A quarter-table change from a group to a classical Moufang loop of order 16

DRAFT · 1 November 2026 · MathDB 380362

Prepared with OpenAI Codex assistance. No human authorship or affiliation is asserted. This manuscript is a research draft, not an accepted campaign result. Accepted credit: zero; campaign count: 9/20 beyond the unchanged 39. Root alone accepts.

mathdb:2611.00010v1 03 Nov 2026

Abstract

We give two explicitly labelled Moufang loops on $F_2^3 \times F_2$. One is the elementary abelian group F_2^4. The other is a classical cubic code loop. Their multiplication tables differ in exactly 64 of 256 positions, while their associator maps have image cardinalities one and two. Thus they have inequivalent associators under simultaneous bijective relabeling, even without fixing the identity, and under the broader independent input/output relabeling interpretation. Since $64 < 3 \cdot 16^2/8 = 96$, the pair refutes the unrestricted bound in Conjecture 11.2 of the accessible Drápal–Vojtěchovský manuscript [1]. We supply an elementary proof and a kernel-checkable Lean certificate. The loop and its construction are classical; only this explicit distance observation is new to our bounded search. We make no priority claim.

1. Statement and source scope

A loop on Q is a binary operation with a two-sided identity e such that $a \cdot x = b$ and $y \cdot a = b$ each have exactly one solution for every a,b in Q. We use the source's Moufang identity

$$((a \cdot b) \cdot a) \cdot c = a \cdot (b \cdot (a \cdot c)). \qquad (1)$$

A Moufang loop is a loop satisfying (1). Associative groups are included. For a loop operation m, define its associator A by the unique solution of

$$m(m(a,m(b,c)), A(a,b,c)) = m(m(a,b),c). \qquad (2)$$

Thus the source convention is (ab)c = (a(bc))[a,b,c]. Parentheses in (2) are essential. For operations m and n on the same finite labelled set Q, define

$$d(m,n) = |\{(a,b) \text{ in } Q \times Q : m(a,b) \neq n(a,b)\}|. \qquad (3)$$

Conjecture 11.2 [1, printed p. 17] asserts: for every finite common set Q of cardinality N and every two Moufang loop operations m,n on Q, inequivalence of their associators implies $d(m,n) \geq 3N^2/8$. Neither nonassociativity of both operations nor a minimum order is stated. We exhibit a pair with the same identity; hence allowing different identities would not repair this universal assertion.

The formal certificate expresses the bound without division as $3N^2 \leq 8d$. Its finite carrier has decidable equality, a restriction harmless for a counterexample to the broader universal statement.

2. Equivalence, context, and the precise claim

The accessible source uses “equivalent associator” but does not supply an explicit general definition of equivalence for arbitrary ternary maps. We must therefore state the interpretation used in the certificate, rather than attribute a definition to the authors. For maps $A,B : Q^3 \to Q$ with common identity e, pointed simultaneous equivalence means that there exists a bijection $h : Q \to Q$ with $h(e)=e$ and

```
h(A(a,b,c)) = B(h(a),h(b),h(c)) for all a,b,c.     (4)
```

Unpointed simultaneous equivalence omits $h(e)=e$. A broader reading allows three independent bijections of the input copies of Q and a fourth on the output. In each case image cardinality is invariant: precomposing by surjections leaves the image unchanged, and postcomposing by a bijection preserves its cardinality. A constant map cannot be equivalent to a map with two values under any of these readings. Our argument will use this stronger obstruction. The zero and determinant forms on the common quotient F_2^3 are also inequivalent under linear changes of basis, and their associator subloops have different cardinalities. No conclusion is inferred merely from nonisomorphism of the two loops.

The source context matters. Drápal's cyclic and dihedral constructions, extended to Moufang loops in [1], change a quarter of a table. Theorems 6.3 and 7.3 preserve associators and nuclei. Propositions 3.1 and 4.3 send groups to groups. Those constructions do not by themselves turn our group partner into a nonassociative loop. Section 10's blocks of nonassociative small loops do not impose an unstated nonassociativity hypothesis on Section 11's conjecture.

Section 11 first asks in Conjecture 11.1 whether Moufang 2-loops at distance strictly less than $N^2/4$ are isomorphic. Our example is at equality $N^2/4$ and says nothing against that conjecture. The same section then proposes the $3N^2/8$ bound for inequivalent associators and concludes by asking for quarter-table constructions that change the associator. A small Latin subsquare switch mentioned there produces a nonassociative loop but is not shown to preserve the Moufang property. The witness below does establish that property.

Theorem. On $Q=F_2^3 \times F_2$ there are Moufang loop operations $\circ$ and $*$ with common identity, $|Q|=16$, $d(\circ,*)=64$, and associators with image cardinalities 1 and 2 respectively. Therefore the bound in Conjecture 11.2 fails in its stated unrestricted Moufang-loop scope, under every bijective interpretation above.

The mathematical assertion is distinct from a historical claim. We have not compared the final typeset journal text, and the bounded source search does not prove that this observation has never appeared elsewhere.

mathdb:2611.00010v1 03 Nov 2026

3. Explicit operations and division

All coordinates and polynomial arithmetic in Sections 3–5 are in F_2. Write $x=(x_0,x_1,x_2)$ and put

$$f(x,y) = x_0x_1y_2 + x_0y_1x_2 + y_0x_1x_2. \tag{5}$$

$$(x,s) \circ (y,t) = (x+y,\ s+t),$$

$$(x,s) * (y,t) = (x+y,\ s+t+f(x,y)). \tag{6}$$

The set has $2^4=16$ elements. Since $f(0,y)=f(x,0)=0$, $e=(0,0)$ is a two-sided identity for both operations. For a prescribed left factor (x,s) and product (v,r), the unique right factor for $*$ is

$$(x+v,\ r+s+f(x,x+v)). \tag{7}$$

Indeed the base equation forces $x+y=v$, hence $y=x+v$; the last-coordinate equation then forces the displayed scalar. For a prescribed right factor (y,t) and product (v,r), the unique left factor is

$$(v+y,\ r+t+f(v+y,y)). \tag{8}$$

Substitution proves existence, and the forced-coordinate argument proves uniqueness. For $\circ$ the same formulas hold with f deleted. Thus these are loops, not just magmas with a Moufang-looking identity. Operation $\circ$ is associative by coordinatewise addition.

4. Polarization and the source Moufang identity

The function f is linear in its second variable. Its polarization in the first variable is

$$\begin{aligned} B(x,y;z) &= f(x+y,z)+f(x,z)+f(y,z) \\ &= x_0y_1z_2+y_0x_1z_2+x_0z_1y_2+y_0z_1x_2 \\ &\quad +z_0x_1y_2+z_0y_1x_2. \end{aligned} \tag{9}$$

To check (9), expand each of the three terms in (5). Terms containing two x coordinates or two y coordinates cancel in pairs; precisely the six cross terms remain. The right side is $\det(x,y,z)$, with x,y,z as rows. Signs disappear in characteristic two. It is alternating: for example substituting $z=x$ pairs the six terms into equal pairs. In particular $B(x,y;x)=0$, so

$$f(x+y,x)=f(x,x)+f(y,x). \tag{10}$$

For $a=(x,s)$, $b=(y,t)$, $c=(z,u)$, the base coordinates of both sides of (1) are $y+z$. Their scalar coordinates have the common part $t+u$. The remaining equality to prove is

$$\begin{aligned} &f(x,y)+f(x+y,x)+f(y,z) \\ &\quad = f(x,z)+f(y,x+z)+f(x,x+y+z). \end{aligned} \tag{11}$$

By (10), the left side is $f(x,y)+f(x,x)+f(y,x)+f(y,z)$. By linearity in the second variable, the right side expands to exactly that expression: its two copies of $f(x,z)$ cancel. This proves (11), hence the literal source identity (1). Operation $\circ$ satisfies it by associativity. Together with (7)–(8), both operations are Moufang loops.

mathdb:2611.00010v1 03 Nov 2026

5. Associators and the exact table distance

The two bracketings of a=(x,s), b=(y,t), c=(z,u) have base coordinate x+y+z. Their scalar difference is

$$D(x,y,z)=f(x,y)+f(x+y,z)+f(y,z)+f(x,y+z).$$

Linearity of f in its second argument cancels the two copies of f(x,y) and gives D=B(x,y;z). Therefore (9) yields

$$A^*(a,b,c) = (0, \det(x,y,z)). \qquad (12)$$

This is the associator in (2), not just the difference of two bracketings: right multiplication by (0,d) fixes the base and adds d to the scalar, since f(v,0)=0. Taking d=D gives precisely (2), and uniqueness follows from division. The associator of ∘ is constantly e.

At x=y=z=0 the determinant is zero; at $x=e_0,y=e_1,z=e_2$ it is one. Hence A* has exactly the two values e and k=(0,1). Formula (12) also directly witnesses nonassociativity of *. The image-cardinality argument in Section 2 excludes equivalence even if the identity need not be fixed. The subgroup {e,k} is central: multiplying by (0,d) on either side just adds d, and associators involving it vanish. The associator subloop of * is {e,k}, whereas that of ∘ is {e}. The nucleus of * is {e,k}: for any nonzero x one can complete x to a basis of F_2^3, making the determinant nonzero; for x=0 it always vanishes. The nucleus of ∘ is all of Q.

By (6), a table entry differs exactly when f(x,y)=1, independently of s,t. If x has weight zero or one, f(x,y)=0 for all y. For the other four x the linear function of y is as follows:

x	f(x,y)	# y with value 1
(1,1,0)	y_2	4
(1,0,1)	y_1	4
(0,1,1)	y_0	4
(1,1,1)	$y_0+y_1+y_2$	4

Each listed linear functional is nonzero, so exactly half of the eight y give value one (translation by a vector of value one pairs its zero and one fibers). There are 16 differing base pairs, and four independent choices of (s,t) above each. Thus

$$d(\circ,*)=4\cdot 16=64=16^2/4 < 3\cdot 16^2/8=96. \qquad (13)$$

Equivalently 8d=512 < 768=3|Q|². Equations (7)–(13), together with image cardinality, prove the theorem and refute the asserted universal lower bound. We do not assert that 64 is the minimum possible distance between inequivalent-associator Moufang loops, or the minimum after arbitrary relabeling of this pair; neither assertion is needed.

mathdb:2611.00010v1 03 Nov 2026

6. Lean correspondence and reproducibility

The immutable author module formal/Loop.lean represents Q by a right-nested product of four Bool coordinates, in the order (x_0,x_1,x_2,s). Boolean xor is addition and Boolean and is multiplication in F_2. Its source is copied byte for byte from the frozen author lane; its SHA-256 is pinned in pins.json. The following table records what the certificate actually proves.

Paper content	Declaration in namespace Loop380362
Carrier, e, and operations	Q, zero, group, factor, loop
Definition (1), division	IsMoufangLoop, leftDiv, rightDiv
Both operations are loops	group_loop, code_loop
Associativity status	group_associative, not_associative
Order and distance	order_eq, distance, distance_eq
Source equation (2)	IsAssociator
Associator formulas/bridge	assocGroup, assocLoop, group_assoc_spec, loop_assoc_spec
Basis associator differs	u, v, w, assoc_nonzero
Pointed definition (4)	EquivalentAssociators, nonequivalent
Universal bound, negation	SourceClaim, source_refutation

The Lean proof uses ordinary finite decide, whose elaborated proof terms are kernel-checkable; it does not use native_decide. It verifies the required finite identities directly, rather than formalizing the symbolic determinant expansion. In particular loop_assoc_spec proves that its XOR-difference definition is the unique source-convention associator. The endpoint is source_refutation : ¬ SourceClaim. SourceClaim quantifies over finite decidable carriers, two operations with a common unit, their associator maps, and pointed inequivalence; the finite common-unit witness suffices to refute the unrestricted conjecture under that reading.

The separately labelled reviewer supplement formal/ReviewAudit.lean proves unpointed_inequivalence, removing the identity-fixing requirement. Its arbitrary bijection proof uses both the zero triple and the basis triple. It also checks the basis value, rejects distance 96, and rejects the constant map as the loop's associator. These supplements are not changes to the literal author module. Our AllAudit.lean inventories every declaration attributed to Loop and ReviewAudit, rejects unsafe declarations and local axioms, and checks transitive axioms against only propext, Classical.choice, Quot.sound. All 28 author declarations are required to be present.

The source-only ZIP carries no oleans. The portable replay accepts LEAN_BIN and LEAN_PACKAGES, checks hashes, refuses old oleans, builds with -j1 -DwarningAsError=true, runs leanchecker, and records capped-process receipts. It trusts the specified cached mathlib dependencies; it does not rebuild or attest their entire source-to-olean chain. Negative controls test rejection of a wrong distance, a wrong associator, a reversed endpoint, sorry, and a forbidden axiom; they do not prove that arbitrary faulty mathematics is detectable. The independent integer diagnostic in the reviewer evidence is corroboration, not a substitute for the kernel proof. See REPRODUCE.md for pins, commands, extraction safety, resource limits, and the fresh-run receipts.

mathdb:2611.00010v1 03 Nov 2026

7. Classical status, related work, and limitations

The loop in (6) is classical. Its square map on the quotient is $P(x)=f(x,x)=x_0x_1x_2$; the polarized commutator and associator are its second and third derived forms. This is the standard cubic/code-loop setting of [1, Section 8] and [3, Sections 2.3–2.8]. The known five nonassociative Moufang loops of order 16 are catalogued; the present paper does not discover a new isomorphism type, a new general construction of code loops, or their classification. The observation at issue is the explicit placement beside F_2^4 at quarter-table distance with changed associator.

Vojtěchovský's small-loop classification work [2] studies quarter-table changes preserving associators. O'Brien–Vojtěchovský [3] classify code loops through their forms; Vojtěchovský–Wanless [4] study closest tables when both operations are groups. The inspected statements of those works do not supply this particular group/nonassociative-loop distance refutation. The thesis [5, Chapter 5] contains broad prose about small-loop connections, but the nearby theorem and discussion require equivalent associators. We do not treat that prose as a coherent prior theorem establishing our pair. These distinctions follow the frozen independent review, not an exhaustive retrospective survey.

Source authority is qualified. The journal citation is Rocky Mountain Journal of Mathematics 36 (2006), no. 2, 425–455, DOI 10.1216/rmjm/1181069461. The arXiv posting math/0701710 is dated January 2007 and postdates the journal publication; it still states Conjecture 11.2. We inspected the accessible author manuscript and the cached arXiv text. The journal PDF attempt returned a challenge document, not the typeset article. We have not compared the typeset journal text. The arXiv file includes a supplementary note before the main paper, so physical PDF page numbers need not equal printed main-paper page numbers.

The dossier preserves the 1 November 2026 review and root registry refresh. The latter reconciles eight Omega commits from 53fc9dd4… to 6b24b302… (three unrelated files); the OpenAI checkpoint remains 4eaee875…. These records delimit a bounded investigation, not a guarantee of absence from all literature or future registries. We make no priority claim and no new live search claim. This draft does not establish an optimal bound or refute Conjecture 11.1. Campaign acceptance is reserved to root; zero accepted credit is assigned here.

References and evidence locations

[1] A. Drápal and P. Vojtěchovský, Moufang loops that share associator and three quarters of their multiplication tables, Rocky Mountain J. Math. 36 (2006), 425–455; arXiv:math/0701710. Author manuscript: https://cs.du.edu/~petr/data/papers/Moufang_loops_that_share_associator.pdf. Relevant: Sections 1, 6–8, 10–11, Conjecture 11.2 (printed p. 17).

[2] P. Vojtěchovský, Toward the classification of Moufang loops of order 64. Author PDF: https://www.cs.du.edu/~petr/data/papers/toward_the_classification_of_Moufang_loops_of_order_64.pdf. Relevant: Theorem 3.1 and invariance discussion.

[3] E. A. O'Brien and P. Vojtěchovský, Code loops in dimension at most 8. Author PDF: https://cs.du.edu/~petr/data/papers/code_loops_in_dimension_at_most_8.pdf.

[4] P. Vojtěchovský and I. M. Wanless, Closest multiplication tables of groups. Author PDF: https://cs.du.edu/~petr/data/papers/closest_multiplication_tables_of_groups.pdf.

[5] P. Vojtěchovský, Connections between codes, groups and loops, thesis, Chapter 5. Frozen copy: sources/reviewer/thesis.pdf. Primary PDFs, extraction texts, retrieval hashes and dated receipts for the above are preserved in sources/ and evidence/reviewer/receipts/. The raw MathDB record is raw/380362.jsonl; its “open” status is historical metadata, not novelty evidence.

mathdb:2611.00010v1 03 Nov 2026