# Symmetries for Cube-and-conquer in Finite Model Finding

João Araújo Choiwah Chow *Mikoláš Janota*

Universidade Nova de Lisboa, Lisbon, Portugal
Universidade Aberta, Lisbon, Portugal
Czech Technical University in Prague

27 August 2023, Toronto, CP 2023

# First Order Logic for Algebra

- First Order Logic:
  a language to represent classes of algebras
- **Example:** Semigroups

$$(\forall xyz)((x * y) * z = x * (y * z))$$

- but also more complicated expressions:

$$(\exists xy)(x * y \neq y * x)$$
$$(\forall xz)((x * r(x)) * z = z)$$

# Finiteness and Orders

**Example:** Binary operation $*$
on domain $\{0, 1\}$
(a semigroup of order 2):

| $*$ | **0** | **1** |
|---|---|---|
| **0** | 0 | 1 |
| **1** | 1 | 0 |

Some FOL formulas only have infinite models

$$(\forall xy)(g(x) = g(y) \Rightarrow x = y)$$
$$(\exists x \forall y)(g(y) \neq x)$$

# The Task

**Given:** A FOL $\phi$
**Given:** Fixed order $n \in \mathbb{N}^+$
**Calculate:**
An algebra of order $n$ satisfying $\phi$
*Or* **Calculate:**
All non-isomorphic algebras of order $n$ satisfying $\phi$

# Isomorphism

Operations $*$ and $\diamond$ are isomorphic
iff there is a bijection $f$, s.t.

$$f(x * y) = f(x) \diamond f(y)$$

equivalently: $x * y = f^{-1}(f(x) \diamond f(y))$

## Example

$$f(x) = 1 - x$$

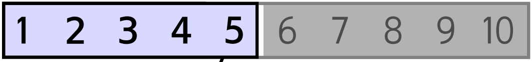
| $\vee$ | **0** | **1** |
|---|---|---|
| **0** | 0 | 1 |
| **1** | 1 | 1 |

| $\wedge$ | **0** | **1** |
|---|---|---|
| **0** | 0 | 0 |
| **1** | 0 | 1 |

# Searching for Finite Models

- Convert to SAT/CP (Paradox)
- **Dedicated solver** (**Mace4**)
  - Skolemize
  - Ground
  - Backtracking + propagation
  - Symmetries? — Least Number Heuristic
- Dedicated solvers especially good for enumerating all solutions

# The Least Number Heuristic (LNH)

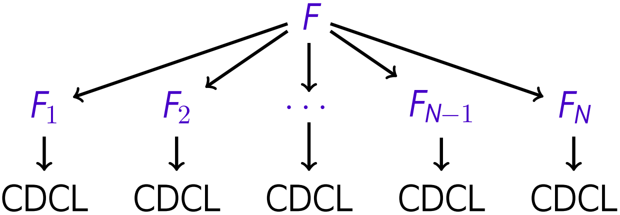



| * | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| **1** | 1 | 2 | 2 | ? | ? | ? | ? | ? | ? | ? |
| **2** | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |
| **...** | ? | ? | ? | ? | ? | ? | ? | ? | ? | ? |

# Isomorphism Inherent Issue in Search

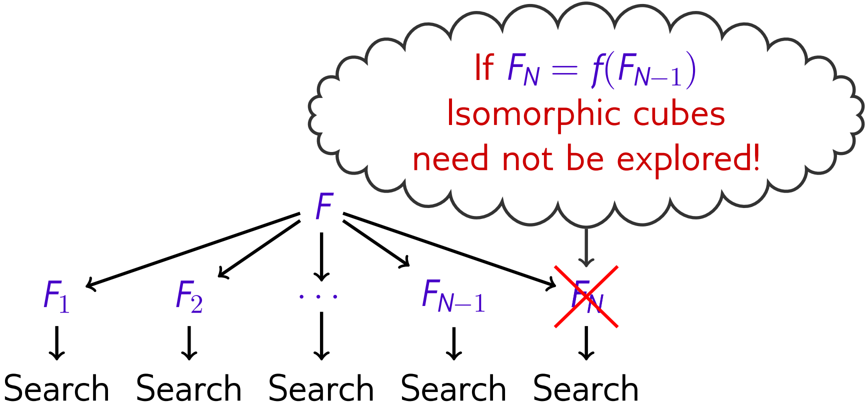
- For semigroups order 7, Mace4 generates 1,021,120,198 models,
- with 1,627,672 non-isomorphic $\approx 0.16\%$
- How to reduce amount of isomorphic models?
- How to parallelize?

# Cube and Conquer on SAT




- $F_i$ partition $F$.
- $F_i \equiv l_1 \wedge l_2 \cdots \wedge l_{k_i}$ (a cube)
- Different solver may be used for finding $F_i$.

# Cube and Conquer for Finite Models




- $F_i$ partition $F$.
- $F_i \equiv l_1 \wedge l_2 \cdots \wedge l_{k_i}$, where $l_j \equiv c_1 * c_2 = v$

# Isomorphic Cubes

- $\langle 0 * 0 = 0 \rangle$ isomorphic to $\langle 1 * 1 = 1 \rangle$
- $\langle 8 * 2 = 7 \rangle$ isomorphic to $\langle 0 * 1 = 2 \rangle$
- $\langle 0 * 0 = 0; 1 * 1 = 0 \rangle$ isomorphic to $\langle 0 * 0 = 1; 1 * 1 = 1 \rangle$.
- $\langle 0 * 0 = 0; 1 \diamond 1 = 0 \rangle$ isomorphic to $\langle 0 \diamond 0 = 1; 1 * 1 = 1 \rangle$.

# LNH Meets Cube Isomorphism

**Can we use LNH with cube pruning?**

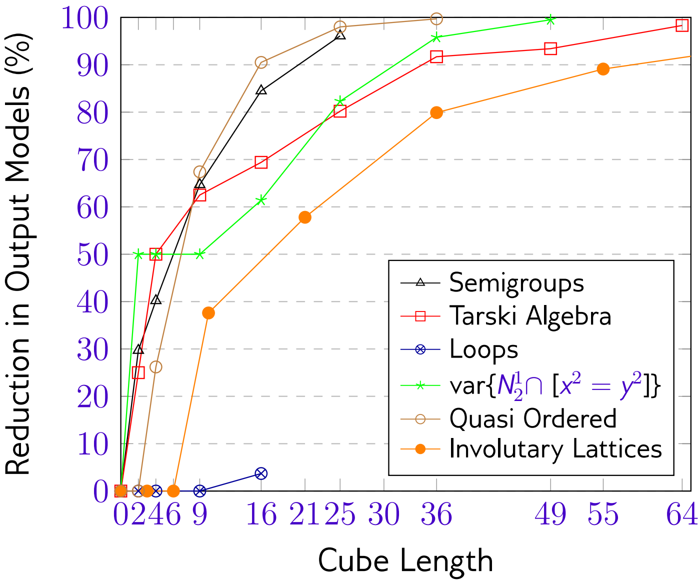
**Prove:**

- For any isomorphic $B_1$ and $B_2$ . . .
- for any search strategy of the solver . . .
- LNH search on $B_1$ gives only models isomorphic to the LNH search on $B_2$.
- **Remark:** Since we also care about enumeration, equisatisfiability is not enough.

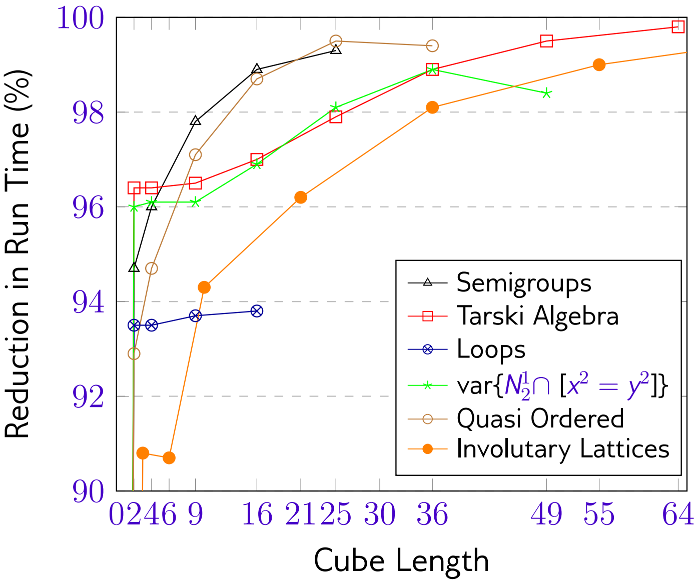
# Implementation

- On top of Mace4
- Work stealing — re-distribute workload
- Isomorphic cubes removal
  - at fixed lengths $(k, 2^k, 3^k, \cdots)$
  - invariants — divide cubes into buckets
  - rest, brute-force isocheck

# Experiments Isomorph Reduction



# Experiments Time Reduction



# Summary

- Cube and conquer for finite model finding:
  - Parallelization
  - Removal of isomorphic cubes
- Without sacrificing existing breaker LNH
- Significant speed up and model reduction

# What next?

- Better isomorphic cube removal?
- Optimal cube length?
- Optimal cube contents?