Complexity-Theoretic Stories Around Two Theorems of Schützenberger

Denis Thérien
McGill University

March 2016

Languages and Monoids

$$\phi : A^* \to M \text{ homomorphism}$$

We say $L \subseteq A^*$ is recognized by M if there is some subset $F \subseteq M$ such that $L = \phi^{-1}(F)$.

Religion: The algebraic structure of M and the combinatorial properties of L are closely realted.

Miracle: This works beyond expectations!

Schützenberger Theorem # 1

Definition

Star-Free Languages: Smallest class of languages containing finite sets, closed under boolean operations and concatenation.

Definition

Aperiodic Monoid: M is aperiodic if no subset of M forms a non-trivial group

Theorem

L is star-free $\iff$ L can be recognized by an aperiodic monoid

Corollary

PARITY is not star-free.

Generalizing Morphisms to Programs

$$\phi = (\phi_n)_{n \geq 0} : A^* \to M$$

with $\phi_n : A^n \to M$ given by $(i_1, f_1) \ldots (i_s, f_s)$ where $\begin{cases} 1 \leq i_j \leq n \\ f_j : A \to M \end{cases}$

$$\phi_n(a_1 \ldots a_n) = f_1(a_{i_1}) \ldots f_s(a_{i_s})$$

Given $(F_n)_{n \geq 0}$ with $F_n \subseteq M$ this set-up recognizes the language $L \subseteq A^*$ where

$$L \cap A^n = \phi_n^{-1}(F_n) \text{ for each } n$$

Boolean Circuits

$C = (C_n)$ where $C_n : A^n \to \{0, 1\}$ is given by an acyclic directed graph with nodes of in-degree 0 labeled "$x_i = a?$" for $1 \leq i \leq n$, $a \in A$, and nodes of in-degree $k > 0$ labeled by some $k - ary$ boolean function.

This set-up recognizes the language $L \subseteq A^*$ where

$$L \cap A^n = \{\text{strings accepted by the output gate of } C_n\}$$

Computational Complexity

Definition

AC^0 : Circuits of constant depth, polynomial size, using AND/OR gates of unbounded fan-in

Theorem

Furst-Saxe-Sipser, Ajtai, Razborov, Smolenksly, Hastad:

$$PARITY \notin AC^0$$

Closing The Loop

Theorem

Barrington-T: $L \in AC^0 \iff$ *L can be recognized by a polynomial-length program over an aperiodic monoid.*

Corollary? $PARITY \notin AC^0$

Modular Counting Gates

Definition

CC^0: Circuits of constant-depth, polynomial size, using modular counting gates (e.g MOD_6).

Theorem

Barrington-Straubing-T: $L \in CC^0 \iff$ L can be recognized by a polynomial-length program over a solvable group

Conjecture: $AND \notin CC^0$.

Current state of affairs: It could be that $CC^0 = NP$.

Schützenberger Theorem # 2

Definition

Unambiguous Language: Finite disjoint union of languages of the form $A_0^* a_1 A_1^* \dots a_k A_k^*$ *where* $a_i \in A$, $A_i \subseteq A$, *and the concatentation is unambiguous*

Definition

DA:
monoids M *such that* $(MsM = MtM \text{ and } s = s^2) \implies t = t^2$

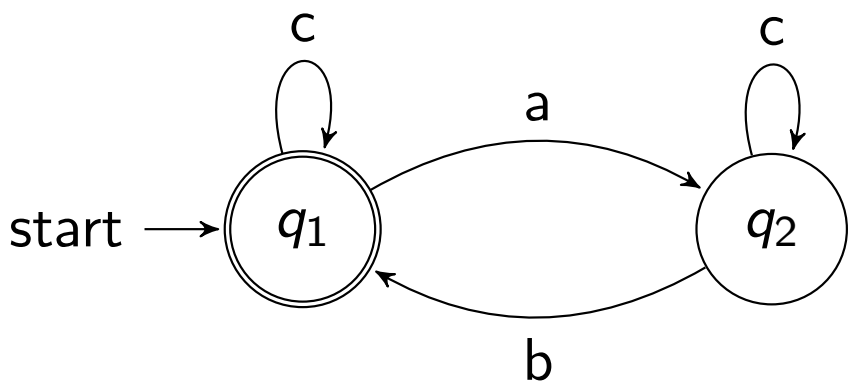
Theorem

L *is unambiguous* $\iff$ L *can be recognized by a monoid in* **DA**.

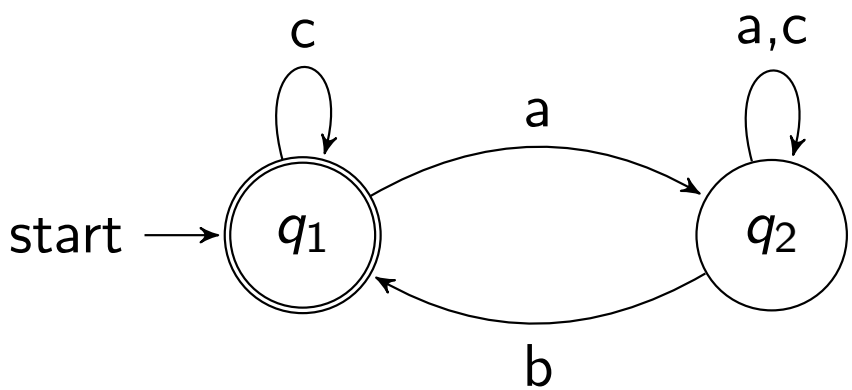
Schützenberger Theorem # 2

Corollary: neither of the following languages is unambiguous

Brandt Monoid:



Universal Monoid:



Computational Look at Monoids

Definition

A monoid M is universal if every language can be recognized by a program over M, when no restriction on length is imposed.

A monoid M has the polynomial length property (PLP) if any program over M is equivalent to a program of polynomial length over that monoid.

Conjecture: A monoid has the polynomial length property $\iff$ it is not universal

Special Cases

Groups:

- every nilpotent group has *PLP*
- every non-nilpotent group is universal

Aperiodic:

- every monoid in **DA** has *PLP*
- the universal monoid is universal
- the Brandt monoid is not universal but is not known to have *PLP*

The Conjecture

A monoid M has PLP

$$\Longleftrightarrow$$

It belongs to the variety $\mathbf{DA} * \mathbf{G}$, and every group in M is nilpotent.

Conclusion

Schützenberger has done lots of beautiful mathematics.

His proof of the two theorems outlined here certainly belong to The Book.

He thus lives forever!