Inclusions among diassociativity-related loop properties

Warren D. Smith
WDSmith@fastmail.fm

January 30, 2005

***Abstract* — We attempt to find all implications among 19 commonly used diassociativity, Moufang, Bol, alternativity and inverse-related properties in loops. There are 6 among these that appear to be valid in finite but not infinite loops. Under that assumption, we completely settle the problem. We study in detail the apparently-simplest among the 6 nasty cases: the "LRalt⟹2SI" question of whether a left- and right-alternative loop necessarily has 2-sided inverses. We construct an infinite loop in which this is false. However, X must have a 2-sided inverse in any LRalt loop with ≤ 185 elements or in which $X^n = 1$ with $n \leq 13$ (M.K.Kinyon has improved "13" to "31"), results suggesting this is the case in all finite loops. The problem of fully resolving this may be the hardest natural problem in mathematics that is this simply posed.**

Contents

1 Introduction

A *magma* is a set L equipped with a binary operation ab. A *quasigroup* is a magma in which there exists a unique solution x to $yx = z$ (usually denoted $x = y\backslash z$) and to $xy = z$ (usually denoted $x = z/y$). A *loop* is a quasigroup in which there exists an identity element e so $ex = xe = x$ for all $x \in L$. (Colloquially: "a loop is a non-associative group.")

Sometimes the loop operation is regarded as multiplication (in which case we usually call the identity 1), other times it is regarded as addition (in which case we usually call the identity 0). We shall use both notations in this paper.

Probably the most widely studied properties of loops are:

Group: the property of being a *group*, i.e. of obeying the associative law $x \cdot yz = xy \cdot z$;

Moufang: the Moufang property[1] $(x \cdot yz)x = xy \cdot zx$, equivalent to obeying both the left-Bol $x(y \cdot xz) = (x \cdot yx)z$ and right-Bol $x(yz \cdot y) = (xy \cdot z)y$ properties.

Lalt: the left-alternative law $x \cdot xy = xx \cdot y$;

Ralt: the right-alternative law $yx \cdot x = y \cdot xx$;

Flex: the flexible law $xy \cdot x = x \cdot yx$;

LIP: the left-inverse-property $(1/x) \cdot xy = y$;

RIP: the right-inverse-property $yx \cdot (x\backslash 1) = y$;

Antiaut: the law $1/(xy) = (1/y)(1/x)$ of antiautomorphic inverses;

2SI: the law of 2-sided inverses $1/x = x\backslash 1$;

PA: power-associativity (the statement[2] that x^n is unambiguous for all positive integer n); and

3PA: 3-power-associativity $xx \cdot x = x \cdot xx$;

Diassoc: diassociativity (the statement that any two elements of L generate a subgroup).

Despite the large amount of study devoted to these properties, many fundamental questions about them had never been answered. Foremost among these include

1. Which subsets of these properties imply which others?
2. Is there a finite equational basis for (finite set of equations implied by and implying) diassociativity?

The latter question is settled in the companion paper [20]: loop-diassociativity has no finite equational basis. The present paper attacks the former question.

The attack is initially straightforward: we consider all possible subsets among these properties and decide which ones are achievable. Our achievability proofs are simply specific constructions of finite loops, and our unachievability proofs are sequences of logical deductions.

However, a surprising development prevents this attack from attaining victory: it appears there are 6 implications among properties which are true in all finite loops (so that no finite counterexample exists) but false in certain infinite loops (preventing any "pure proof" of that implication i.e. via any finite sequence of deductions in first order logic).

[1] There are 4 Moufang identities, all equivalent by lemma 3.1 p.115 of [2]. The other three are $x(yz \cdot x)x = xy \cdot zx$, $(xy \cdot z)y = x(y \cdot zy)$, and $y(z \cdot yx) = (yz \cdot y)x$.

[2] Warning: Power-associativity is defined slightly differently in the companion paper [20].

Define a loop to be *LR-alternative* if it is both L- and R-alternative, *IPLR* if it is both LR-alternative and IP, *alternative*[3] (Alt) if it is both LR-alternative and flexible, and *IP-alternative* if it is both IP and alternative, i.e. both IPLR and flexible.

Consider the implications in loops in table 1.1. I do not believe these are the only 6 implications of this finiteness-dependent kind in loop theory; instead I suspect that the world of loops is absolutely rife with them.

#	implication	n
1	LRalt $\Longrightarrow$ 2-sided inverses	185
2	Flexible $\wedge$ Ralt $\wedge$ LIP $\Longrightarrow$ Lalt	38
3	Flexible $\wedge$ Ralt $\wedge$ LIP $\Longrightarrow$ RIP	36
4	Alt $\wedge$ LIP $\Longrightarrow$ IP	*
5	Alt $\wedge$ antiaut $\Longrightarrow$ IP	19
6	Lalt $\wedge$ Ralt $\wedge$ RIP $\Longrightarrow$ IP	17

Figure 1.1. 6 implications conjectured to be true in finite but false in infinite loops. Each of the implications is true in all loops with $\leq n$ elements for the value of n tabulated (proven by exhaustive search using `mace4` [10]).

In §4.1 we show statement 1 is false in an infinite loop, so that no "pure" proof of it can exist. Searches with `otter` [11] show there are no short pure proofs of statements 2-6. ▲

Here is my effort to find the *simplest* example of a finiteness-dependent fact about loops:

Theorem 1 (PA$\underset{\mathrm{F}}{\Longrightarrow}$2SI). *Power associativity implies 2-sided inverses in finite loops, but not in infinite loops.*

Proof: An element X in a finite loop obeys $XX_\ell^{n-1} = 1$ for some $n \geq 0$, so by power-associativity $X_\ell^{n-1}X = 1$ proving X has a 2-sided inverse $X^{-1} = X_\ell^{n-1}$. (For exponent notation and the fact n exists see EQ 12 and lemma 4.) But the infinite LRalt loop we shall construct in §4.1 is power associative but lacks 2-sided inverses. □

Obviously, if one of the implications in table 1.1 is false in some infinite loop, then there cannot be a pure proof of it. It is less obvious that the reverse is also true:

Theorem 2. *If any of the 6 implications in table 1.1 has no pure proof, then there is a countably-infinite (or finite) loop in which that implication is violated.*

Proof: Follows immediately from "Gödel's completeness theorem for first-order logics" [4][5][7][14]. □

2 Which subsets of properties imply which?

Any two among {LIP, RIP, antiaut} implies the third[4]. A loop with these three properties is said to have the "inverse property" (IP).[5]

Then our loop properties obey the inclusions in figure 2.1.

All the inclusion relations in figure 2.1 are well known and/or easy except for theorem 1 and these three

1. Bol loops are power-associative [18].
2. Moufang loops are diassociative. This is "Moufang's theorem" of 1933. Section VII.4 page 117 of [2] proves the stronger statement that in a Moufang loop, if $ab \cdot c = a \cdot bc$ then a, b, c generate a subgroup.
3. The question of whether LR-alternative loops have 2-sided inverses (shown with dashed line in figure) turns out to be remarkably complicated, and will be discussed later.

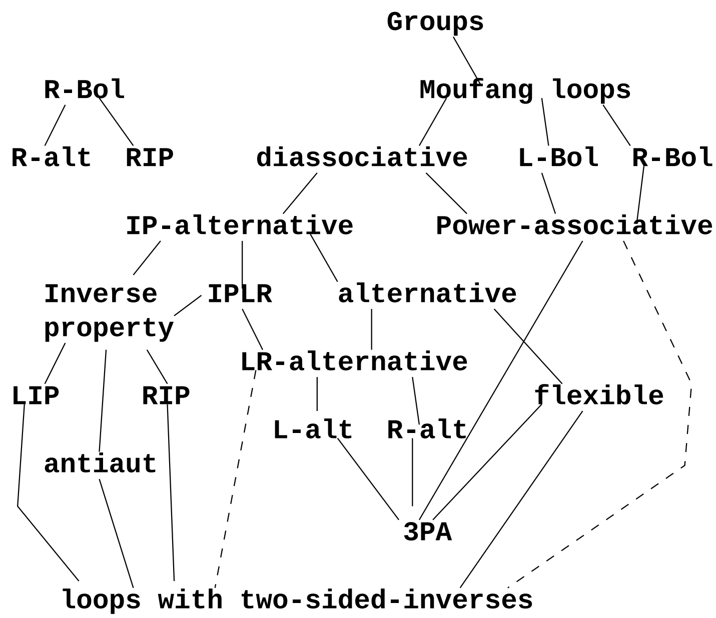

Figure 2.1. Taxonomy of loop-type inclusions. (A much larger version of this taxonomy will be in the upcoming book [21].) ▲

In the presence of antiaut, any left-property and its mirror right-property imply one another, e.g. antiaut causes 2-sided inverses and causes Lalt to imply Ralt. Also, of course, any logical statement (such as R-Bol$\Longrightarrow$RIP, proven by Bol [1]) always has exactly the same validity as its mirrored version (in this case L-Bol$\Longrightarrow$LIP).

Here are statements and proofs of several implications:

1. L-Bol$\wedge$Flexible$\Longrightarrow$Moufang. Proof: Simply apply the flexible identity to the term in parentheses on the right hand side of the L-Bol identity to get the last Moufang identity from footnote 1.
2. L-Bol$\wedge$Ralt$\Longrightarrow$Moufang. Proof: Rename yx to be Q in the LBol identity $(x \cdot yx)z = x(y \cdot xz)$ to get $xQ \cdot z = x((Q/x) \cdot xz)$. Now let $y = Q/x$ to get the Moufang identity $(x \cdot yx)z = x(y \cdot xz)$.

[3] Some other authors have used "alternative" to mean what we call "LR-alternative."

[4] See EQ 1.4-1.8 page 111 of [2].

[5] We also mention Osborn's [15] "Weak Inverse Property" $y((xy)\backslash 1) = x\backslash 1$. We have not seen these two remarks previously: WIP together with any one among {LIP, RIP, antiaut} suffice to imply the full inverse property IP. Also WIP and Lalt together imply that a loop is Ralt. Another candidate for an implication true in finite but not in infinite loops is that WIP and Lalt together imply IP. This is true in loops with ≤ 11 elements. It appears that our flagship question of whether LRalt$\longrightarrow$2SI is unaffected by also assuming WIP and the automorphic inverse property AI. Exhaustive search shows that every WIP and LRAlt loop with ≤ 45 elements has 2-sided inverses, but `otter` indicates that there is no short pure proof of that, and the infinite loop in §4.1 obeys both WIP and AI.

3. L-Bol∧RIP⟹Moufang. Because L-Bol⟹LIP and LIP∧RIP⟹IP⟹antiaut, and antiaut converts L-Bol into R-Bol.
4. LIP⟹2SI. Proof: the LIP with $y = 1/x$ gives $(1/x) \cdot x(1/x) = 1/x$; and since $xy = x \implies y = 1$ we have $x(1/x) = 1$.
5. Lalt∧WIP⟹Ralt:

   To prove: a loop obeying Lalt $xx \cdot y = x \cdot xy$ and WIP $x((yx)\backslash 1) = y\backslash 1$ must obey Ralt $xy \cdot y = x \cdot yy$.

   (i) From Lalt and the definition of $\backslash$ we find $x \cdot x((xx)\backslash y) = y$, $x((xx)\backslash y) = x\backslash y$, and $(xx)\backslash y = x\backslash(x\backslash y)$.

   (ii) From Lalt and the definition of $/$ we find $(y(yx))/x = yy$, then by replacing x with $y\backslash x$ we get $(yx)/(y\backslash x) = yy$, then by taking $x = 1$ we get $y/(y\backslash 1) = yy$.

   (iii) From the final identity in i using the above expression for xx we get $(x/(x\backslash 1))\backslash y = x\backslash(x\backslash y)$.

   (iv) From the definitions of $/$ and $\backslash$ we have:
   $(y/x)\backslash y = x$ and $y/(x\backslash y) = x$.
   and then by taking $y = 1$ in these we have:
   $(1/x)\backslash 1 = x$ and $1/(x\backslash 1) = x$.

   (v) From WIP and $\backslash$ we have $(xy)\backslash 1 = (y\backslash(x\backslash 1))$ from which using the final identity in iv we deduce $xy = 1/(y\backslash(x\backslash 1))$.

   Finale: if Ralt were untrue, i.e. A and B existed so that $(AB)B \neq A \cdot B$, then from Lalt and the expression for BB in ii we would conclude $(AB)B \neq A \cdot B/(B\backslash 1)$, and then by combining this with the conclusions of ii, iii, iv, v we could derive the contradiction: $1/(B\backslash(B\backslash(A\backslash 1)))\backslash \neq 1/(B\backslash(B\backslash(A\backslash 1)))$. QED.

The fact that there are no other inclusion relations besides the ones in the figure is proven by constructing counterexample loops. (For example, the octonions are Moufang but not a group.) The ones we tabulate throughout section 3 more than suffice for that purpose *except* that there are *two* instances where we were unsuccessful at constructing either a finite counterexample or an inclusion proof. These two cases are shown with dashed lines in figure 2.1: the LRalt⟹2SI problem and PA⟹2SI (settled in theorem 1).

How can we attack the question of which subsets among the 19 properties in figure 2.1 imply which? An equivalent question is: which of the $2^{19} = 524288$ possible property-subsets are achievable in loops?

Upon requiring the property subset to obey the inclusions indicated by both the undashed lines in figure 2.1 and PA⟹2SI, the number of possibilities shrinks[6] to 324. If we then also use the fact that antiaut causes any property to imply its mirror property, it shrinks to 202. If we then also employ the implications that any two among {LIP, RIP, antiaut} implies IP, and that LRalt=Lalt∧Ralt, Alt=LRalt∧flex, IPalt=alt∧IP=IPLR∧flex, IPLR=IP∧LRalt, and Moufang=L-Bol∧Ralt=L-Bol∧Flex=L-Bol∧RIP, it shrinks to 79. Further adjoining all 6 of the implications in table 1.1 would shrink the count to 64. Actually, because some of the 64 sets are there twice (in mirror-duplicated form) there are really fewer to worry about.

[6]Shown by exhaustive computer checking of the original 2^{19}.

It then becomes a matter of working through the 64 possibilities with the help of `mace4` and (my own program) `loopbeaut`.

In all 64 cases either `mace4` was able to create an example loop, or such an example arises as a direct product of two `mace4` discoveries. The examples are compiled in §3. Hence:

Theorem 3 (Main result). *Under the assumption that the 6 implications in table 1.1 hold in finite loops, figure 2.1*

1. *lists all inclusion-relations among the 19 finite-loop properties therein;*
2. *all those inclusions are strict;*
3. *all 2^{19} possible subsets of these properties are achieveable except for those forbidden by the implications listed throughout the text of this section. In other words, those implications are the full set; there are no others.*

Additional kinds of loops will be permitted if any of the implications in table 1.1 are invalid.

3 Collected counterexample loops

All have been "beautified," i.e. their elements have been rearranged and renamed in an effort to make the loop's structure maximally apparent from its table. Most are minimum possible cardinality. In all cases the identity element is $e = 0$. "Mirror" examples with all left-handed properties changed to right-handed ones and vice versa, may be got by transposing the matrix and hence are omitted. Taking the direct product of two loops intersects their property-sets. This trick is very useful both for reducing the number of counterexamples needed, and for constructing counterexamples too large for brute force computer searching to find. Although we undoubtably could have used products more, we have chosen to present non-product constructions whenever small ones are available.

*	0	1	2	3	4
0	0	1	2	3	4
1	1	2	4	0	3
2	2	3	1	4	0
3	3	4	0	2	1
4	4	0	3	1	2

Figure 3.1. 5-element loop. Not PA3, 2SI. ▲

*	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	6	1	0	4	5
3	3	0	1	5	6	2	4
4	4	5	0	6	2	1	3
5	5	6	4	2	3	0	1
6	6	4	5	0	1	3	2

Figure 3.2. 7-element loop. PA3, but not LALT, RALT, 2SI. ▲

*	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	0	5	2	1	4
4	4	5	0	1	2	3
5	5	4	1	0	3	2

Figure 3.3. 6-element loop. LALT, but not RALT, 2SI.▲

*	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	0	5	4
2	2	5	0	4	1	3
3	3	0	4	5	2	1
4	4	3	5	1	0	2
5	5	4	1	2	3	0

Figure 3.4. 6-element loop. 2SI, but not LIP, RIP, Antiaut, PA3.▲

*	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	4	0	5	1	3
3	3	5	4	0	2	1
4	4	3	5	1	0	2
5	5	0	1	2	3	4

Figure 3.5. 6-element loop. LIP, but not RIP, Antiaut, PA3.▲

*	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	4	0	5	1	3
3	3	5	1	0	2	4
4	4	3	5	2	0	1
5	5	0	4	1	3	2

Figure 3.6. 6-element loop. Antiaut, but not LIP, RIP, PA3.▲

*	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	5	4	7	6	3	0	1
3	3	6	5	0	7	2	1	4
4	4	3	6	1	0	7	2	5
5	5	4	7	6	1	0	3	2
6	6	7	0	5	2	1	4	3
7	7	0	1	2	3	4	5	6

Figure 3.7. 8-element loop. IP, but not PA3.▲

*	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	5	6	1	0	4
3	3	4	1	0	6	2	5
4	4	5	6	1	0	3	2
5	5	6	0	2	3	4	1
6	6	0	4	5	2	1	3

Figure 3.8. 7-element loop. PA3, 2SI, $xx = e$, but not PA, LIP, RIP, LALT, RALT, FLEX, Antiaut.▲

*	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	0	3	4	5	2
2	2	3	0	5	1	4
3	3	5	4	0	2	1
4	4	2	5	1	0	3
5	5	4	1	2	3	0

Figure 3.9. 6-element loop. PA, $xx = e$, but not LIP, RIP, LALT, RALT, FLEX, Antiaut.▲

*	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	5	7	6	0	1	4
3	3	5	4	6	1	7	0	2
4	4	7	6	5	0	3	2	1
5	5	6	0	1	7	2	4	3
6	6	4	7	0	2	1	3	5
7	7	0	1	2	3	4	5	6

Figure 3.10. 8-element loop. LIP, PA3, but not PA, RIP, LALT, RALT, FLEX, Antiaut.▲

*	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	0	4	5	6	3
2	2	0	1	6	3	4	5
3	3	4	6	5	2	0	1
4	4	5	3	1	6	2	0
5	5	6	4	0	1	3	2
6	6	3	5	2	0	1	4

Figure 3.11. 7-element loop. PA, LIP, but not RIP, LALT, RALT, FLEX, Antiaut.▲

Construction 3.12. LALT, 2SI, but not PA, LIP, RIP, RALT, FLEX, Antiaut: Get a $(12 \cdot 21 = 252)$-element example by taking direct product of 3.13 with 3.35.

*	0	1	2	3	4	5	6	7	8	9	A	B
0	0	1	2	3	4	5	6	7	8	9	A	B
1	1	2	3	0	5	6	B	8	9	A	7	4
2	2	3	0	1	6	B	4	9	A	7	8	5
3	3	0	1	2	7	8	9	6	B	4	5	A
4	4	5	6	7	8	9	A	B	0	1	2	3
5	5	4	B	6	3	2	1	A	7	8	9	0
6	6	7	8	5	A	3	0	1	2	B	4	9
7	7	6	9	4	1	A	3	2	5	0	B	8
8	8	9	A	B	0	1	2	3	4	5	6	7
9	9	8	7	A	B	4	5	0	3	2	1	6
A	A	B	4	9	2	7	8	5	6	3	0	1
B	B	A	5	8	9	0	7	4	1	6	3	2

Figure 3.13. 12-element loop. PA, LALT, but not LIP, RIP, RALT, FLEX, Antiaut.▲

Construction 3.14. LIP, LALT, but not PA, RIP, RALT, FLEX, Antiaut: Get a $(6 \cdot 27 = 162)$-element example by taking direct product of 3.15 with 3.49.

*	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	0	4	5	3
2	2	0	1	5	3	4
3	3	4	5	0	1	2
4	4	5	3	2	0	1
5	5	3	4	1	2	0

Figure 3.15. 6-element loop. PA, LIP, LALT, but not LBOL, RIP, RALT, FLEX, Antiaut.▲

*	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	0	5	6	7	4
2	2	3	0	1	6	7	4	5
3	3	0	1	2	7	4	5	6
4	4	5	6	7	0	1	2	3
5	5	4	7	6	3	2	1	0
6	6	7	4	5	2	3	0	1
7	7	6	5	4	1	0	3	2

Figure 3.16. 8-element loop. LBOL, but not RIP, RALT, FLEX, Antiaut.▲

Construction 3.17. RIP, LALT, but not PA, LIP, RALT, FLEX, Antiaut: Get a $(12 \cdot 27 = 324)$-element example by taking direct product of 3.18 with 3.49.

*	0	1	2	3	4	5	6	7	8	9	A	B
0	0	1	2	3	4	5	6	7	8	9	A	B
1	1	2	3	0	5	6	7	4	A	B	9	8
2	2	3	0	1	6	7	4	5	9	8	B	A
3	3	0	1	2	B	8	A	9	7	5	4	6
4	4	5	6	7	2	3	0	1	B	A	8	9
5	5	9	B	4	8	A	1	2	3	6	0	7
6	6	B	4	A	0	9	2	8	5	7	1	3
7	7	4	A	9	1	B	8	0	6	3	2	5
8	8	A	9	B	7	4	5	6	2	0	3	1
9	9	7	8	5	A	1	B	3	0	2	6	4
A	A	6	7	8	3	0	9	B	4	1	5	2
B	B	8	5	6	9	2	3	A	1	4	7	0

Figure 3.18. 12-element loop. PA, RIP, LALT, but not LIP, RALT, FLEX, Antiaut.▲

*	0	1	2	3	4	5	6	7	8	9	A	B
0	0	1	2	3	4	5	6	7	8	9	A	B
1	1	2	3	0	5	6	7	4	A	B	9	8
2	2	3	0	1	9	B	8	A	6	4	7	5
3	3	0	1	2	7	4	5	6	B	A	8	9
4	4	5	6	7	0	1	2	3	9	8	B	A
5	5	6	B	8	1	2	A	9	7	3	4	0
6	6	B	4	A	8	3	9	1	2	0	5	7
7	7	8	A	6	3	9	B	2	5	1	0	4
8	8	A	9	B	6	7	4	5	0	2	1	3
9	9	7	8	5	2	A	0	B	4	6	3	1
A	A	9	7	4	B	8	3	0	1	5	2	6
B	B	4	5	9	A	0	1	8	3	7	6	2

Figure 3.19. 12-element loop. PA, LIP, RALT, but not RIP, LALT, FLEX, Antiaut.▲

*	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	0	7	6
2	2	3	6	7	0	1	4	5
3	3	6	7	0	1	2	5	4
4	4	5	0	1	6	7	2	3
5	5	0	1	6	7	4	3	2
6	6	7	4	5	2	3	0	1
7	7	4	5	2	3	6	1	0

Figure 3.20. 8-element loop. RIP, RALT, but not PA, LIP, LALT, FLEX, Antiaut.▲

*	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	0	5	3	4
2	2	0	1	4	5	3
3	3	5	4	0	1	2
4	4	3	5	2	0	1
5	5	4	3	1	2	0

Figure 3.21. 6-element loop. PA, RIP, RALT, but not RBOL, LIP, LALT, FLEX, Antiaut.▲

*	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	0	7	6	5	4
2	2	3	0	1	6	7	4	5
3	3	0	1	2	5	4	7	6
4	4	5	6	7	2	3	0	1
5	5	6	7	4	1	0	3	2
6	6	7	4	5	0	1	2	3
7	7	4	5	6	3	2	1	0

Figure 3.22. 8-element loop. RBOL, but not LIP, LALT, FLEX, Antiaut.▲

*	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K	L
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K	L
1	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K	L	0
2	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K	L	0	1
3	3	4	5	6	E	8	F	H	B	0	D	7	J	G	A	C	K	L	9	1	2
4	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K	L	0	1	2	3
5	5	6	E	8	9	A	B	K	D	7	F	G	H	J	C	L	0	1	2	3	4
6	6	E	8	F	A	B	C	L	7	3	G	H	9	K	D	J	1	2	0	4	5
7	7	F	G	A	J	C	D	E	1	2	H	4	K	L	0	8	9	3	B	5	6
8	8	9	A	B	C	D	E	F	G	H	J	K	L	0	1	2	3	4	5	6	7
9	9	A	B	0	D	E	3	G	H	J	K	L	F	1	2	6	4	5	C	7	8
A	A	B	C	D	7	F	G	3	J	K	L	0	1	2	H	4	5	6	E	8	9
B	B	C	D	E	F	G	H	J	K	L	0	1	2	3	4	5	6	7	8	9	A
C	C	D	7	J	G	H	9	5	L	F	1	2	3	4	K	0	E	8	6	A	B
D	D	7	F	G	H	J	K	6	0	1	2	3	4	5	L	E	8	9	A	B	C
E	E	8	9	H	B	K	L	0	F	G	3	J	5	6	7	1	2	A	4	C	D
F	F	G	H	C	K	L	J	1	2	6	4	5	0	7	8	9	A	B	3	D	E
G	G	H	J	K	L	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
H	H	J	K	L	0	1	2	A	4	5	6	E	8	9	3	B	C	D	7	F	G
J	J	K	L	9	1	2	0	4	5	C	7	8	6	A	B	3	D	E	F	G	H
K	K	L	0	1	2	3	4	C	6	E	8	9	A	B	5	D	7	F	G	H	J
L	L	0	1	2	3	4	5	D	E	8	9	A	B	C	6	7	F	G	H	J	K

Figure 3.23. 21-element loop. LRA, 2SI, but not PA, LIP, RIP, FLEX, Antiaut.▲

Construction 3.24. PA, LRA, but not LIP, RIP, FLEX, Antiaut: Get a $(14 \cdot 12 = 168)$-element example by taking direct product of 3.36 with 3.44.

*	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	0	5	1	4
3	3	4	5	2	0	1
4	4	5	1	0	3	2
5	5	0	4	1	2	3

Figure 3.25. 6-element loop. FLEX, but not PA, LIP, RIP, LALT, RALT, Antiaut.▲

*	0	1	2	3	4
0	0	1	2	3	4
1	1	0	3	4	2
2	2	4	0	1	3
3	3	2	4	0	1
4	4	3	1	2	0

Figure 3.26. 5-element loop. PA, FLEX, $xx = e$, but not LIP, RIP, LALT, RALT, Antiaut.▲

Construction 3.27. LIP, FLEX, but not PA, RIP, LALT, RALT, Antiaut: Get a $(12 \cdot 10 = 120)$-element example by taking direct product of 3.28 with 3.47.

*	0	1	2	3	4	5	6	7	8	9	A	B
0	0	1	2	3	4	5	6	7	8	9	A	B
1	1	2	3	0	7	4	B	A	5	6	9	8
2	2	3	0	1	8	9	A	B	4	5	6	7
3	3	0	1	2	5	8	9	4	B	A	7	6
4	4	5	6	7	0	1	2	3	A	B	8	9
5	5	8	9	4	3	0	7	6	1	2	B	A
6	6	9	8	B	A	7	0	5	2	1	4	3
7	7	4	B	A	1	6	5	0	9	8	3	2
8	8	B	A	5	6	3	4	9	0	7	2	1
9	9	A	5	6	B	2	3	8	7	0	1	4
A	A	7	4	9	2	B	8	1	6	3	0	5
B	B	6	7	8	9	A	1	2	3	4	5	0

Figure 3.28. 12-element loop. PA, LIP, FLEX, but not RIP, LALT, RALT, Antiaut.▲

Construction 3.29. LALT, FLEX, but not PA, LIP, RIP, RALT, Antiaut: Get a $(6 \cdot 21 = 162)$-element example by taking direct product of 3.32 with 3.35.

Construction 3.30. PA, LALT, FLEX, but not LIP, RIP, RALT, Antiaut: Get a $(6 \cdot 14 = 84)$-element example by taking direct product of 3.32 with 3.36.

Construction 3.31. LIP, LALT, FLEX, but not PA, RIP, RALT, Antiaut: Get a $(6 \cdot 27 = 162)$-element example by taking direct product of 3.32 with 3.49.

*	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	0	3	2	5	4
2	2	4	0	5	1	3
3	3	5	4	0	2	1
4	4	3	5	1	0	2
5	5	2	1	4	3	0

Figure 3.32. 6-element loop. PA, LIP, LALT, FLEX, $xx = e$, but not LBOL, RIP, RALT, Antiaut.▲

Construction 3.33. RIP, RALT, FLEX, but not PA, LIP, LALT, Antiaut: Get a $(6 \cdot 27 = 162)$-element example by taking direct product of 3.34 with 3.49.

*	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	0	3	4	5	2
2	2	4	0	5	3	1
3	3	5	1	0	2	4
4	4	2	5	1	0	3
5	5	3	4	2	1	0

Figure 3.34. 6-element loop. PA, RIP, RALT, FLEX, $xx = e$, but not RBOL, LIP, LALT, Antiaut.▲

*	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K	L
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K	L
1	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K	L	0
2	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K	L	0	1
3	3	4	5	6	7	8	F	A	B	0	D	E	J	G	H	C	K	L	9	1	2
4	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K	L	0	1	2	3
5	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K	L	0	1	2	3	4
6	6	7	8	F	A	B	C	D	E	3	G	H	9	K	L	J	1	2	0	4	5
7	7	8	9	A	B	C	D	E	F	G	H	J	K	L	0	1	2	3	4	5	6
8	8	9	A	B	C	D	E	F	G	H	J	K	L	0	1	2	3	4	5	6	7
9	9	A	B	0	D	E	3	G	H	J	K	L	F	1	2	6	4	5	C	7	8
A	A	B	C	D	E	F	G	H	J	K	L	0	1	2	3	4	5	6	7	8	9
B	B	C	D	E	F	G	H	J	K	L	0	1	2	3	4	5	6	7	8	9	A
C	C	D	E	J	G	H	9	K	L	F	1	2	3	4	5	0	7	8	6	A	B
D	D	E	F	G	H	J	K	L	0	1	2	3	4	5	6	7	8	9	A	B	C
E	E	F	G	H	J	K	L	0	1	2	3	4	5	6	7	8	9	A	B	C	D
F	F	G	H	C	K	L	J	1	2	6	4	5	0	7	8	9	A	B	3	D	E
G	G	H	J	K	L	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
H	H	J	K	L	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G
J	J	K	L	9	1	2	0	4	5	C	7	8	6	A	B	3	D	E	F	G	H
K	K	L	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J
L	L	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K

Figure 3.35. 21-element loop. ALT but not PA, LIP, RIP, Antiaut. ▲

*	0	1	2	3	4	5	6	7	8	9	A	B	C	D
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D
1	1	2	3	4	5	6	0	A	7	8	D	C	9	B
2	2	3	4	5	6	0	1	D	A	7	B	9	8	C
3	3	4	5	6	0	1	2	8	9	C	7	D	B	A
4	4	5	6	0	1	2	3	C	B	D	9	7	A	8
5	5	6	0	1	2	3	4	B	D	A	C	8	7	9
6	6	0	1	2	3	4	5	9	C	B	8	A	D	7
7	7	8	9	A	B	C	D	0	1	2	3	4	5	6
8	8	9	C	7	D	B	A	3	0	1	6	5	2	4
9	9	C	B	8	A	D	7	6	3	0	4	2	1	5
A	A	7	8	D	C	9	B	1	2	5	0	6	4	3
B	B	D	A	C	8	7	9	5	4	6	2	0	3	1
C	C	B	D	9	7	A	8	4	6	3	5	1	0	2
D	D	A	7	B	9	8	C	2	5	4	1	3	6	0

Figure 3.36. 14-element loop. PA, ALT, but not LIP, RIP, Antiaut.▲

*	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	0	7	6
2	2	3	0	1	7	6	4	5
3	3	5	4	6	1	7	0	2
4	4	6	7	2	0	1	5	3
5	5	0	6	7	3	2	1	4
6	6	7	5	0	2	4	3	1
7	7	4	1	5	6	3	2	0

Figure 3.37. 8-element loop. Antiaut, PA3, but not PA, LIP, RIP, LALT, RALT, FLEX.▲

*	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	0	5	6	3	7	4
2	2	0	1	4	7	6	3	5
3	3	4	5	0	2	7	1	6
4	4	7	6	1	0	2	5	3
5	5	6	3	7	1	0	4	2
6	6	3	7	2	5	4	0	1
7	7	5	4	6	3	1	2	0

Figure 3.38. 8-element loop. PA, Antiaut, but not LIP, RIP, LALT, RALT, FLEX.▲

*	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	5	6	7	8	4	9	0	1
3	3	6	4	5	9	7	8	0	1	2
4	4	7	6	8	0	9	2	1	3	5
5	5	4	8	7	1	0	9	3	2	6
6	6	5	7	9	8	1	0	2	4	3
7	7	8	9	0	2	3	1	5	6	4
8	8	9	0	1	6	2	3	4	5	7
9	9	0	1	2	3	4	5	6	7	8

Figure 3.39. 10-element loop. IP, PA3, but not PA, LALT, RALT, FLEX.▲

*	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	0	6	3	7	5	4
2	2	0	1	4	7	6	3	5
3	3	4	7	5	2	0	1	6
4	4	5	3	7	6	2	0	1
5	5	6	4	0	1	3	7	2
6	6	7	5	2	0	1	4	3
7	7	3	6	1	5	4	2	0

Figure 3.40. 8-element loop. PA, IP, but not LALT, RALT, FLEX.▲

Construction 3.41. LRA, Antiaut, but not PA, LIP, RIP, FLEX: Get a $(12 \cdot 21 = 252)$-element example by taking direct product of 3.34 with 3.35.

*	0	1	2	3	4	5	6	7	8	9	A	B
0	0	1	2	3	4	5	6	7	8	9	A	B
1	1	2	3	0	5	6	7	4	A	B	9	8
2	2	3	0	1	6	7	4	5	9	8	B	A
3	3	0	1	2	9	B	8	A	4	6	5	7
4	4	5	6	7	2	3	0	1	B	A	8	9
5	5	6	9	B	3	8	A	2	0	7	1	4
6	6	9	4	8	0	A	2	B	1	3	7	5
7	7	B	8	6	A	9	3	0	2	5	4	1
8	8	A	7	4	B	0	1	9	5	2	6	3
9	9	4	5	A	1	2	B	8	7	0	3	6
A	A	7	B	5	8	1	9	3	6	4	2	0
B	B	8	A	9	7	4	5	6	3	1	0	2

Figure 3.42. 12-element loop. PA, LRA, Antiaut, but not LIP, RIP, FLEX.▲

Construction 3.43. IPLR, but not PA, FLEX: Get a $(12 \cdot 18 = 216)$-element example by taking direct product of 3.44 with 3.49.

*	0	1	2	3	4	5	6	7	8	9	A	B
0	0	1	2	3	4	5	6	7	8	9	A	B
1	1	2	3	4	5	0	B	A	7	6	9	8
2	2	3	4	5	0	1	8	9	A	B	6	7
3	3	4	5	0	1	2	7	6	9	8	B	A
4	4	5	0	1	2	3	A	B	6	7	8	9
5	5	0	1	2	3	4	9	8	B	A	7	6
6	6	7	8	9	A	B	2	3	4	5	0	1
7	7	8	9	A	B	6	5	0	1	2	3	4
8	8	9	A	B	6	7	4	5	0	1	2	3
9	9	A	B	6	7	8	1	2	3	4	5	0
A	A	B	6	7	8	9	0	1	2	3	4	5
B	B	6	7	8	9	A	3	4	5	0	1	2

Figure 3.44. 12-element loop. PA, IPLR, but not LBOL, RBOL, FLEX.▲

*	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	0	5	4
2	2	3	4	5	0	1
3	3	0	5	4	1	2
4	4	5	0	1	2	3
5	5	4	1	2	3	0

Figure 3.45. 6-element loop. FLEX, Antiaut, but not PA, LIP, RIP, LALT, RALT.▲

*	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	0	3	4	5	2
2	2	3	0	5	1	4
3	3	4	5	0	2	1
4	4	5	1	2	0	3
5	5	2	4	1	3	0

Figure 3.46. 6-element loop. PA, FLEX, Antiaut, $xx = e$, but not LIP, RIP, LALT, RALT.▲

*	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	5	6	7	8	4	9	0	1
3	3	4	6	5	8	7	9	0	1	2
4	4	5	7	8	2	9	0	1	6	3
5	5	6	8	7	9	0	1	3	2	4
6	6	7	4	9	0	1	8	2	3	5
7	7	8	9	0	1	3	2	5	4	6
8	8	9	0	1	6	2	3	4	5	7
9	9	0	1	2	3	4	5	6	7	8

Figure 3.47. 10-element loop. IP, FLEX, but not PA, LALT, RALT.▲

*	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	0	5	3	6	4
2	2	0	1	4	6	3	5
3	3	4	5	6	2	1	0
4	4	6	3	1	5	0	2
5	5	3	6	2	0	4	1
6	6	5	4	0	1	2	3

Figure 3.48. 7-element loop. PA, IP, FLEX, but not LALT, RALT.▲

*	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K	L	M	N	P	Q	R	S
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K	L	M	N	P	Q	R	S
1	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K	L	M	N	P	Q	R	S	0
2	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K	L	M	N	P	Q	R	S	0	1
3	3	4	5	6	7	8	J̈	A	B	M̈	D	E	F	G	H	9̈	K	L	C̈	N	P	Q	R	S	0	1	2
4	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K	L	M	N	P	Q	R	S	0	1	2	3
5	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K	L	M	N	P	Q	R	S	0	1	2	3	4
6	6	7	8	J̈	A	B	C	D	E	Q̈	G	H	9̈	K	L	M	N	P	F̈	R	S	0	1	2	3	4	5
7	7	8	9	A	B	C	D	E	F	G	H	J	K	L	M	N	P	Q	R	S	0	1	2	3	4	5	6
8	8	9	A	B	C	D	E	F	G	H	J	K	L	M	N	P	Q	R	S	0	1	2	3	4	5	6	7
9	9	A	B	M̈	D	E	Q̈	G	H	J	K	L	3̈	N	P	6̈	R	S	0	1	2	C̈	4	5	F̈	7	8
A	A	B	C	D	E	F	G	H	J	K	L	M	N	P	Q	R	S	0	1	2	3	4	5	6	7	8	9
B	B	C	D	E	F	G	H	J	K	L	M	N	P	Q	R	S	0	1	2	3	4	5	6	7	8	9	A
C	C	D	E	F	G	H	9̈	K	L	3̈	N	P	Q	R	S	0	1	2	M̈	4	5	6	7	8	J̈	A	B
D	D	E	F	G	H	J	K	L	M	N	P	Q	R	S	0	1	2	3	4	5	6	7	8	9	A	B	C
E	E	F	G	H	J	K	L	M	N	P	Q	R	S	0	1	2	3	4	5	6	7	8	9	A	B	C	D
F	F	G	H	9̈	K	L	M	N	P	6̈	R	S	0	1	2	3	4	5	Q̈	7	8	J̈	A	B	C	D	E
G	G	H	J	K	L	M	N	P	Q	R	S	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
H	H	J	K	L	M	N	P	Q	R	S	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G
J	J	K	L	C̈	N	P	F̈	R	S	0	1	2	M̈	4	5	Q̈	7	8	9	A	B	3̈	D	E	6̈	G	H
K	K	L	M	N	P	Q	R	S	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J
L	L	M	N	P	Q	R	S	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K
M	M	N	P	Q	R	S	0	1	2	C̈	4	5	6	7	8	J̈	A	B	3̈	D	E	F	G	H	9̈	K	L
N	N	P	Q	R	S	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K	L	M
P	P	Q	R	S	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K	L	M	N
Q	Q	R	S	0	1	2	3	4	5	F̈	7	8	J̈	A	B	C	D	E	6̈	G	H	9̈	K	L	M	N	P
R	R	S	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K	L	M	N	P	Q
S	S	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K	L	M	N	P	Q	R

Figure 3.49. The unique (< 36)-element IPALT but not PA loop. (Not PA since `1+8=9≠J=3+6`). Entries $a * b$ not agreeing with integer addition $a + b$ mod 27 have been decorated with umlauts (`M̈` versus `M`). Note that these exceptions occur only on the index-3 subgrid and that the diagonal entries $a+a$, the first row and column $0 + a = a + 0$, and the antidiagonal $(-a) + a = 0$ never are umlauted. This loop has 27 elements and is commutative, Lalt, Ralt, Flexible, LIP, RIP, antiaut, but not power-associative, L-Bol, nor R-Bol. ▲

*	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H
1	1	2	3	4	5	0	F	H	E	C	G	D	7	9	A	8	6	B
2	2	3	4	5	0	1	8	B	A	7	6	9	H	C	G	E	F	D
3	3	4	5	0	1	2	E	D	H	G	F	C	B	7	6	A	9	8
4	4	5	0	1	2	3	A	9	6	B	8	7	D	H	F	G	E	C
5	5	0	1	2	3	4	G	C	F	D	E	H	9	B	8	6	A	7
6	6	D	8	C	A	H	7	0	B	4	9	2	F	G	5	3	1	E
7	7	G	B	F	9	E	0	6	2	A	4	8	3	1	H	C	D	5
8	8	C	A	G	6	D	B	2	9	0	7	4	E	F	1	5	H	3
9	9	E	7	H	B	F	4	A	0	8	2	6	1	5	C	D	3	G
A	A	H	6	D	8	C	9	4	7	2	B	0	G	E	3	1	5	F
B	B	F	9	E	7	G	2	8	4	6	0	A	5	3	D	H	C	1
C	C	A	H	6	D	8	5	G	1	E	3	F	2	0	7	9	B	4
D	D	8	C	A	H	6	3	E	5	F	1	G	0	4	9	B	7	2
E	E	7	G	B	F	9	D	3	C	1	H	5	A	8	2	0	4	6
F	F	9	E	7	G	B	H	1	D	5	C	3	8	6	0	4	2	A
G	G	B	F	8	E	7	C	5	3	H	D	1	6	A	4	2	0	9
H	H	6	D	9	C	A	1	F	G	3	5	E	4	2	B	7	8	0

Figure 3.50. 18-element loop. PA, IPALT, but not LBOL, RBOL, DIA.▲

*	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	0	3	2	7	9	8	4	6	5
2	2	3	0	1	9	8	7	6	5	4
3	3	2	1	0	8	7	9	5	4	6
4	4	7	9	8	0	6	5	1	3	2
5	5	9	8	7	6	0	4	3	2	1
6	6	8	7	9	5	4	0	2	1	3
7	7	4	6	5	1	3	2	0	9	8
8	8	6	5	4	3	2	1	9	0	7
9	9	5	4	6	2	1	3	8	7	0

Figure 3.51. Unique 10-element Steiner loop. DIA, Commutative, $xx = e$, but not LBOL, RBOL. The 12 Steiner triples are the rows, columns, and generalized diagonals of $\left(\begin{smallmatrix}123\\456\\789\end{smallmatrix}\right)$. ▲

*	0	1	2	3	4	5	6	7	8	9	A	B
0	0	1	2	3	4	5	6	7	8	9	A	B
1	1	2	0	5	3	4	8	6	7	B	9	A
2	2	0	1	4	5	3	7	8	6	A	B	9
3	3	4	5	0	1	2	9	B	A	6	8	7
4	4	5	3	2	0	1	B	A	9	8	7	6
5	5	3	4	1	2	0	A	9	B	7	6	8
6	6	7	8	9	B	A	0	1	2	3	5	4
7	7	8	6	B	A	9	2	0	1	5	4	3
8	8	6	7	A	9	B	1	2	0	4	3	5
9	9	A	B	6	8	7	3	5	4	0	1	2
A	A	B	9	8	7	6	5	4	3	2	0	1
B	B	9	A	7	6	8	4	3	5	1	2	0

Figure 3.52. Unique 12-element non-associative Moufang loop. ▲

*	0	1
0	0	1
1	1	0

Figure 3.53. The 2-element group. ▲

4 Do LRalt loops have 2-sided inverses?

The question of whether LRalt loops have 2-sided inverses sounds innocent. But it ushers us into a hurricane of complexity.

In §4.1 we shall see that there are countably-infinite LRalt loops without 2-sided inverses. However, there are no *continuum*-infinite analytically-smooth ones, since Sabanin [19] showed that analytic LRalt loops are diassociative.

In §4.2 we examine the evidence suggesting that inverses are always 2-sided in any finite LRalt loop.

In §4.5 we suggest that the LRalt⟹2SI problem may actually be among the hardest mathematical problems that are this simply posed.

4.1 A countably infinite LRalt loop without 2-sided inverses

All the elements of the loop may be defined in terms of 6 particular elements we call e, s, and G_0, G_1, G_2, G_3.

The loop will obey Lalt $xx \cdot y = x \cdot xy$, and Ralt $x \cdot yy = xy \cdot y$. The identity element is e so that $xe = ex = x$ for all x. The *s*pecial element s (which also may stand for either *s*ign or *s*wap) obeys

- $xs = sx$ (s commutes with everything);
- $s \cdot s = e$ (s is self-inverse; consequently $s^k = s$ or e if k is odd or even respectively);
- Hence as a consequence of Lalt, $ss \cdot x = s \cdot sx = s \cdot xs = x$, and as a consequence of Ralt, $x \cdot ss = xs \cdot s = sx \cdot s = x$ (thus multiplication by s is a self-inverse operation);
- if $xy = z$ then $sx \cdot sy = z$ and $sx \cdot y = x \cdot sy = sz$, (multiplication by s has interesting "pairing" effect; also s associates with everything);
- if $xy = 1$ and $zx = 1$ then either $y = z$ or $\{ys = sy = z$ and $zs = sz = y\}$ (if x has two unequal one-sided inverses, then s-multiplication interchanges them);
- either $xy = yx$ or $xy = yxs$ (near-commutativity).

G_0, G_1, G_2, G_3 obey

$$G_0 = sG_2 = G_2 s, \quad G_2 = sG_0 = G_0 s, \tag{1}$$

$$G_1 = sG_3 = G_3 s, \quad G_3 = sG_1 = G_1 s \tag{2}$$

and

$$G_a G_{a+1 \bmod 4} = e \tag{3}$$

so that each of them has two distinct 1-sided inverses.

The full set of elements of the loop are

$$\{G_0^n,\ G_1^m,\ G_2^n,\ G_3^m,\ sG_0^{2n},\ sG_1^{2n},\ e,\ s\}, \quad n, m \geq 1, \ m \text{ odd}. \tag{4}$$

The reason we said that m had to be odd was to prevent element-duplication, because $G_2^{2k} = G_0^{2k}$ and $G_1^{2k} = G_3^{2k}$ if $k \geq 0$. (Similarly, $G_0^m s = G_2^m$ and $G_1^m s = G_3^m$ if m is odd.)

The remaining effects of multiplying these elements by s are covered by the facts that s associates and commutes with everything and that

$$G_2^m = sG_0^m = G_0^m s, \quad G_0^m = sG_2^m = G_2^m s, \tag{5}$$

$$G_3^m = sG_1^m = G_1^m s, \quad G_1^m = sG_3^m = G_3^m s \tag{6}$$

for all *odd* $m \geq 1$.

The effects of multiplying G_a powers by each other are (where $n, m, j, k \geq 0$ always denote integers)

$$G_a^j G_a^k = G_a^{j+k}, \tag{7}$$

$$G_0^j G_2^k = G_2^k G_0^j = G_0^{j+k} s^k, \tag{8}$$

$$G_1^j G_3^k = G_3^k G_1^j = G_1^{j+k} s^k, \tag{9}$$

$$G_0^m G_1^n = \begin{cases} G_1^{n-m} & \text{if } m \leq n \\ G_0^{m-n} & \text{if } m \geq n \end{cases} \tag{10}$$

$$G_1^m G_0^n = \begin{cases} G_0^{n-m} s^m & \text{if } m \leq n \\ G_1^{m-n} s^n & \text{if } m \geq n \end{cases} \tag{11}$$

It is now a straightforward matter to see that both left- *and* right-division are uniquely defined, so that we indeed have a loop, and that Lalt and Ralt indeed are obeyed.

Power-associativity is obeyed. The *anti*automorphic inverse property $(x\backslash 1)(y\backslash 1) = (yx)\backslash 1$ is false in this loop. Indeed we do not have any antiautomorphism, nor does the loop obey LIP nor RIP, since any of these would have caused 2-sided inverses.

However, the following three maps all are automorphisms: $x \to 1/x$ (which maps $G_a \to G_{a-1 \bmod 4}$), $x \to x\backslash 1$ (which maps $G_a \to G_{a+1 \bmod 4}$) and $x \to 1/(1/x)$ (or $x \to (x\backslash 1)\backslash 1$, which in this loop happens to be the same map; note that this map is involutive) which swaps $G_a \leftrightarrow G_{a+2 \bmod 4}$.

Osborn's [15] weak inverse property $y((xy)\backslash 1) = x\backslash 1$ is obeyed in this loop; thus both WIP and the automorphic inverse property hold, which is often called the *crossed inverse property* CIP.

An *A-loop* is a loop whose inner mappings (i.e the identity-preserving permutations of the loop's elements induced by compositions of left- and/or right-multiplications) all are automorphisms. Our infinite loop is not an A-loop because its inner mapping $x \to xG_0 \cdot G_1$ is not an isomorphism.

4.2 Do finite LRalt loops have 2-sided inverses?

Exhaustive searches with `mace4`[7] show that every LRalt loop (indeed, every LRalt magma with \-division and $x1 = x$) with ≤ 185 elements has 2-sided inverses.

Define

$$X_\ell^n \stackrel{\text{def}}{=} \underbrace{X(X(X(X \ldots X)))}_{n \ X\text{'s in all}}, \tag{12}$$

i.e. X_ℓ^n denotes the result of starting with 1 and doing a *l*eft-multiplication by X repeatedly n times. (It was this leftward kind of exponentiation that was intended in the abstract.) We shall later also have use of X_r^n, which is defined similarly but using *r*ight-multiplication; and we shall use X^n without any subscript when we intentionally wish to leave its parenthesization ambiguous.

[7] It is necessary to modify the source code to permit loops with over 100 elements. `Mace4` reached 185 in only 1 day and then stopped because it ran out of memory.

Lemma 4 (Exponents of finite loops exist). *Let X be an element of a finite loop L. Then there exists a positive integer n, called its "left-exponent," such that $X_\ell^n = 1$. Further, there exists N (the "left-exponent of the loop") such that for all $U \in L$, $U_\ell^N = 1$.*

Proof: The repeated left-multiplication process must by finiteness ultimately repeat a value. Suppose the first repeat is $X_\ell^a = X_\ell^b$ with $0 \le a < b$. Then $X_\ell^a = XZ$ and $X_\ell^b = XY$ by the loop postulates imply $Y = Z$, which would represent an earlier repeat and thus a contradiction unless $a = 0$. Therefore we conclude that every $X \in L$ obeys $X_\ell^n = 1$ for *some* positive integer n (possibly depending on X) no greater than the cardinality of L. The exponent N of the loop is then the least common multiple of all of these n. □

Remark. We could also define right-exponents similarly. We also could take N to be the LCM of the left- and right-exponents of all the loop elements if we instead wanted to get a "two-sided exponent" for the loop.

Let us now discuss the nature of `otter`'s proofs for small n, and more generally, the question of what a proof that LRalt$\Longrightarrow$2SI in finite loops must be like (if it exists).

Consider some loop element X. Suppose for some integer $n \ge 1$ we have $X_\ell^n = 1$. In a finite loop such an n always exists. We then have $X \cdot X_\ell^{n-1} = 1$. The Lalt and Ralt properties imply that X has a two sided inverse if and only if they imply that $X_\ell^{n-1} X = 1$.

Lemma 5 (LRalt$\Longrightarrow$2SI if $n \le 6$). *Any element X in an LRalt magma obeys $X \cdot X_\ell^{n-1} = X_\ell^{n-1} \cdot X$, for each $n = 1, 2, 3, 4, 5, 6$.*

Proofs: (where $\underset{R}{=}$ means "= due to Ralt," etc.)

n=1,2: Trivially $X = X$ and $XX = XX$.

n=3: $1 = X \cdot XX \underset{R}{=} XX \cdot X$.

n=4: $1 = X(X \cdot XX) \underset{R}{=} XX \cdot XX \underset{L}{=} (XX \cdot X)X \underset{R}{=} (X \cdot XX)X$.

n=5: $1 = X(X[X \cdot XX]) \underset{L}{=} XX \cdot [X \cdot XX] \underset{R}{=} XX \cdot [XX \cdot X] \underset{L}{=} (XX \cdot XX)X \underset{L}{=} (X[X \cdot XX])X$.

n=6: $1 = X(X[X(X \cdot XX)]) \underset{L}{=} XX \cdot [X(X \cdot XX)] \underset{L}{=} XX \cdot [XX \cdot XX] \underset{L}{=} [XX \cdot XX] \cdot XX \underset{R}{=} [(XX \cdot X)X] \cdot XX \underset{R}{=} ([(XX \cdot X)X]X)X \underset{R}{=} [(XX \cdot X) \cdot XX]X \underset{R}{=} [(X \cdot XX) \cdot XX]X \underset{R}{=} [X(XX \cdot XX)]X \underset{L}{=} [X(X[X \cdot XX])]X$. □

Sketches of alternate proofs. It is also possible to prove something more general than the $n = 4$ case by showing the identity

$$(x \cdot xy)y = x(x \cdot yy) \tag{13}$$

and than the $n = 5$ case by showing

$$(x \cdot x(xx))y = x \cdot x(x \cdot xy). \tag{14}$$

The $n = 6$ case may be proven by showing the identities

$$(x \cdot yy)y \underset{R}{=} (xy \cdot y)y \underset{R}{=} xy \cdot yy, \tag{15}$$

$$xy \cdot (y \cdot y(yy)) = (x \cdot y(y \cdot yy))y \tag{16}$$

then letting $y = x$ in the latter and applying Lalt to its left hand side. (All 4 of these identities arise solely from the LRalt axioms.) □

One might now conjecture that "the pattern continues" in the sense that we somehow may always convert $X \cdot X_\ell^{n-1}$ into $X_\ell^{n-1} X$ by "playing with parentheses," i.e. by using the LRalt magma axioms only, without even requiring an identity element or a quasigroup. But that conjecture fails at the very next case $n = 7$.

Lemma 6 (Which loop axioms are needed?). *Any proof that LRalt$\Longrightarrow$2SI will require the following axioms that go beyond magmas: the loop axioms that 1 is a left-identity, and that at least one kind of division (x/y or $x \backslash y$) exists.*[8]

Proof: The proof consists of the counterexamples in figures 4.2 and 4.3. (We have also previously seen examples of loops with one-sided alternativity but without 2-sided inverses, so that both Ralt and Lalt are needed.)

We now point out that $ex = x$ (left-identity) in an LRalt magma with one-sided (/ only) division *implies* $xe = x$ (two-sided identity): we have $(y/x) \cdot xx = yx$ by Ralt, so that $(y/e)e = ye$ so that $y/e = y = ye$ by the definition of /. □

*	0	1	2	3	4
0	4	0	0	0	1
1	0	1	2	3	4
2	2	2	3	1	2
3	3	3	1	2	3
4	1	4	4	4	0

Figure 4.1. 5-element LRalt magma with 2-sided identity $e = 1$ and with 1-sided, but not 2-sided, division. Exhaustive search with `mace4` shows that any element X in any cardinality-n LRalt magma with identity and (≥ 1)-sided division *must* have a two sided inverse if $1 \le n \le 38$. ▲

*	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K	L
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K	L	0
1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K	L	0	1
2	3	4	5	D	7	8	G	A	B	C	6	E	F	9	H	J	K	L	0	1	2
3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K	L	0	1	2	3
4	5	D	7	8	9	A	J	C	6	E	F	G	H	B	K	L	0	1	2	3	4
5	D	7	8	9	A	B	K	6	E	F	G	H	J	C	L	0	1	2	3	4	5
6	E	F	9	H	B	C	D	0	1	G	3	J	K	L	7	8	2	A	4	5	6
7	8	9	A	B	C	D	E	F	G	H	J	K	L	0	1	2	3	4	5	6	7
8	9	A	B	C	D	E	F	G	H	J	K	L	0	1	2	3	4	5	6	7	8
9	A	B	C	6	E	F	2	H	J	K	L	0	1	G	3	4	5	D	7	8	9
A	B	C	D	E	F	G	H	J	K	L	0	1	2	3	4	5	6	7	8	9	A
B	C	6	E	F	G	H	4	K	L	0	1	2	3	J	5	D	7	8	9	A	B
C	6	E	F	G	H	J	5	L	0	1	2	3	4	K	D	7	8	9	A	B	C
D	7	8	G	A	J	K	L	E	F	2	H	4	5	6	0	1	9	3	B	C	D
E	F	G	H	J	K	L	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E
F	G	H	J	K	L	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
G	H	J	K	L	0	1	9	3	4	5	D	7	8	2	A	B	C	6	E	F	G
H	J	K	L	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H
J	K	L	0	1	2	3	B	5	D	7	8	9	A	4	C	6	E	F	G	H	J
K	L	0	1	2	3	4	C	D	7	8	9	A	B	5	6	E	F	G	H	J	K
L	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H	J	K	L

Figure 4.2. 21-element LRalt quasigroup in which $0 * 0_\ell^6 = 0 * 5 = 6 \ne D = 5 * 0 = 0_\ell^6 * 0$. This is in fact a *loop* with identity element `L`. ▲

[8]That is, among the usual loop axioms *alone*, we cannot omit the demand that at least one kind of division exists, and we cannot omit the demand that the quantity 1 such that $x^{-1}x = 1$ defines left-inverses, must in fact be a left-identity. However, we might, conceivably, be able to replace these "non-omittable" axioms with some other, less-usual, statement.

*	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	1
2	2	3	4	5	6	7	1	2
3	3	4	5	6	0	1	2	3
4	4	5	6	7	1	2	3	4
5	5	6	0	1	2	3	4	5
6	6	0	1	2	3	4	5	6
7	7	1	2	3	4	5	6	0

Figure 4.3. 8-element magma with identity $e = 0$ but without left- or right-division. Obeys LRalt but $3 * 3_\ell^6 = 3 * 4 = 0 \neq 7 = 4 * 3 = 3_\ell^6 * 3$ so 2SI is false. ▲

Nevertheless, the conjecture is true if $n = 2^k+1$ or $n = 2^k+2$:

Lemma 7 (LRalt$\Longrightarrow$2SI if $X_\ell^n = 1$ where $n - 2^k = 1, 2$). *If $n = 2^k + 1$ or $n = 2^k + 2$ then each element X in an LRalt magma obeys $XX_\ell^{n-1} = X_\ell^{n-1}X$.*

Proof: Consider the expression

$$X(X[X(X[X \cdots Xy])]) \tag{17}$$

where the number of X's is 2^k. By using Lalt in a top-down manner to pair up X's this becomes

$$= XX \cdot (XX \cdot [XX \cdot (XX \cdots [XX \cdot y])]). \tag{18}$$

Now by again using Lalt in a top-down manner to pair up XX's this becomes

$$= X_c^4 \cdot (X_c^4 \cdot [X_c^4 \cdot (X_c^4 \cdots [X_c^4 \cdot y])]) \tag{19}$$

where X_c^4 here denotes $XX \cdot XX$. Now by again using Lalt in a top-down manner to pair up X_c^4's to get X_c^8's, which here denotes $(XX \cdot XX)(XX \cdot XX)$, we get

$$= X_c^8 \cdot (X_c^8 \cdot [X_c^8 \cdot (X_c^8 \cdots [X_c^8 \cdot y])]) \tag{20}$$

and so on, until ultimately we have

$$= X_c^{(2^k)} \cdot y \tag{21}$$

where $X_c^{(2^k)}$ is $X^{(2^k)}$ parenthesized in the manner of a complete depth-k binary tree.

We now use the equality of EQs 17 and 21 in the cases $y = X$ and $y = 1$. The result is that $XX_\ell^{n-1} = X_\ell^{n-1}X$ if $n = 2^k+1$. To now consider $n = 2^k + 2$, let $y = XX$ and find that EQ 17 is just X_ℓ^n while EQ 21 is $X_c^{(2^k)} \cdot XX$. This by Ralt is $X_c^{(2^k)}X \cdot X$ and by the preceding result about $2^k + 1$ this is just $X_\ell^{n-1}X$. □

"Mirrorable" n: Define n to be *mirrorable* if $X_\ell^n = X_r^n$ in an LRalt loop, or magma, or whatever algebraic structure we are talking about at the moment of use.

Lemma 8. *If n is mirrorable in LRalt magmas, then so is $2n$.*

Proof: By making an Lalt pass, $X_\ell^{2n} = (XX)_\ell^n$ By assumption this is $(XX)_r^n$ which by an Ralt pass is X_r^{2n}. □

Consequently, by induction, powers of 2 are mirrorable. A more general statement is

Lemma 9. *If $n = 2^k + 2^j$, then n is mirrorable in LRalt magmas.*

Proof: When $n = 2^k+1$ lemma 7 shows that $X_\ell^n = X_\ell^{n-1}X$. But since $n - 1$ is a power of 2, lemma 9 shows this is $= X_r^{n-1}X = X_r^n$.

When $n = 2^k + 2$ lemma 7 shows that $X_\ell^n = X_\ell^{n-2} \cdot XX$. But since $n - 2$ is a power of 2, lemma 9 shows this is $= X_r^{n-2} \cdot XX \underset{R}{=} X_r^{n-2}X \cdot X = X_r^n$.

We may indeed use lemma 9 to double $2^{k-j} + 1$ repeatedly j times to get that 2^k+2^j is mirrorable for any j with $0 \le j \le k$. □

Lemma 10. *Let $n > 1$ be odd. A necessary condition that either $X \cdot X_\ell^{n-1} = X_\ell^{n-1}X$ or that n be mirrorable, in any LRalt magma, is that n divide some $2^k + 2^j$ with $0 \le j \le k$. For the former problem, it is necessary in addition that $0 \le j < k$ if $k \ge 2$. These conditions in general remain necessary even if the LRalt magma is known to have an identity element e and it is known that $X_\ell^n = e$.*

Proof: Since $n > 1$ is odd, for any $a, b > 0$ with $a + b = n$ we have, without loss of generality, $0 < a < b$. We here are asking that an expression of form X^aX^b be equal to an expression of form X^bX^a. Under Lalt and Ralt we can transform X^aX^b to $X^{2a}X^{b-a}$ and X^bX^a to $X^{b-a}X^{2a}$, but no other changes to (a, b) are possible. If the magma has an identity element e, we have the additional option of multiplying some subexpression by e (where there may be many forms of X^{kn} that are equivalent to e), or of recognizing that some subexpression is equivalent to e and therefore removing it. These operations change neither a nor b modulo n. We thus are asking that 1 be connected to -1 modulo n by a chain of doublings. For this to happen it is necessary that $2^k \equiv -2^j \bmod n$ for some $0 \le j \le k$, i.e. that n divide some number of the form $2^k + 2^j$. Finally, to see that $e = X_\ell^n = X_\ell^{n-1}X$ will not happen in general if $n = 2^k \ge 8$, note that we know that $X_\ell^n = X_r^n = X_r^{n-1}X$, so that if the magma supports cancellation we would have to have $X_r^{n-1} = X_\ell^{n-1}$. That, however, violates the very necessary condition we have just proven, if $n \ge 8$ is a power of 2, and indeed in figure 4.2 we gave a loop counterexample. □

The above lemmas show that the following n with $1 \le n \le 20$ are mirrorable: 1,2,3,4,5,6,8,9,10,12,16,18,20, while the following n are *not* mirrorable in general LRalt magmas: 7,15. Further, 7 is not even mirrorable in LRalt *loops* due to the 21-element counterexample in figure 4.2. `Mace4` also found explicit LRalt magmas with 1 in which 11,13, are not mirrorable. Nevertheless, I conjecture that 11 and 13 *are* mirrorable in magmas with *right-division* (exhaustive searches show that any counterexample must have > 185 elements) and indeed that:

Conjecture 11 (Mirrorability). *An integer $n > 0$ is mirrorable in an LRalt magma with right-division if n divides some number of the form $2^k + 2^j$ where $0 \le j \le k$.*

Lemma 12. *Let n be the least common multiple of the left- and right-exponents of an element X in an LRalt loop, i.e. let $n > 0$ be the least integer such that $X_\ell^n = X_r^n = 1$. (If the loop is finite, such an n always exists.) Let $g, j, k \ge 0$ and let $m = 2^j[2^k + 1] - gn > 0$. Then $X_\ell^m = X_r^m$.*

Proof: $2^j[2^k+1]$ is mirrorable by previous results, and then we may simply "chop off" g chunks of n X's from the products X_ℓ^n and X_r^n on the grounds that multiplying by 1 has no effect. □

Lemma 7 suffices to get quite far.

Lemma 13. *If $n > 0$ is any integer which divides some number of the form 2^k+2, then $1 = X \cdot X_\ell^{n-1}$ implies $1 = X_\ell^{n-1} \cdot X$ in an LRalt magma with identity.*

In particular, this criterion includes

1. *All primes not congruent to* 7 mod 8 *(but primes congruent to* 7 mod 8 *are excluded),*
2. *All n which factor into primes congruent to* 3 mod 8 *(for example $n = 99 = 3 \cdot 3 \cdot 11$),*
3. *Among the n with $2 \le n \le 20$, precisely the following:* $2, 3, 5, 6, 9, 10, 11, 13, 17, 18, 19$.

Proof: Because $X_\ell^n = 1$ implies that $X_\ell^{kn} = 1$ we have that $X_\ell^{kn-1} = X_\ell^{n-1}$ so that it suffices to prove $X_\ell^{kn-1}X = 1$. In other words, "if it works for some multiple kn of n, then it works for n." We now sketch the proofs of the specific cases:

1. We have already dealt with $p = 2$. So let p be an odd prime. Then it follows from Gauss's quadratic reciprocity theorem that some power of 2 is congruent to -1 mod p, i.e. p divides $2^k + 1$ for some k, if and only if p is not congruent to 7 mod 8.
2. If n factorizes into primes congruent to 3 mod 8, then some power of 2 is congruent to -1 mod n because 2^k will do where k is the least common multiple of the individual k's; note this will always be an *odd* multiple of each.
3. $2^6 + 2 = 66 = 2 \cdot 3 \cdot 11$, $2^7 + 2 = 130 = 2 \cdot 5 \cdot 13$, $2^{10}+2 = 2 \cdot 9 \cdot 19$, $2^{13}+2 = 2 \cdot 17 \cdot 241$. But 7 and hence 14 are excluded by claim#1; 8, 12, 16, and 20 obviously cannot divide any 2^k+2; finally 15 does not divide any $2^k + 1$ because $3|(2^k + 1)$ only when k is odd, whereas $5|(2^k + 1)$ only when $k \equiv 2$ mod 4.

□

The criterion of lemma 13 admits a fairly large set of integers n. The number of primes not congruent to 7 mod 8 below x is asymptotic to $0.75x/\ln x$. The set of n with $1 < n < x$ which factor into primes congruent to 3 mod 8 is asymptotic to $Cx(\ln x)^{-0.75}$ for some positive constant C.

However, figure 4.3 makes it clear that arguments such as these, which only employ the axioms of a magma with 1, ultimately cannot suffice; quasigroup axioms (the existence of division) must play a role even when $n = 7$.

With the aid of `otter`, I was able to prove that any X obeying $X_\ell^n = 1$ in an LRalt loop has a 2-sided inverse, for each n with $1 \le n \le 20$ with the possible exception of 15. More precisely, of the cases $n = 7, 8, 12, 14, 16, 20$ not already covered by preceding results: we shall soon describe the proof for $n = 7$, and the cases $8, 12, 16, 20$ all were proven by `otter` from the left-identity $1x = x$ and LRalt magma axioms *alone*, with no quasigroup axioms being needed. That suggests

Conjecture 14. *If n divides some number of the form $2^k + 2^j$ where $0 \le j < k$, then each element X in an LRalt magma with left-identity obeying $XX_\ell^{n-1} = e$ necessarily obeys $X_\ell^{n-1}X = e$.*

(Incidentally, it is not hard to prove that the sets of numbers obeying the conditions in conjectures 11 and 14, while infinite, contain arbitrarily large "gaps.")

Finally, neither `otter` nor I were able to handle $n = 14, 15$, directly, although 14 eventually succumbed to an indirect attack. Specifically, we shall provide proofs for 14 and 15 *under the assumption* of conjecture 11. Later `otter` was able to settle that conjecture in 13-case, providing a proof for $n = 14$.

Unfortunately, `otter`'s proofs get more and more complicated with increasing n and lack any recognizable pattern.

`Otter` produced a spectacularly complicated 88-step proof for the case $n = 7$. `Otter` is a computerized deduction engine by W.McCune. One may input axioms to it (e.g. the LRalt and loop axioms) and ask to to prove some desired conclusion (e.g. that $1/x = x\backslash 1$). In some cases, `otter` will succeed in finding a proof; in others it will run out of time or memory. Sometimes `otter` can be far inferior to a human mathematician. Other times – favorable circumstances are when there are few axioms and little human-exploitable "structure" – `otter` seems to achieve vastly superhuman deductive power. This is one of them: `otter` found its proof for the case $n = 7$ in 17 seconds, and similar proofs for all cases we've mentioned combined in under 10 minutes. I do not believe any human can match that performance[9]. Indeed, *this* human was unable even to fully *understand* `otter`'s $n = 7$ proof. Even *single* deductive steps in an `otter` proof can be quite nontrivial, e.g. "paramodulations" with many parameters. For example, according to `otter`'s notion of a "single step," settling the case $n = 6$ (as we did above) requires only 2 steps! Thus really, `otter`'s "88-step" proof perhaps would be more properly regarded as a 200-300 step proof.

Nevertheless, the honor of humanity ultimately partially reasserted itself when I produced the following much simpler $n = 7$ proof. It comes quite easily once one adopts the goal of incorporating both the identity element 1, and cancellation, into the proof, in the simplest possible manner.

n=7: To prove $1 = z_\ell^7$ implies $z_\ell^6 z = 1$ in an LRalt loop, we begin by multiplying both sides of the former equation by z on the left to get $z = z_\ell^8$. By the equality of EQs 17 and 21 when $y = 1$ and $k = 3$, it follows that z_ℓ^8 is equal to its mirror, so that $z = ([(zz)z \cdot z]z \cdot z)z \cdot z$. Now cancel z's to get $1 = ([(zz)z \cdot z]z \cdot z)z$, i.e. we have proven $z_\ell^7 = z_r^7$ if $1 = z_\ell^7$. This reduces our task to proving that $z_\ell^6 = z_r^6$, i.e. proving that 6 is mirrorable – but we already know that from lemma 9. □

n=8: We provide an extremely sparse sketch of `otter`'s spectacularly complicated 40-step proof[10] that $A_\ell^8 = 1$ implies $A_\ell^7 A = 1$ in an LRalt magma with left-identity 1 (i.e. $1x = x$ for all x).

[9] A famous case was the solution of the open "Robbins problem" by McCune's other deduction engine EQP [13], which on contemporary computers would take about 1 day. I defy any human to solve the Robbins problem in anywhere near 1 day.

[10] Although `otter`'s proof definitely may be simplified if we allow ourselves additional loop axioms, I have been unable to produce a truly simple proof, nor have I been able to simplify it at all in the absence of additional axioms.

First otter derived the following 5 identities from the LRalt axioms alone:

$$[x \cdot y(y \cdot yy)]y = xy \cdot [y(y \cdot yy)] \tag{22}$$

$$[(x \cdot xy)(x[x \cdot yy])]y = (x \cdot xy)[(x \cdot xy) \cdot yy] \tag{23}$$

$$[xy \cdot (x \cdot yy)]y = xy \cdot [xy \cdot yy] \tag{24}$$

$$[x \cdot x(x \cdot xy)]y = x \cdot x[x(x \cdot yy)] \tag{25}$$

$$x_\ell^3 x_\ell^5 = x_\ell^8. \tag{26}$$

Various facts are true about A which are not true for general x. For example, $A \cdot 1 = A$, even though we had only assumed 1 was a *left* identity. This arises from the identity $x \cdot x(x \cdot x[x \cdot x(x \cdot xy)]) = x_\ell^8 y$ (which is a special case of the proof of lemma 7) by using $y = x = A$ to get $A_\ell^9 = A_\ell^8 A$ and then recognizing the left hand side as $A \cdot 1$ and the right as $1 \cdot A = A$.

Note that we derived $A1 = A$ by starting with some generally true identity applied to A, left-multiplying various subexpressions by some form of $1 = A^8$, rearranging parentheses, and then recognizing certain other subexpressions as forms of 1 and hence removing them. Otter used this same strategy (but in more complicated ways) to find $A_\ell^3 A_\ell^3 = A_\ell^6$, $A_\ell^4 A_\ell^3 = A_\ell^7$, $A_\ell^6 A_\ell^6 = A_\ell^4$, $A_\ell^5 A_\ell^6 = A_\ell^3$, $A_\ell^3 A_\ell^6 \cdot A_\ell^3 A_\ell^4 = 1$, $A_\ell^3 A_\ell^6 = A$, $A_\ell^3 A_\ell^4 = A_\ell^7$, and the goal of the proof, namely $A_\ell^7 A = A_\ell^8 = 1$ (as well as many other, less simply expressible, claims). All of these are true for A but are unobtainable (in LRalt magmas with left-identity) for general x.

The finale of otter's proof is as follows. It manages to obtain $A_\ell^3 A_\ell^6 \cdot A_\ell^3 A_\ell^4 = 1$. It then uses this fact (among others) to derive $A_\ell^3 A_\ell^4 = A_\ell^7$. From this we know $(A_\ell^3 A_\ell^4)A = A_\ell^7 A$. Now applying EQ 23 with $x = y = A$ to the left hand side gives $A_\ell^8 = A_\ell^7 A$ and upon recognizing the left hand side as 1 we have proven the theorem. □

n=14: To prove $X_\ell^{14} = 1$ implies $X_\ell^{13} X = 1$ in an LRalt loop *in which 13 is mirrorable*: Left-multiply by XX and employ Lalt to get $X_\ell^{16} = 1$. Now by repeated uses of Lalt to pair X's into XX's, then into X_c^4's, and so on we have $X_\ell^{16} = (XX)_\ell^8 = (X_c^4)_\ell^4 = (X_c^8)^2 = X_c^{16}$ so that now by a mirror argument $X_\ell^{16} = X_c^{16} = X_r^{16} = X_r^{14} X \cdot X \underset{R}{=} X_r^{14} \cdot XX$. Now since $X_\ell^{14} = 1$ we have that $XX = X_r^{14} \cdot XX$ so that by cancelling the XX we get $X_r^{14} = 1$. This is $X_r^{13} X = 1$. Now if 13 is mirrorable, then $X_r^{13} = X_\ell^{13}$ and we are done. □

Remark. M.K.Kinyon (private communication) was able to get otter to prove 11 and 13 mirrorable in loops. That completes the $n = 14$ proof above.

n=15: To prove $X_\ell^{15} = 1$ implies $X_\ell^{14} X = 1$ in an LRalt loop *in which 29 is mirrorable*: It suffices to prove $X_\ell^{29} X = 1$. Left-multiply by XX and employ Lalt to get $X_\ell^{32} = 1$. Now by repeated used of Lalt to pair X's into XX's, then into X_c^4's, and so on we get (similarly to in the previous proof) $X_\ell^{32} = X_c^{32} = X_r^{32} = X_r^{30} X \cdot X \underset{R}{=} X_r^{30} \cdot XX$. Now since $X_\ell^{30} = 1$ we have that $XX = X_r^{30} \cdot XX$ so that by cancelling the XX we get $X_r^{30} = 1$. This is $X_r^{29} X = 1$. If 29 is mirrorable then $X_r^{29} = X_\ell^{29}$ and we are done. □

It probably would be possible to establish fully rigorously the fact that elements X with left-exponent n in an LRalt loop have 2-sided inverses for both $n = 14$ and 15, by: writing a special purpose computer program based on standard graph-connectivity algorithms and the graph-reformulation of the problem in §4.3. If so, then the next open case would be $n = 21$.

4.3 The graph picture

Let G_n be the graph whose vertices consist of the ordered rooted binary trees with n leaves. Each such tree represents a way to parenthesize X^n. The edges of G_n join two trees which are equivalent by an Lalt or Ralt re-parenthesization. The question of whether an element X in an LRalt magma obeys $X_\ell^{n-1} X = X_\ell^n$, is then equivalent to the question of whether these two particular vertices of G_n lie in the same connected component. This view enables proving certain statements easily, which otherwise might have been difficult. For example

Lemma 15 (Unboundedly large proof lengths). *The graphical distance (number of edges in the shortest path between) these two vertices is at least $n - 2$.*

Proof: Each n-leafed ordered roted binary tree may be regarded as the planar dual of a triangulation by diagonals of a convex $(n+1)$-gon with one distinguished "root edge" AB. Each associative transformation corresponds to erasing a diagonal and then retriangulating the resulting quadrilateral-shaped hole using the other diagonal (and LRalt transformations are a subset of associative transformations). Originally all the $n - 2$ diagonals have endpoint A but none have endpoint B, but in the final state, the opposite is true, so at least $n - 2$ transformations have to be made. □

Now define the graph G'_n, which has an infinite number of vertices, as follows. Its vertices correspond to the ordered rooted binary trees with kn leaves for all $k = 1, 2, 3, \ldots$. In addition to the LRalt edges we mentioned before, there are also edges linking kn-leaf trees to $(k+1)n$-leaf trees, corresponding to multiplying some subexpression on the left or right by $X_e ll^n = 1$. The question of whether an element X in an LRalt magma with 2-sided identity 1 has a 2-sided inverse, given that $X_\ell^n = 1$, is then equivalent to the question of whether two particular vertices of G'_n lie in the same connected component.

Finally, define the graph G''_n. It too has an infinite number of vertices. Now they correspond to the *unordered pairs* of ordered rooted binary trees with finite numbers of leaves. In addition to the LRalt and 1-multiplication edges we mentioned before (now operating independently on each member of the pair; so far $G''_n = G'_n \times G'_n$ but we shall now adjoin an infinite number of additional edges), there are also edges linking pairs of trees to pairs of trees each with K extra leaves, corresponding to multiplying both entire expressions by some common K-term expression on the left or right, i.e. (in the latter case) to adjoining new roots to both trees in the pair, whose two left children are the two old trees, and whose two right children are two copies of the same new K-leaf tree. The question of whether an element X in an LRloop has a 2-sided inverse, given that $X_\ell^n = 1$, is then equivalent to the question of whether the two particular vertices of G''_n representing $\{X_\ell^n, 1\}$ and $\{X_\ell^{n-1} X, 1\}$ lie in the same connected component.

Connectivity questions about infinite graphs or directed graphs are notoriously difficult, the "$3x+1$ problem" [8] being a simple prototypical unsolved example.

4.4 Possible 87% solution?

The situation so far is: The LRalt$\Longrightarrow$2SI problem remains unsolved in finite loops. Even for the (apparently simpler) problem in magmas with left-identity, or magmas with right-division, we have been unable to completely settle the questions of which n cause $X_\ell^n = X_r^n$ and which n cause $X_\ell^n = 1$ to imply $X_\ell^{n-1}X = 1$. But we have made some progress by finding some necessary, and some sufficient conditions.

We now sketch a plan of argument which may enable an "87.5% solution." A conjecture essentially the same as the standard conjecture that there are an infinite number of twin primes $(p, p+2)$ is

Conjecture 16 (Modified twin-primes). *Given an odd number n, there are an infinite set of numbers k such that $4kn+1$ and $4kn-1$ both are prime.*

Theorem 17. *Let $n > 0$ be an integer not divisible by 8. Under the assumption of conjectures 11 and 16: in an LRalt magma with identity 1 and with right-division, $X^n = 1$ implies that X has a 2-sided inverse.*

Proof: Let n not be divisible by 8. Find k so $kn \pm 1$ both are prime, and $kn \equiv 4 \bmod 8$. Then observe that by conjecture 11 and some easy number theory, that $kn\pm1$ both are mirrorable. Left-multiply X_ℓ^{kn} by X to get $X_\ell^{kn+1} = X_r^{kn+1} = X$. Right-cancel the X's to get $X_r^{kn} = 1 = X_r^{kn-1}X$. Now mirror to get $= X_\ell^{kn-1}X = 1 = X_\ell^{n-1}X$.

This would totally settle the LRalt$\Longrightarrow$2SI problem except for those n that are multiples of 8 (i.e. $7/8 = 0.875$ of all n). Further, some of the multiples of 8 could be handled by conjecture 14; the first open case would be $n = 56$. □

This proof-plan, of course, still would only provide "87% of a solution," and cannot be implemented at least until the 3000-year-open twin-primes problem is settled! In that case, theorem 17 merely would serve to reduce the problem to proving conjectures 14 and especially 11. Still, that reduction arguably is progress since these conjectures concern LRalt magmas with left-identity and right-division, respectively (i.e. not both at the same time) – more simply defined objects than LRalt loops.

4.5 Candidate for the most frustrating problem in the world?

Connoisseurs of frustration prefer their problems to be simple to state, mathematically natural, and difficult to solve. According to these criteria, the LRalt$\Longrightarrow$2SI problem is a surprising contender for the world's top problem!

The LRalt$\Longrightarrow$2SI problem has an extremely simple statement:

Given that, in a finite universe,

$$1 * x = x; \qquad (x/y) * y = x; \tag{27}$$

$$x*(y*y) = (x*y)*y; \quad (y*y)*x = y*(y*x); \tag{28}$$

does it then follow that $x * (1/x) = 1$?

For the purpose of comparison, consider these 8 problems:

1. What is the maximum number of faces of a convex polyhedral space-tiler?
2. Does white always win a perfectly played chess game?
3. Are there an infinite number of primes of the form $n^2 + 1$?
4. The "$3x+1$ problem" [8] of whether the iteration on the positive integers $x \to 3x+1$ if x is odd, $x \to x/2$ if x is even, will always reach the value $x = 1$, no matter what the starting point.
5. Does P=NP? [6]
6. Are all planar graphs 4-colorable? [17]
7. Classify all finite simple groups. [3]
8. Do there exist integers $a, b, c > 0$ and $n > 2$ with $a^n + b^n = c^n$? [22]

All are mathematically natural with the possible exception of the $3x + 1$ problem.

The first 5 problems (with the possible exception of the first, which has not been worked on as hard as the others) seem well beyond reach, whereas problems 6-8 have (with immense effort) been solved, albeit the solutions of 6 and 7 seem sufficiently long that it is almost beyond the ability of any single human to check them.

Although all of these problems may seem simple to state, one gets a more precise perspective on the "simplicity" of a problem statement after gaining some experience inputting problems to computerized proof- and counterexample-finding tools such as `otter` and `mace`. If one is only allowed to employ first order logic and must describe the problems to a completely naive listener, i.e. such a computerized system, then the descriptions of each of these 8 problems are longer – usually much longer – than ours. (Just getting started by defining notions such as "integers," "primes," "space-tiling," "convex polyhedron," "planar graphs," "classification of simple groups," "P," "NP," or the rules of chess already takes too long.) Probably the simplest 3 to state among our 8 are the $3x + 1$ problem, the classification of simple groups, and Fermat's last theorem, but neither is as simple as ours.

It is notoriously hard to estimate the difficulty of open problems, and especially so in the case of LRalt$\Longrightarrow$2SI since M.K.Kinyon[11] and I are the only people who have tried hard on it. But let us say this.

1. The $(n^2 + 1)$-primes and twin-primes problems have been open for thousands of years, which makes them harder than the last three (solved) problems. We've seen reasons to suspect the LRalt$\Longrightarrow$2SI problem may be at least equally hard as them and the $3x + 1$ problem.

2. Everybody is confident they already know the answers to problems 3,4,5 but merely cannot prove it; and it is trivial to investigate 3,4, and 8 up into the billions by computer. In contrast, computer investigation of LRalt$\Longrightarrow$2SI is much harder and I feel considerably less confidence I know its answer.

3. Solving chess is a "trivial" problem in that it may be solved purely mechanically by a finite case analysis using only first order logic. But (we have shown in §4.1) no such solution is

[11] See §5.

possible for LRalt$\underset{F}{\Longrightarrow}$2SI (at least, if the answer, as expected, is positive).

Should the joys of LRalt$\Longrightarrow$2SI pall, the reader is reminded that there are 5 more problems of the same ilk listed in table 1.1. All of them are only slightly harder to state and they may be even harder to solve.

5 Acknowledgements and updates

J.D.Phillips found a few of the loop examples in §3, or closely related loops, before I did, and also did some work on the LRalt$\Longrightarrow$2SI problem, which I had dropped on him rather like a bomb. We both initially thought that problem was going to be *far* easier than it now seems. It was he who initially suggested the conjecture that its solution depends on the finiteness of the loop; all my investigations so far support that.

P.Vojtechovsky spotted a typo which caused the appearance of a serious error. (It has been corrected.)

It should be obvious that I have made heavy use of `mace4` [10] and `otter` [11]. My own programs `loop-beaut.c` and `setinc.c`, are available on my website `http://math.temple.edu/~wds/homepage/works.html`. The use of all 4 of these programs (albeit `setinc.c` would have to be appropriately modified) should enable future investigations of the same sort to proceed in a highly automated way.

Updates: M.K.Kinyon and I (with computer aid) have examined the LRalt$\Longrightarrow$2SI problem further since this paper was written and conceivably a followup paper by one or both of us may appear. In particular Kinyon showed that X must have a 2-sided inverse in an LRalt loop if $X^n = 1$ with $n \le 31$ and $n = 63$ and I showed this is true in an LRalt magma with 2-sided identity if n divides any number of the form $2^k + 2$.

Kinyon suggests that a possibly-productive line of attack on the LRalt$\Longrightarrow$2SI problem would be to prove in an LRalt magma with $1x = x1 = x$, that $A_\ell^n = 1$ implies these two equations hold: $A_\ell^{n-1}A^2 = A$, $A_\ell^{n-1}(A_\ell^{n-1}A) = A_\ell^{n-1}$. If the magma has right or left cancellation (respectively), then these respectively would suffice to imply 2SI. Kinyon also suggests investigating $A_\ell^{n-1}A_\ell^{n-1} = A_\ell^{n-2}$ and $(A_\ell^{n-1})_\ell^{n-1} = A$.

References

[1] G.Bol: Gewebe und Gruppen, Math. Annalen 114 (1937) 414-437.

[2] Richard Hubert Bruck: A survey of binary systems, Springer-Verlag 1958, third corrected printing 1971 (Ergebnisse der Math. #20).

[3] J.H.Conway, R.T.Curtis, S.P.Norton, R.A.Parker, R.A.Wilson: ATLAS of Finite Groups, now reprinted with corrections and additions Oxford Univ. Press, November 2003.

[4] Vilnis Detlovs & Karlis Podnieks: Introduction to Mathematical Logic, electronically available textbook at University of Latvia, `http://www.ltn.lv/~podnieks/mlog/ml.htm`. Chapter 4 covers completeness theorems.

[5] Herbert B. Enderton: A mathematical introduction to logic, Academic Press 1972.

[6] M.R. Garey & D.S. Johnson: Computers and Intractability, W.H.Freeman and Company, San Francisco, 1979.

[7] Kurt Gödel: Die Vollständigkeit der Axiome des logischen Funktionen-kalküls, Monatsh. für Mathematik und Physik 37 (1930) 349-360.

[8] Jeffrey C. Lagarias: The 3x+1 problem and its generalizations, Amer. Math. Monthly 92 (1985) 3-23.

[9] W.McCune: Son of Bird Brain (automated deduction system demonstration web page), `http://www-unix.mcs.anl.gov/AR/sobb/`.

[10] William W. McCune: Mace 2.0 reference manual and guide, `cs.SC/0106042`

[11] William W. McCune: Otter 3.3 reference manual, `cs.SC/0310056`

[12] W. McCune & R. Padmanabhan: Automated Deduction in Equational Logic and Cubic Curves, Springer-Verlag (LNCS [AI subseries] #1095) 1996.

[13] W. McCune: Solution of the Robbins Problem, J.Automated Reasoning 19,3 (1997) 263-276 and `http://www-unix.mcs.anl.gov/~mccune/papers/robbins/`.

[14] Elliot Mendelson: Introduction to mathematical logic, Lewis Publishers Inc. 4th ed. 1997.

[15] J.Marshall Osborn: Loops with the weak inverse property, Pacific J. Math. 10 (1960) 295-304.

[16] J. D. Phillips and Petr Vojtechovsky C-loops: An Introduction, M04/03 at `http://www.math.du.edu/preprints.html`.

[17] N.Robertson, D.P.Sanders, P.D.Seymour, R.Thomas: The four colour theorem, J. Combin. Theory B 70 (1997) 2-44.

[18] D.A.Robinson: Bol loops, Trans.Amer.Math.Society 123 (1966) 341-354.

[19] L.V.Sabanin: On the diassociativity of smooth monoalternative maps, Russian Math. Surveys 51 (1996) 747-749.

[20] Warren D. Smith: Loop diassociativity has no finite basis, available at `http://math.temple.edu/~wds/homepage/works.html`.

[21] Warren D. Smith: Quaternions, octonions, and now, 16-ons and 2^n-ons; New kinds of numbers. Book, under review for publication.

[22] Andrew Wiles; Modular elliptic curves and Fermat's Last Theorem, Annals of Mathematics 141 (1995) 443-551.