The geometry of the three problems is legible in that table: E_1 is Problem 5.6 minus commuting squares, E_4 is Problem 5.11 minus commuting squares, and E_2, E_3, E_5 are the middle-nucleus analogues of the three problems, all realized. In each case exactly one hypothesis is missing, and none of these tables is an answer (Proposition 8.4).

Remark 3.4. In [1] the witness for Example 5.10 is printed as $3^3 \cdot 3$ where $3^2 \cdot 3$ is meant: in that table $3 \cdot 3 = 2$, so the intermediate value $2 \cdot 3$ displayed there is $3^2 \cdot 3$. The values quoted there are otherwise correct. The slip stands in both arXiv versions, v1 and v2, and there is no other version of record; see the bibliography.

4. Associativity modulo the kernel of squaring

The following identity costs four rewritings and constrains a counterexample sharply.

Proposition 4.1. *Let Q be a loop with left nuclear squares and endomorphic squaring. Then*

$$\big((xa)y\big)^2 = \big(x(ay)\big)^2 \qquad \text{for all } x, a, y \in Q,$$

where a is arbitrary and need not be a square.

Proof. Pushing the squaring map through both sides, $((xa)y)^2 = (xa)^2y^2 = (x^2a^2)y^2$ and $(x(ay))^2 = x^2(ay)^2 = x^2(a^2y^2)$, and the two agree because x^2 is left nuclear. □

Since squaring is an endomorphism, its fibres are the cosets of $\mathcal{K} = \{k : k^2 = e\}$ (Lemma 5.1), so Proposition 4.1 says that in such a loop every associator lies in the kernel of squaring: associativity holds modulo that kernel. A counterexample cannot therefore fail associativity wherever it likes.

Corollary 4.2. *Let Q be a loop with left nuclear squares and endomorphic squaring. If squaring is injective then Q is associative, hence a group; such a group is abelian and has the AIP. Consequently any counterexample to Problem 5.8 or to Problem 5.11 has two distinct elements with the same square, and it fails middle nuclear squares only between two such elements: there are x, y, z with $(x \cdot y^2)z \neq x(y^2 \cdot z)$ while $((x \cdot y^2)z)^2 = (x(y^2 \cdot z))^2$.*

Proof. Injectivity turns Proposition 4.1 into $(xa)y = x(ay)$. An associative loop is a group; with endomorphic squaring it is commutative, since $(xy)^2 = x^2y^2$ unwinds to $x(yy) = y(xy)$, hence $(xy)y = (yx)y$, hence $xy = yx$; and in an abelian group $(xy)(x^\rho y^\rho) = e$, which is the AIP. An associative loop has middle nuclear squares, so neither Problem 5.8 nor Problem 5.11 can have an associative counterexample. The last sentence is Proposition 4.1 applied to $a = y^2$ together with the failure of (2). □

Proposition 4.3. *Let Q be a loop with left nuclear and commuting squares. Then Q has middle nuclear squares if and only if it has right nuclear squares. Consequently a counterexample to Problem 5.11 fails RNS as well as MNS — its squares lie in the left nucleus alone — and in a counterexample to Problem 5.6 the conditions MNS and RNS stand or fall together.*

Proof. Five rewritings each way. Writing s for a square, from MNS: $xy \cdot s = s \cdot xy = (sx)y = (xs)y = x(sy) = x(ys)$, where the first and last steps are commuting squares, the second is LNS, and the fourth is MNS. The converse is the same chain read backwards with RNS in place of MNS. □

5. The counting identity

For a loop Q put

$$\mathcal{S} = \{x^2 : x \in Q\}, \qquad \mathcal{K} = \{k \in Q : k^2 = e\},$$

the image and the kernel of the squaring map s.

Lemma 5.1. *Let Q be a finite loop with endomorphic squaring. For $x \in Q$ the fibre of s through x is $x\mathcal{K}$; in particular all fibres have $|\mathcal{K}|$ elements.*

Proof. If $k^2 = e$ then $(xk)^2 = x^2k^2 = x^2$. Conversely, if $y^2 = x^2$, let k be the unique element with $xk = y$; then $x^2k^2 = (xk)^2 = y^2 = x^2$, so $k^2 = e$ by left cancellation. The map $k \mapsto xk$ is injective, so the fibre has exactly $|\mathcal{K}|$ elements. □

Theorem 5.2. *Let Q be a finite loop with endomorphic squaring. Then*

$$|\mathcal{S}| \cdot |\mathcal{K}| = |Q|.$$

Proof. Count Q fibrewise over the image of s and apply Lemma 5.1. □

Theorem 5.2 is the homomorphism theorem for loops — order equals kernel size times image size for a loop endomorphism — and is not new; it is standard, and belongs to the homomorphism theory of loops of [6, Ch. IV]. Its kernel half is published for commutative C-loops in [2, Prop. 5.2], where the squaring map is likewise an endomorphism, and where no cardinalities are taken. The source [1] uses the neighbouring standard fact that each kernel of an iterate s^n is a normal subloop, but only inside its decomposition theory, which assumes that the squares are *central* — the very conclusion Problem 5.11 asks about — so none of that theory applies to a counterexample. What is new here is the use: the identity is the only place where the arithmetic of $|Q|$ enters, and everything in Sections 6–7 is an exploitation of it.

Remark 5.3. Lagrange's theorem fails for loops, and it fails in varieties of exactly this kind: the Steiner loop of order 14 of [2, Example 3.8] has the subloop $\{0, 1, 2, 3\}$ of order 4, and $4 \nmid 14$. (Steiner loops are C-loops, and C-loops have their squares in the nucleus [2].) So Theorem 5.2 is not an instance of Lagrange and cannot be replaced by one; it holds because $\mathcal{S}$ and $\mathcal{K}$ are the image and the kernel of a homomorphism, whose fibres are forced to be equipotent.

6. Involutions, two-element kernels, and a dichotomy

Throughout this section Q is a finite loop. We first dispose of the two degenerate cases.

Proposition 6.1. *Let Q have left nuclear squares and endomorphic squaring. If Q fails middle nuclear squares, or fails the AIP, then $|\mathcal{S}| \geq 2$ and $|\mathcal{K}| \geq 2$.*

Proof. If $|\mathcal{K}| = 1$ then squaring is injective by Lemma 5.1, so Q is an abelian group by Corollary 4.2 and both MNS and the AIP hold. If $|\mathcal{S}| = 1$ then $x^2 = e$ for every x; then MNS holds vacuously because e is nuclear, and the AIP holds because every element is its own right inverse and the identity to be checked reads $(xy)^2 = e$. □

Corollary 6.2. *A loop with left nuclear squares and endomorphic squaring failing middle nuclear squares, or failing the AIP, has composite order.*

Proof. By Theorem 5.2 the order factors as $|\mathcal{S}| \cdot |\mathcal{K}|$ with both factors at least 2, by Proposition 6.1. □

The next two propositions are the two structural facts that take the argument from "composite" to the exclusion of $2p$. Both concern an element of square e; the first uses left nuclear squares, the second does not.

Proposition 6.3. *Let Q have left nuclear squares and endomorphic squaring, and suppose some $s \in \mathcal{S}$ with $s \neq e$ satisfies $s^2 = e$. Then $|\mathcal{S}|$ and $|\mathcal{K}|$ are both even, and hence 4 divides $|Q|$.*

Proof. By LNS, s is left nuclear, so $s(sx) = (ss)x = x$: left translation by s is an involution of Q. It has no fixed point, since $sx = x$ forces $s = e$ by right cancellation. It maps $\mathcal{K}$ into $\mathcal{K}$ because $(sk)^2 = s^2k^2 = e$, and it maps $\mathcal{S}$ into $\mathcal{S}$ because a product of squares is a square. A fixed-point-free involution of a finite set forces the cardinality of that set to be even, so $2 \mid |\mathcal{S}|$ and $2 \mid |\mathcal{K}|$; multiply and use Theorem 5.2. □

Proposition 6.4. *Let Q have endomorphic squaring and suppose $\mathcal{K} = \{e, u\}$ with $u \neq e$. Then u is central: it commutes with every element and lies in all three nuclei.*

Proof. By Lemma 5.1 every fibre of squaring is a pair $\{w, wu\}$. Now $(uw)^2 = u^2w^2 = w^2$, so $uw \in \{w, wu\}$, and $uw = w$ would give $u = e$; hence $uw = wu$. The same two lines applied to $(ux)y$ and to $x(yu)$ — each has the same square as xy and neither equals xy — give $(ux)y = (xy)u = u(xy)$ and $x(yu) = (xy)u$, so u is left and right nuclear. Middle nuclearity follows: $(xu)z = (ux)z = u(xz) = (xz)u = x(zu) = x(uz)$. Note that left nuclear squares is not used. □

Proposition 6.5. *Let Q have left nuclear squares and endomorphic squaring, and suppose $\mathcal{K} = \{e, u\}$ with $u \neq e$ and $u \notin \mathcal{S}$. Then Q is associative, hence a group.*

Proof. Left translation by an element of $\mathcal{S}$ maps $\mathcal{S}$ into itself (endomorphic squaring) and is injective, hence permutes $\mathcal{S}$; so $\mathcal{S}$ is closed under left division. If $a, b \in \mathcal{S}$ have $a^2 = b^2$, the element k with $ak = b$ lies in $\mathcal{K}$ by Lemma 5.1 and in $\mathcal{S}$ by that closure, and $\mathcal{S} \cap \mathcal{K} = \{e\}$ because $u \notin \mathcal{S}$; so $a = b$. Thus squaring is injective on $\mathcal{S}$, hence maps $\mathcal{S}$ onto $\mathcal{S}$. Given $w \in Q$, choose $a \in \mathcal{S}$ with $a^2 = w^2$; then $w \in a\mathcal{K}$, so $w = a$ or $w = au$. Now a is left nuclear by LNS, and au is left nuclear because u is central and left nuclear by Proposition 6.4:

$$(au \cdot p)q = (ua \cdot p)q = \big(u(ap)\big)q = u\big((ap)q\big) = u\big(a(pq)\big) = (ua)(pq) = (au)(pq).$$

So every element of Q is left nuclear and Q is associative. □

Theorem 6.6. *Let Q have left nuclear squares and endomorphic squaring, and suppose Q fails middle nuclear squares, or fails the AIP. Then 4 divides $|Q|$, or else $|\mathcal{S}| \geq 3$ and $|\mathcal{K}| \geq 3$.*

Proof. By Proposition 6.1 both cardinalities are at least 2, and by Corollary 4.2 the loop is not associative. If some $s \in \mathcal{S}$ with $s \neq e$ has $s^2 = e$, Proposition 6.3 gives $4 \mid |Q|$. Otherwise $|\mathcal{S}| = 2$ is impossible, because the non-identity element s of a two-element $\mathcal{S}$ satisfies $s^2 \in \mathcal{S}$ and $s^2 = s$ would force $s = e$, so $s^2 = e$; and $|\mathcal{K}| = 2$ is impossible, because its non-identity element is then not a square and Proposition 6.5 would make Q associative. □

An order is untouched by Theorem 6.6 exactly when it is divisible by 4 or is a product of two factors each at least 3. The orders it *does* exclude are therefore precisely the primes and the numbers $2p$ with p an odd prime, which is the content of the next section.

7. Orders p and $2p$

Theorem 7.1. *Let Q be a finite loop of prime order with left nuclear squares and endomorphic squaring. Then Q has middle nuclear squares and Q has the automorphic inverse property.*

Proof. If either failed, Corollary 6.2 would make $|Q|$ composite. □

Theorem 7.2. *Let p be an odd prime and let Q be a loop of order $2p$ with left nuclear squares and endomorphic squaring. Then Q is associative, or $x^2 = e$ for every $x \in Q$.*

Proof. If $|\mathcal{S}| = 1$ then $x^2 = e$ for all x, and if $|\mathcal{K}| = 1$ then squaring is injective and Q is associative by Corollary 4.2. So assume $|\mathcal{S}|, |\mathcal{K}| \geq 2$. By Theorem 5.2 their product is $2p$, and since p is prime the only possibilities are $(|\mathcal{S}|, |\mathcal{K}|) = (2, p)$ and $(p, 2)$.

In the first case write $\mathcal{S} = \{e, s\}$ with $s \neq e$. Then $s^2 \in \mathcal{S}$, and $s^2 = s$ would give $s = e$; so $s^2 = e$, and Proposition 6.3 makes $|\mathcal{K}| = p$ even, contradicting p odd.

In the second case write $\mathcal{K} = \{e, u\}$. If $u \in \mathcal{S}$ then Proposition 6.3, applied to $s = u$, makes $|\mathcal{S}| = p$ even, again a contradiction. If $u \notin \mathcal{S}$ then Q is associative by Proposition 6.5. □

Corollary 7.3. *Let p be an odd prime and let Q be a loop of order $2p$ with left nuclear squares and endomorphic squaring. Then Q has middle nuclear squares and has the automorphic inverse property.*

Proof. In the associative case Q is a group, which has middle nuclear squares, and with endomorphic squaring it is abelian, hence has the AIP (Corollary 4.2). In the exponent-two case MNS is vacuous and the AIP reads $(xy)^2 = e$, which holds. □

Corollary 7.4. *No counterexample to Problem 5.8 and no counterexample to Problem 5.11 has prime order, and none has order $2p$ with p an odd prime. In particular no loop of order 10, 11, 13 or 14 answers Problem 5.11, and no loop of order 10 or 11 answers Problem 5.8.*

Proof. Both problems assume left nuclear squares and endomorphic squaring, and ask respectively for the failure of the AIP and of middle nuclear squares. Apply Theorem 7.1 and Corollary 7.3; the four named orders are $10 = 2 \cdot 5$, 11, 13 and $14 = 2 \cdot 7$. □

Remark 7.5. Problem 5.11 also assumes commuting squares and the AIP, and neither is used anywhere above. So Theorem 7.1 and Corollary 7.3 settle, at all orders p and $2p$, the strictly stronger implication $\mathrm{LNS} \wedge \mathrm{END} \Rightarrow \mathrm{MNS}$, and in particular the implication $\mathrm{LNS} \wedge \mathrm{CS} \wedge \mathrm{END} \Rightarrow \mathrm{MNS}$, whose validity at every order would answer Problem 5.11. Nothing above bears on Problem 5.6, which assumes that squaring is *not* an endomorphism.

8. Sharpness, non-vacuity, and definitional controls

The results of Sections 6–7 are stated for the exact hypothesis set they need, and each of the following records what happens when one part of it is removed.

Proposition 8.1 (sharpness)**.** *The loop E_4 of* [1, Example 5.10] *has left nuclear squares and endomorphic squaring and fails middle nuclear squares, at order $8 = 2 \cdot 4$, with $|\mathcal{S}| = 2$ and $|\mathcal{K}| = 4$.*

So the exclusion in Corollary 7.4 cannot be widened to composite orders, nor even to even orders: loops with the hypotheses of Theorem 1.1 and without middle nuclear squares exist; they merely cannot have order p or $2p$. This is also the control that prevents the main theorem from being misread as a solution of Problem 5.11.

Proposition 8.2 (non-vacuity)**.** *The cyclic group of order* 6 *has left nuclear squares, commuting squares and endomorphic squaring, with $|\mathcal{S}| = 3$ and $|\mathcal{K}| = 2$, both at least* 2*, at the composite order* 6*. The cyclic group of order* 11 *has every positive hypothesis of Problem 5.11 — left nuclear squares, commuting squares, endomorphic squaring and the AIP — and has middle nuclear squares.*

The second statement matters for reading Corollary 7.4 at $n = 11$: it says that there really are loops of that order satisfying all the positive hypotheses, so the corollary is an assertion about a non-empty class and not a vacuous one.

Proposition 8.3 (endomorphic squaring is load-bearing)**.** *There is a loop C of order* 5 *whose squaring map is not an endomorphism, with $|\mathcal{S}| = 4$ and $|\mathcal{K}| = 2$. For it, $|\mathcal{S}| \cdot |\mathcal{K}| = 8 \neq 5$, the number of squares does not divide the order, and the non-identity element of its two-element kernel lies in none of the three nuclei.*

Thus endomorphic squaring cannot be dropped from Theorem 5.2, nor from Proposition 6.4. Without it not even divisibility survives: in C the number of squares does not divide $|C|$. Compare Remark 5.3.

Proposition 8.4 (definitional and structural controls)**.**

(1) Too small. *The symmetric group S_3 is a group, so its squares lie in all three nuclei, and it fails commuting squares, endomorphic squaring and the AIP. Nuclear hypotheses alone therefore give nothing, and the endomorphic-squaring hypothesis of Problem 5.8 is not decorative.*

(2) Too large. *The cyclic group of order* 6 *has all six properties of Definition 2.1, so no hypothesis set used here is vacuous.*

(3) Commuting squares. *In E_1, E_4 and S_3 the squares commute with one another but not with every element. So the weaker reading of commuting squares is strictly weaker, and adopting it would manufacture order-*6 *"answers" to Problem 5.6.*

(4) AIP versus AAIP. *The two inverse properties are independent in both directions: E_1 has the AIP and not the AAIP, and S_3 has the AAIP and not the AIP.*

(5) Not answers. *E_1 is not a counterexample to Problem 5.6 and E_4 is not one to Problem 5.11; each fails exactly the commuting-squares hypothesis.*

(6) Two nuclei are needed in Theorem 3.1. *E_4 has endomorphic squaring, does not have its squares in two nuclei, and fails commuting squares.*

(7) Endomorphic squaring is needed in Proposition 4.1. *In E_4, which has LNS and END, the two sides of* every *associativity instance have the same square, and yet MNS fails; in E_1, which has LNS but not END, there is an associativity instance whose two sides have different squares. So left nuclear squares alone give nothing here.*

Proof sketch. Every item is a closed decidable statement about explicit tables of order 5, 6, 8 or 11, and each is discharged by kernel evaluation over that table; item (7) is a complete pass over all 8^3 triples of E_4 and all 6^3 triples of E_1. No compiled evaluation is used in this section. □

9. Small orders by exhaustive search

Below the reach of the arithmetic the only instrument is enumeration. A loop of order n in the normal form of Remark 2.3 is a reduced Latin square of order n, so the numbers of tables to inspect are 56 at order 5, 9 408 at order 6 and 16 942 080 at order 7 (sequence A000315 of [7]).

Theorem 9.1. *No loop of order* 5 *and no loop of order* 6 *is a counterexample to Problem 5.6, to Problem 5.8 or to Problem 5.11.*

Proof sketch, and what rests on computation. The space $\{0,\dots,n-1\}^{n\times n}$ of tables has n^{n^2} points — about 2×10^{41} already at $n=7$ — so the universally quantified statement is not decided directly. Instead the table is built one row at a time, keeping a row only if it is injective, sends 0 to its own index, and disagrees with every earlier row in every column. These are exactly the conditions imposed by the loop axioms, and the completeness of the filter is *proved*: the row list of an arbitrary loop table survives every step, by induction on the list of row indices, each step discharged from the loop axioms. That completeness bridge is a kernel proof and uses no computation. What is delegated to compiled evaluation is exactly two Boolean runs, one at $n=5$ and one at $n=6$: the assertion that no table in the enumeration satisfies any of the three problems' conditions. Order 6 is the first order at which any of the three problems could have had an answer, since the boundary examples E_1 and E_2 of [1] live there. Order 7 is roughly 1 800 times larger and is not covered by this enumeration; for Problems 5.8 and 5.11 it is covered instead by Theorem 7.1, 7 being prime. As always in this paper the statement proved is about tables in normal form (Remark 2.3). □

Remark 9.2 (unverified external runs). *Everything in this remark is unverified.* The runs below were carried out in C and in a SAT encoding; they are not part of the machine-checked development, they have not been independently reproduced, and no statement anywhere else in this paper depends on them. They are recorded for orientation only, and a reader who discards this remark loses no theorem. A direct enumeration of reduced Latin squares finds no counterexample to any of the three problems at orders 4 through 7; a propositional encoding, solved with a CDCL solver, returns unsatisfiable for all three problems at orders 8 and 9, while at order 10 the single instance attempted did not finish within an hour on a heavily loaded machine. Ablations at order 8 locate the difficulty: LNS and commuting squares alone do not force MNS there, whereas adding either endomorphic squaring or the AIP does. A caution recorded with those runs is that the counts involved are not monotone in n — the profile LNS∧AIP∧¬END has 60 solutions at order 6, none at order 7 and none at order 8 — so a null result at one order is not evidence about the next. Separately, a structured enumeration of central extensions confirms Corollary 7.3 at order 10 and covers the case $|\mathcal{K}|=2$ at order 12, where 96 loops with LNS and endomorphic squaring fail MNS and none of them has commuting squares.

Remark 9.3 (the frontier). Combining Theorem 9.1, Theorem 7.1 and Corollary 7.3, the machine-checked development leaves, for Problems 5.8 and 5.11, the orders 8, 9, 12, 15, 16, 18, 20, 21, 24, 25, … — and no order that is prime or twice an odd prime, ever. Taking the computations of Remark 9.2 into account as well, the smallest order at which a counterexample to either problem could still live is 12.

10. Verification

Every theorem, proposition, corollary and lemma stated above has been formally verified in Lean 4 (toolchain `v4.32.0`) against *Mathlib* [8, 9] at revision `81a5d257c8e410db227a6665ed08f64fea08e997`; the development contains no `sorry` and no new axioms. The runs reported in Remark 9.2, and the independent C cross-checks mentioned at the end of this section, are the only computations outside that development; both are labelled as such and nothing above depends on either. The arithmetic and structural results — Theorem 5.2, Propositions 6.1, 6.3, 6.4, 6.5, Theorem 6.6, Theorems 7.1 and 7.2 and their corollaries — are proved for an arbitrary order with no decidability and no enumeration, and depend on no axioms beyond `propext`, `Classical.choice` and `Quot.sound`; Proposition 2.2, Theorem 3.1 and Propositions 4.1–4.3 depend on `propext` or on nothing at all. The statements about explicit tables — Proposition 3.3 and all of Section 8 — are discharged by kernel evaluation, not by compiled code. The only place where compiled evaluation is used is Theorem 9.1, and there it is confined to two Boolean assertions, one per order, about an enumeration whose completeness is itself a kernel proof; the reduction from "all tables" to "all tables produced by the enumeration" involves no compiled step. Each theorem of Sections 5–7 was checked exhaustively by an independent implementation in C, over all loops of orders 4 through 7 and over two million loops of order 12, before it was formalized, with no violations found; those runs are external and unverified in the sense of Remark 9.2, and are reported here only as a cross-check on the formalization, not as evidence for any statement. The repository is private; repository reference to be added at submission.

References

[1] M. Kinyon and J. D. Phillips, *Loops with squares in two nuclei*, arXiv:2510.19961 (2025). Theorem, example and problem numbers here are those of **v2** (26 October 2025), the latest version as of 28 August 2026; v1 and v2 differ only by a typographical correction in the abstract. No journal version is recorded in Crossref or zbMATH, and the arXiv record carries no journal reference.

[2] J. D. Phillips and P. Vojtěchovský, *C-loops: an introduction*, Publ. Math. Debrecen **68** (2006), no. 1–2, 115–137; DOI 10.5486/PMD.2006.3187. Also arXiv:math/0701711, whose numbering is the one cited above.

[3] A. Drápal and M. Kinyon, *Normality, nuclear squares and Osborn identities*, Comment. Math. Univ. Carolin. **61** (2020), no. 4, 481–500; arXiv:2006.08734.

[4] R. P. Burn, *Finite Bol loops*, Math. Proc. Cambridge Philos. Soc. **84** (1978), no. 3, 377–385.

[5] M. Kinyon, K. Kunen, J. D. Phillips and P. Vojtěchovský, *The structure of automorphic loops*, Trans. Amer. Math. Soc. **368** (2016), no. 12, 8901–8927; arXiv:1210.1642.

[6] R. H. Bruck, *A Survey of Binary Systems*, Ergebnisse der Mathematik und ihrer Grenzgebiete **20**, Springer, Berlin, 1958. The homomorphism theory of loops is its Chapter IV, *Homomorphism Theory of Loops*, pp. 60–92; we cite the chapter rather than a numbered statement.

[7] OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*, `https://oeis.org`; entry A000315 (reduced Latin squares).

[8] L. de Moura and S. Ullrich, *The Lean 4 Theorem Prover and Programming Language*, in: Automated Deduction — CADE 28, Lecture Notes in Computer Science 12699, Springer, 2021, pp. 625–635.

[9] The mathlib Community, *The Lean mathematical library*, in: Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020), pp. 367–381.