Decision Problems in Invertible Automata

Evan Bergeron & Klaus Sutner

May 10, 2017

Carnegie Mellon University

What is your research?

What is your research?

Geometric group theory, from a computer scientist's view!

What is your research?

Automata theory turns out to be pretty useful for some recent developments in abstract algebra. Putting 251 and CDM to good use!

What did you prove?

What did you prove?

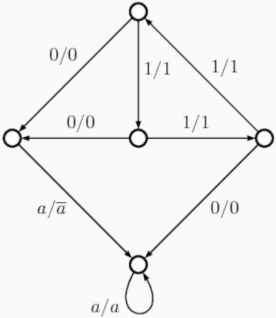
Three major results:

- MEMBERSHIP testing is decidable in the commutative case.
- ISGROUP is decidable in the commutative case.
- A KNAPSACK variant is undecidable.

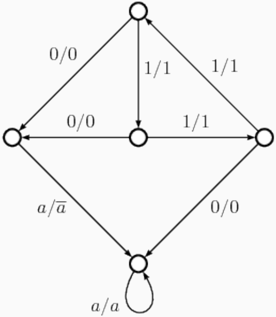
We'll focus on the last one for this talk.

Some quick background

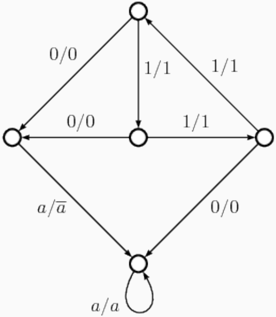
An *automaton* looks like this:



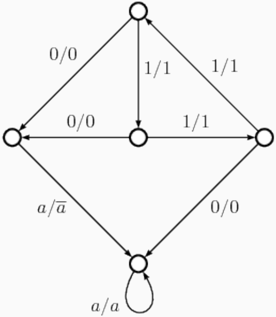
Each state corresponds with a function mapping strings to strings.



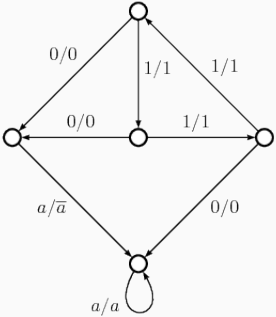
Starting at the middle state, on input "1100", we output "1101."



Since states are functions, we can compose them.



Composing the left corner with itself yields the identity function.



Some notation

If s is the function for some state, s^i is the function corresponding to running that state i times.

If s and s' are function for two states, ss' is the composition of s and s', first running s, then s'.

Knapsack definition

Given as input state functions $s_1 \ldots s_k$ and a target function s, do there exist natural numbers $a_1 \ldots a_k$ such that

$$s_1^{a_1} \cdots s_k^{a_K} = s$$

This turns out to be undecidable. We'll reduce from Hilbert's tenth problem.

Hilbert's Tenth Problem

Define HILBERT as following:

Given a polynomial $P(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ and an integer a, do there exist values $y_i \in \mathbb{N}$ such that $P(y_1, \ldots, y_n) = a$?

(There exist polynomials for which this is undecidable).

The reduction

A running example for clarity's sake:

$$P(x) = x^2 - x + 7,$$
$$a = -5$$

First, force all coefficients to be postive.

$x^2 - x + 7 = -5$

if and only if

$x^2 + 12 = x$

Second, generate a system of equations.

Each equation will look like

- $x + y = z$,
- $x = c$, or
- $x \cdot y = z$.

Second, generate a system of equations.

For example,

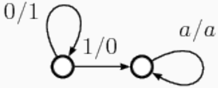
$$x^2 + 12 = x$$

if and only if *there exist* x_i's such that

$$\begin{aligned} x_1 &= x, \\ x_2 &= x * x_1, \\ x_3 &= x_2 + 12, \text{ and} \\ x_3 &= x. \end{aligned}$$

Third, model each equation with automata.

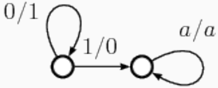
Addition can be represented using the adding machine:



If a is the left state, $x + y = z$ if and only if $a^x a^y = a^z$.

Third, model each equation with automata.

Constant equality also uses the adding machine.



$x = c$ if and only if $a^x = a^c$.

Third, model each equation with automata.

Multiplication can be represented using the Heisenberg semigroup:

$$H_3(\mathbb{N}) = \left\{ \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} ; a, b, c \in \mathbb{N} \right\}$$

(Multiplication of matrices of this form can be represented with automata).

The multiplication trick

$$H^x_{1,0,0}H^y_{0,0,1} = \begin{bmatrix} 1 & x & xy \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix} = H^z_{1,0,0}H^y_{0,0,1}H^x_{1,0,0}$$

where

$$H_{x,y,z} = \begin{bmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{bmatrix}$$

Then $x \cdot y = z$ iff $H^x_{1,0,0}H^y_{0,0,1} = H^z_{1,0,0}H^y_{0,0,1}H^x_{1,0,0}$.

Our running example previously

$$x^2 + 12 = x$$

if and only if *there exist* x_i's such that

$$x_1 = x$$

$$x_2 = x * x_1$$

$$x_3 = x_2 + 12$$

$$x_3 = x$$

Our running example now

$$x^2 + 12 = x$$

if and only if *there exist* x_i's such that

$$\begin{aligned}
a^{x_1} &= a^x && \text{in } \mathbb{N} \\
H_{1,0,0}^{x} H_{0,0,1}^{x_2} &= H_{1,0,0}^{x_1} H_{0,0,1}^{x_2} H_{1,0,0}^{x} && \text{in } H_3(\mathbb{N}) \\
a^{x_3} &= a^{x_2} a^{12} && \text{in } \mathbb{N} \\
a^{x_3} &= a^x && \text{in } \mathbb{N}
\end{aligned}$$

Lastly, combine into a single equation.

$$x^2 + 12 = x$$

if and only if *there exist* x_i's such that

$$(a^{x_1}, H^{x}_{1,0,0} H^{x_2}_{0,0,1}, a^{x_3}, a^{x_3}) = (a^{x}, H^{x_1}_{1,0,0} H^{x_2}_{0,0,1} H^{x}_{1,0,0}, a^{x_2} a^{12}, a^{x})$$

in $(\mathbb{N}, H_3(\mathbb{N}), \mathbb{N}, \mathbb{N})$.

(This corresponds with taking the product machine of different machines).

Recap

On input polynomial P,

1. Separate into positive and negative parts.
2. Generate system of equations.
3. Model each equation with an automaton.
4. Take product of all equations, feed to KNAPSACK oracle.

Questions?

Thanks!