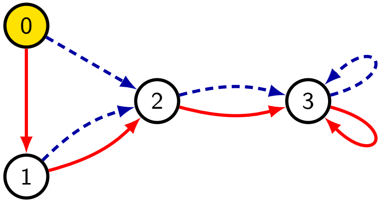
Computing Finite Index Congruences

Reinis Cirpons

University of St Andrews



Marina Anagnostopoulou-Merkouri, R. C, James D. Mitchell, and Maria Tsalakou (2024). *Computing finite index congruences of finitely presented semigroups and monoids*. arXiv: 2302.06295 [math.RA]

Some classical computational problems

Word problem

Given a monoid M generated by A and generators $a_i, b_j \in A$, does $a_1 \cdot a_2 \cdot \ldots \cdot a_n = b_1 \cdot b_2 \cdot \ldots \cdot b_m$ hold?

Triviality problem

Given a monoid M, is $|M| = 1$?

Isomorphism problem

Given two monoids M, N is $M \cong N$?

Finite monoids are nice

Theorem

If M is a finite monoid, then the following are all decidable:

- *Word problem,*
- *Triviality problem,*
- *Isomorphism problem*[a]*.*

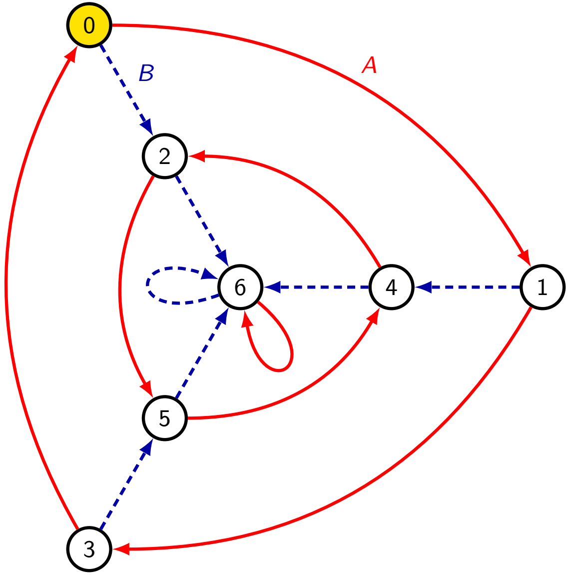
[a] When both monoids are finite.

Let $M = \langle A, B \rangle$ where

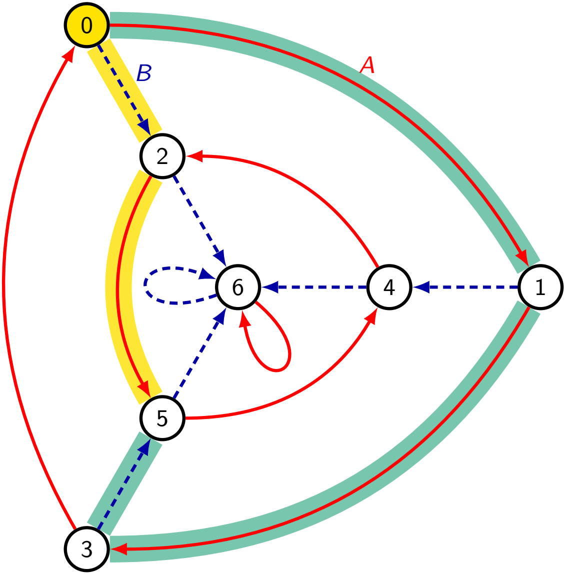
$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Is $B \cdot A = A \cdot A \cdot B$?

Is $B \cdot A = A \cdot A \cdot B$?



Is $B \cdot A = A \cdot A \cdot B$? Yes!



Finitely presented monoids are horrible

Example

Let M be the monoid presented by $\langle a, b \mid ab = ba \rangle$. Then

$$abba =_M baba =_M baab.$$

Furthermore $M \cong \mathbb{N} \times \mathbb{N}$

Finitely presented monoids are horrible

Example

Let M be the monoid presented by $\langle a, b \mid ab = ba \rangle$. Then

$$abba =_M baba =_M baab.$$

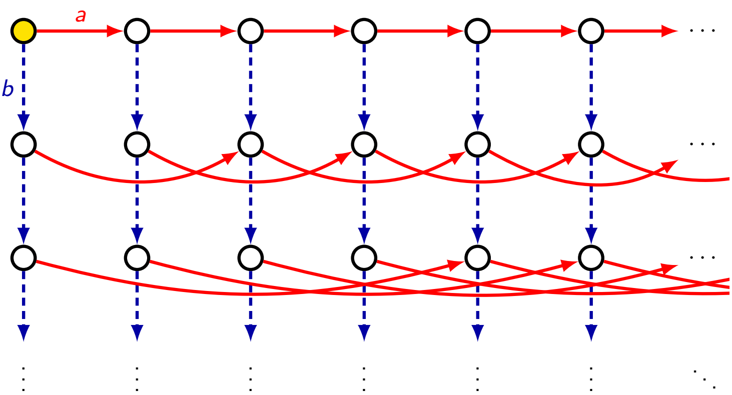
Furthermore $M \cong \mathbb{N} \times \mathbb{N}$

Theorem

The following are all undecidable for the class of f.p. monoids:

- *Word problem (Markov 1947; Post 1947),*
- *Triviality problem (Markov 1951),*
- *Isomorphism problem (Markov 1951).*

Consider the right Cayley graph of $\langle a, b \mid ba = a^2 b \rangle$:



Finite index congruences

Definition

Let M be a monoid. A congruence on M is an equivalence relation $\rho \subseteq M \times M$ such that

$$(x, y) \in \rho \Rightarrow (xs, ys) \in \rho \text{ and } (sx, sy) \in \rho \ \forall s \in M.$$

The set of equivalence classes of ρ form the quotient monoid M/ρ. There exists a unique surjective homomorhpism $\varphi : M \to M/\rho$. The index of ρ is $|M/\rho|$.

Definition

Let M be a monoid. A congruence on M is an equivalence relation $\rho \subseteq M \times M$ such that

$$(x, y) \in \rho \Rightarrow (xs, ys) \in \rho \text{ and } (sx, sy) \in \rho \ \forall s \in M.$$

The set of equivalence classes of ρ form the quotient monoid M/ρ. There exists a unique surjective homomorhpism $\varphi : M \to M/\rho$. The index of ρ is $|M/\rho|$.

Let M, ρ and $\varphi : M \to M/\rho$ be as above.

- If $\varphi(a_1) \cdot \ldots \cdot \varphi(a_n) \neq \varphi(b_1) \cdot \ldots \cdot \varphi(b_m)$, then $a_1 \cdot \ldots \cdot a_n \neq b_1 \cdot \ldots \cdot b_m$.
- If M/ρ is nontrivial, then so is M.
- If N does not admit an index $|M/\rho|$ congruence σ such that $M/\rho \cong N/\sigma$, then $M \ncong N$.

Finite index congruences

Definition

Let M be a monoid. A congruence on M is an equivalence relation $\rho \subseteq M \times M$ such that

$$(x, y) \in \rho \Rightarrow (xs, ys) \in \rho \text{ and } (sx, sy) \in \rho \ \forall s \in M.$$

The set of equivalence classes of ρ form the quotient monoid M/ρ. There exists a unique surjective homomorhpism $\varphi : M \to M/\rho$. The index of ρ is $|M/\rho|$.

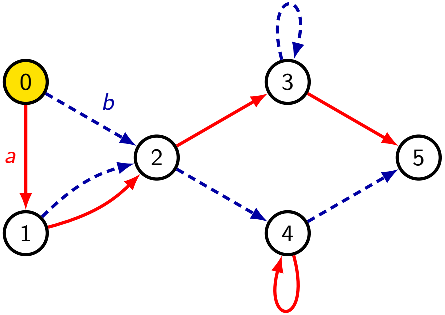
Let M, ρ and $\varphi : M \to M/\rho$ be as above.

- If $\varphi(a_1) \cdot \ldots \cdot \varphi(a_n) \neq \varphi(b_1) \cdot \ldots \cdot \varphi(b_m)$, then $a_1 \cdot \ldots \cdot a_n \neq b_1 \cdot \ldots \cdot b_m$.
- If M/ρ is nontrivial, then so is M.
- If N does not admit an index $|M/\rho|$ congruence σ such that $M/\rho \cong N/\sigma$, then $M \ncong N$.

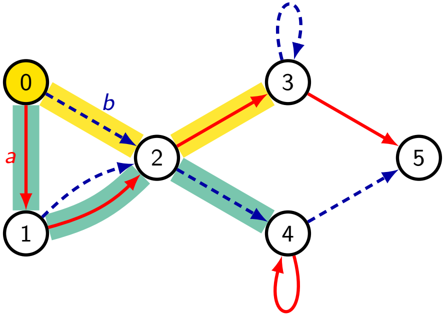
Theorem

Any k-generated monoid has at most n^{nk} distinct congruences of index n.

Let M be presented by $\langle a, b \mid ba = a^2b\rangle$. Can the following be the Cayley graph of M/ρ for any congruence ρ on M?



Let M be presented by $\langle a, b \mid ba = a^2b \rangle$. Can the following be the Cayley graph of M/ρ for any congruence ρ on M?



No!

Finite index congruence backtrack search

Let M be a finitely presented monoid. In (Anagnostopoulou-Merkouri et al. 2024) we give conditions for determining if a (possibly incomplete) word graph can be extended to one that

- corresponds to a two-sided congruence on M,
- corresponds to a right/left congruence on M,
- corresponds to a Rees congruence[1] on M,
- corresponds to a group congruence on M,
- defines a faithful action[2] on M.

We also give a backtrack search framework for efficiently iterating over all such word graphs up to a given number of vertices. Our backtrack method avoids double counting. Our approach can be seen as a generalization of the Sims low index subgroup algorithm for groups (Sims 1994).

---

[1] Provided the word problem in M is decidable.

[2] This only makes sense when M is finite.

Applications

- Counting finite index (left, right, two-sided) congruences of a f.p. monoid or semigroup.
- Counting finite index (left, right, two-sided) ideals of a f.p. monoid or semigroup with decidable word problem.
- Improving non-isomorphism and non-triviality testing.
- A more efficient implementation of McKinsey's algorithm for solving the word problem in residually finite monoids.
- Finding small transformation representations of finite monoids.

Thank you for your attention!

For more details see:

Marina Anagnostopoulou-Merkouri, R. C, James D. Mitchell, and Maria Tsalakou (2024). *Computing finite index congruences of finitely presented semigroups and monoids*. arXiv: 2302.06295 [math.RA]

`Semigroups` package for GAP system: semigroups.github.io/Semigroups

`libsemigroups` C++ library: libsemigroups.github.io

Anagnostopoulou-Merkouri, Marina, R. C, James D. Mitchell, and Maria Tsalakou (2024). *Computing finite index congruences of finitely presented semigroups and monoids*. arXiv: 2302.06295 [math.RA].

Markov, A. A. (1947). “On the impossibility of certain algorithms in the theory of associative systems”. In: *Doklady Akad. Nauk SSSR (N.S.)* 55, pp. 583–586.

— (1951). “The impossibility of certain algorithms in the theory of associative systems”. Russian. In: *Dokl. Akad. Nauk SSSR, n. Ser.* 77, pp. 19–20. ISSN: 0002-3264.

Post, Emil L. (1947). “Recursive unsolvability of a problem of Thue”. In: *J. Symbolic Logic* 12, pp. 1–11. ISSN: 0022-4812. DOI: 10.2307/2267170. URL: https://doi-org.uea.idm.oclc.org/10.2307/2267170.

Sims, Charles C. (1994). *Computation with Finitely Presented Groups*. Encyclopedia of Mathematics and its Applications. Cambridge University Press. DOI: 10.1017/CBO9780511574702.