Automatic semigroups

Rick Thomas

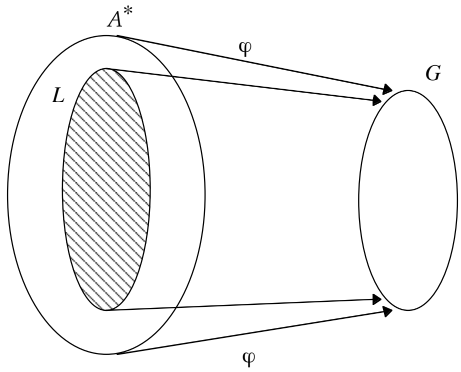
University of Leicester

Department of Computer Science

http://www.cs.le.ac.uk/people/rmt/

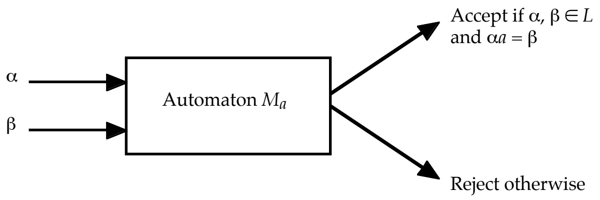
We have a group G or a semigroup S with a set of (semigroup) generators A. We have a natural mapping $\varphi : A^* \rightarrow G$.

Various notions of classes of groups and semigroups give rise to (the possibility of) effective computation. In the cases we will consider, we have $L \subseteq A^+ = A^* - \{\varepsilon\}$ such that L is regular and $L\varphi = G$.



Automatic groups *(Epstein et al)*

For each $a \in A \cup \{\varepsilon\}$ we have



We read our words synchronously and say that the group is *automatic*.

a_1	a_2	a_3	....	a_n	\$	....	\$
b_1	b_2	b_3	....	b_n	b_{n+1}	....	b_m

We can assume that L maps bijectively onto G. (If L does not map bijectively, we can replace L by a regular subset of L that does.) We then say that (A, L) is an automatic structure with *uniqueness*.

All of this (including the uniqueness) generalizes naturally to semigroups.

If a group G has an automatic structure with respect to one finite generating set, then it has an automatic structure with respect to any finite generating set. (Epstein et al)

This result generalizes to monoids. (Duncan, Robertson & Ruskuc)

A semigroup S is automatic if and only if S^1 is automatic. (Campbell, Robertson, Ruskuc & Thomas) We will concentrate on automatic monoids.

If G is an automatic group, then we can solve the word problem for G in quadratic time. (Epstein et al)

This also generalizes to monoids. (Campbell, Robertson, Ruskuc & Thomas)

Not everything generalizes to monoids …

Automatic groups are finitely presented. (Epstein et al)

This is not true for automatic monoids. (Campbell, Robertson, Ruskuc & Thomas)

A language L is said to be *prefix-closed* if, whenever $\alpha \in L$ and β is a prefix of α, then $\beta \in L$.

An automatic structure (A, L) is said to be *prefix-closed* if L is prefix-closed.

Every automatic group has a prefix-closed automatic structure.

Question. Does every automatic monoid have a prefix-closed automatic structure?

In groups, we have a nice geometric characterization of automaticity (the *fellow traveller property*).

Let M be a monoid, A be a finite generating set for M and L be a regular subset of A^+ mapping onto M. Let

$$N = (Q, A \cup \{\$\}, \tau, s, E)$$

be a DFA accepting $L\{\$\}^*$ with no dead states. For $\alpha \in A^+\{\$\}^*$, let $\underline{\underline{\alpha}} \in A^+$ be defined by $\alpha = \underline{\underline{\alpha}}\$^n$.

If $v, w \in M$, then define:

$$Q_{v,w,N} = \{ (\tau(s, \alpha), \tau(s, \beta)) \in Q \times Q : (\alpha, \beta) \in (A^+\{\$\}^* \times A^+) \cup (A^+ \times A^+\{\$\}^*), |\alpha| = |\beta|, \underline{\underline{\alpha}} =_M v, \underline{\underline{\beta}} =_M w \}.$$

For $v, v', w, w' \in M$ we say that (v, w) and (v', w') *have the same continuation graph* with respect to N, and write $(v, w) \equiv (v', w')$, if

- $Q_{v,w,N} = Q_{v',w',N}$;
- $\forall a \in A \cup \{\varepsilon\}, (p, q) \in Q_{v,w,N}$ & $\eta, \theta \in A^*$ with $\tau(p, \eta), \tau(q, \theta) \in E$, we have

$$v\eta a = w\theta \Leftrightarrow v'\eta a = w'\theta.$$

$\equiv$ is an equivalence relation on $M \times M$.

If $(M \times M)/\equiv$ is finite then we say that M has a *finite number of continuation graphs* with respect to N.

M has a finite number of continuation graphs with respect to N if and only if (A, L) is an automatic structure for M. (Hoffmann & Thomas)

In a monoid we have choices …

- which side do we multiply the generators on?
- which side do we take the paddings?

left-left automatic	pad on the left multiply on the left
left-right automatic	pad on the left multiply on the right
right-left automatic	pad on the right multiply on the left
right-right automatic	pad on the right multiply on the right

A monoid is said to be *X-Y automatic* if it has an X-Y automatic structure. The choices make no difference in groups - but they do in monoids!

If P is any subset of the set of these four notions, then there is an example of a monoid which satisfies all the properties in P but none of the properties outside P. (Hoffmann & Thomas)

These distinctions make no difference to the results we have mentioned so far.

However, if G and H are automatic groups, then the free product $G*H$ is automatic.

Question. If S and T are X-Y automatic monoids does it follow that $S*T$ is X-Y automatic?

This works if X-Y is right-right or left-left, but not in the other two cases.

Biautomaticity

G a group, $\varphi : A^+ \to G$ a homomorphism, L a regular subset of A^+, $L\varphi = G$.

1. (A, L) is a *biautomatic structure* for G if (A, L) is both a right-right and a right-left automatic structure.
2. (A, L) is a *biautomatic#* structure for G if A is closed under inversion and if (A, L) and (A, L^{-1}) are both right-right automatic structures for G.

Equivalently:

(A, L) is a *biautomatic#* structure for G if A is closed under inversion and if (A, L) is both a right-right and a left-left automatic structure for G.

These two notions for a biautomatic structure are not equivalent (even for groups).

Reassuringly, a group is biautomatic if and only if it is biautomatic#.

We have (at least) four possible notions of biautomaticity in monoids:

left-biautomatic : (A, L) is both a left-left & a left-right automatic structure

right-biautomatic : (A, L) both a right-left & a right-right automatic structure.

cross-biautomatic : (A, L) is both a right-left & a left-right biautomatic structure.

same-biautomatic : (A, L) is both a left-left & a right-right automatic structure.

The cancellative monoid M defined by the presentation

$$< a, b, c, d, f, g, x \;:\; abcx = xdfg,\; bx = xf,\; cax = xgdfgd >$$

satisfies all of the four notions of automaticity but none of the four notions of biautomaticity. (Hoffmann & Thomas)

A biautomatic monoid need not have a finite Noetherian confluent rewriting system. (Otto, Sattler-Klein & Madlener)

This is an open question for groups.

A biautomatic monoid can have an exponential Dehn function. (Otto, Sattler-Klein & Madlener); indeed it can exceed any primitive-recursive function (Otto).

Some advantages of (bi)automaticity:

1. Captures a wide class of groups and monoids.
2. Some computation is effective.

But ...

1. Doesn't seem to generalize naturally to other relational structures.
2. Some natural properties are undecidable (or not known to be decidable).

Structures

A structure $S = (D, R_1, R_2, \ldots, R_n)$ consists of:

- a set D, called the *domain* of S;
- for each i there exists $r = r_i \geq 1$ such that $R_i \subseteq D^r$; r is called the *arity* of R_i.

A structure $S = (D, R_1, R_2, \ldots, R_n)$ is said to be *computable* if:

- $D \subseteq A^*$ for some finite set A and there is a decision-making Turing machine M that outputs true if the input is in D (and false otherwise);
- for each R_i there is a decision-making Turing machine that outputs true on input $(a_1, \ldots, a_r)$ if $a_p \in D$ for all p and $(a_1, \ldots, a_r) \in R_i$ (and false otherwise).

FA-presentable structures

(introduced by Nerode & Khoussainov).

A structure $S = (D, R_1, R_2, \ldots, R_n)$ is said to be *FA-presentable* if:

- there is an alphabet A, a regular language L over A and a surjective map $\varphi : L \to D$;
- there is a finite automaton that accepts (a, b) if and only if $a, b \in L$ and $a\varphi = b\varphi$;
- for each R_i there is a finite automaton that accepts $(a_1, a_2, \ldots, a_r)$ if and only if $a_p \in L$ for all p and $(a_1, a_2, \ldots, a_r) \in R_i$.

We can insist that the map φ is bijective. (As with automatic groups and monoids, if L does not map bijectively onto D, we can replace L with a regular subset of L that does.)

If S is an FA-presentable structure and P is a first-order definable relation on S then P is decidable. (Nerode & Khoussainov)

Example. Conjugacy in a group is a first-order definable relation:

$$C(a, b) := (\exists x : x^{-1}ax = b).$$

There are not many examples where we have a complete characterization of FA-presentable structures:

- ordinals; (Delhommé)
- integral domains; (Khoussainov, Nies, Rubin & Stephan)
- Boolean algebras. (Khoussainov, Nies, Rubin & Stephan)

The following are equivalent for a finitely generated group G:

- G is FA-presentable;
- G is virtually abelian. (Oliver & Thomas)

It follows that a finitely generated FA-presentable group is automatic (but the converse is false).

We still seem to be some way from characterizing all FA-presentable groups (even all FA-presentable abelian groups).

If G is an FA-presentable group, then every finitely generated subgroup of G is virtually abelian. (Nies & Thomas)

Group G; finite set of generators

$$A = \{a_1, .. , a_n\}.$$

We then have a structure $\mathcal{G} = (G, R_1, ... , R_n)$ where $(g, h) \in R_i$ if and only if $ga_i = h$ (the *Cayley graph* of G).

If G is an automatic group then we have an encoding of the elements of G as words in A^* such that there are automata recognizing multiplication by elements of A; this gives that $\mathcal{G}$ is FA-presentable.

The converse is false (there are cases where $\mathcal{G}$ is FA-presentable but G is not automatic).

What about other structures?

A finitely generated commutative monoid need not be automatic. (Hoffmann & Thomas)

However:

A finitely generated commutative monoid is FA-presentable. (Oliver & Thomas)

So a finitely generated FA-presentable monoid is not necessarily automatic; this is in contrast to the situation in groups.

We also have:

An FA-presentable ring R with identity is locally finite (i.e. every finite subset of R generates a finite ring). (Nies & Thomas)