Using Prover9/Mace4 to understand Jordan Loops

Kyle Pula

June 22nd, 2007
A *loop* is a set with binary operation $\cdot$ and constant $e$ such that both

$$x \cdot y = z$$
$$y \cdot x = z$$

have unique solutions $y$ for all pairs $(x, z)$ and

$$x \cdot e = e \cdot x = x$$

A *Jordan loop* is a commutative loop satisfying

$$x^2 y \cdot x = x^2 \cdot yx$$ (1)
For what finite orders do there exist non-associative Jordan loops? Mace9 finds the following:

- None of order less than 6.
- Finds models for orders 6-8 and 10-16.
- Shows that no model of order 9 exists.
- Cannot find a model of order 17 in a “reasonable” amount of time (several days, maybe weeks) using a naive search.
We found constructions giving models of order $n$ for all $n \geq 6$, $n \neq 2^k + 1$, and $n \neq 9$ and prime. The unresolved orders were exactly the Fermat primes greater than 5:

\[
\begin{align*}
2^4 + 1 &= 17 \\
2^8 + 1 &= 257 \\
2^{16} + 1 &= 65537
\end{align*}
\]

Note: It is not known whether an infinite number of Fermat primes exist. These are the only known examples.
Clearly on the verge of solving a famous number theory problem, we had several options:

1. Find a construction for the Fermat prime orders.
2. Understand why no models of order 9 exist and use this knowledge to prove none exist for the Fermat prime orders.
Lemma

A Jordan loop of order 17 is either monogenic or power-associative.

If it is power-associative, then it’s main diagonal consists of copies of $\mathbb{Z}_3$, $\mathbb{Z}_5$, and $\mathbb{Z}_7$.

Feeding this information into Mace4 allows it to find a model of order 17 having copies of $\mathbb{Z}_5$ along the diagonal in a few minutes.

This model leads to a general construction resolving all open cases.
Existence Question Resolved

Theorem

A non-associative Jordan loop of order $n$ exists iff $n \geq 6$ and $n \neq 9$.

Question

Why must a Jordan loop of order 9 be associative?
Existence Question Resolved

Theorem

A non-associative Jordan loop of order $n$ exists iff $n \geq 6$ and $n \neq 9$.

Question

Why must a Jordan loop of order 9 be associative?
Lemma

A Jordan loop of order 9 is either monogenic or of exponent 3.

Lemma

If $\langle x \rangle = L$ is a Jordan loop of order $n$ and $x^k$ is well-defined for $1 \leq k < n$, then $L$ is a cyclic group.
Questions

What powers are well-defined in Jordan loops?

Lemma

\( x^k \) is well-defined for \( 1 \leq k \leq 5 \).

If \( x^6 \) is well-defined, then \( x^7 \) is well-defined. (easy)

If \( x^6 \) is well-defined, then \( x^8 \) is well-defined. (tricky - Prover9)

Mace4 was able to construct a model with an element \( x \) such that \( x^6 \) is well-defined but \( x^9 \) is not.
Corollary

If \( \langle x \rangle = L \) is a Jordan loop of order 9 and \( x^6 \) is well-defined, then \( L \cong \mathbb{Z}_9 \).