Finitely Generated Semiautomatic Groups

Sanjay Jain, Singapore

Bakhadyr Khoussainov, Auckland

Frank Stephan, Singapore

Finite Automata

Recognising Multiples of Three

Three states: Remainders $\mathbf{0}$ (initial), $\mathbf{1}$, $\mathbf{2}$.
Update of state on digit: $(\mathbf{s},\mathbf{d}) \mapsto (\mathbf{s}+\mathbf{d}) \bmod \mathbf{3}$;
for example, state $\mathbf{2}$ and input $\mathbf{8}$ give new state $\mathbf{1}$.
Accept numbers where final state is $\mathbf{0}$.

```
Input:  2 5 6 1 0 2 4 2 0 4 8
State: 0 2 1 1 2 2 1 2 1 1 2 1
Final Decision: Reject
```

Multiples of $\mathbf{p}$

States $\{\mathbf{0},\mathbf{1},\ldots,\mathbf{p}-\mathbf{1}\}$; initial state $\mathbf{0}$.
Update: $(\mathbf{s},\mathbf{d}) \mapsto ((\mathbf{s}\cdot\mathbf{10})+\mathbf{d}) \bmod \mathbf{p}$.
Accept numbers where final state is $\mathbf{0}$.

Automatic Structures - Example

Operations calculated or verified by finite automata

Automaton reads (from front or from end) inputs and has missing digits be replaced by symbol different from the alphabet. Here decimal adder with three states: n (no carry and correct), c (carry and correct), i (incorrect). Automaton works from the back to the front; start state and accepting state are n; states i and c are rejecting.

```
Correct Addition          Incorrect Addition
 # 2 3 5 8 . 2 2 5         3 3 3 3 . 3 3 #
 # 9 1 1 2 . # # #         # # 2 2 . 2 2 2
 1 1 4 7 0 . 2 2 5         # 1 5 5 . 5 5 2
n c n n c n n n n n       i i n n n n n n n
```

Alignment at the positions of "."; if no alignment rule is given, alignment at the first member of the string; "#" are placed to fill up free positions after alignment is done.

Automatic Structures - Formal

In an automatic structure,

- the domain is coded as a regular set;
- each relation in the structure is recognised by a finite automaton reading all inputs at same speed;
- each function in the structure is verified by a finite automaton: the automaton recognises the graph consisting of all valid (input,output)-tuples.

Examples: integers with addition and order; rationals with order, minimum and maximum; positive terminating decimal numbers with addition; finite subsets of the natural numbers with union and intersection and set-inclusion.

The inventors: Bernard R. Hodgson (1976, 1983); Bakhadyr Khoussainov and Anil Nerode (1995); Achim Blumensath and Erich Grädel (1999, 2000).

Characterising automatic functions

Theorem [Case, Jain, Seah and Stephan 2013].
A function $\mathbf{f} : \Sigma^* \to \Sigma^*$ is automatic iff there is a Turing machine with exactly one tape which computes $\mathbf{f}$ in linear time and which lets its output start at the same position where originally the input started.

Turing machine can use tape alphabet Γ much larger than Σ; time-bound linear in input-length.

Finite Automaton	Turing Machine
Goes in one direction	Goes forward and backward
Reads symbols	Reads and writes symbols
Finitely many states	Finitely many states; however, utilises tape as additional memory

Groups

A group $(\mathbf{G}, +)$ satisfies the following axioms:

- (Associativity) $\forall \mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbf{G}\,[(\mathbf{x}+\mathbf{y})+\mathbf{z} = \mathbf{x}+(\mathbf{y}+\mathbf{z})]$;
- (Neutral element) $\mathbf{0} \in \mathbf{G} \wedge \forall \mathbf{x} \in \mathbf{G}\,[\mathbf{x}+\mathbf{0} = \mathbf{x} \wedge \mathbf{0}+\mathbf{x} = \mathbf{x}]$;
- (Inverse element) $\forall \mathbf{x} \in \mathbf{G}\, \exists \mathbf{y} \in \mathbf{G}\,[\mathbf{x}+\mathbf{y} = \mathbf{0}]$.

Abelian groups are commutative: $\forall \mathbf{x}, \mathbf{y} \in \mathbf{G}\,[\mathbf{x}+\mathbf{y} = \mathbf{y}+\mathbf{x}]$.

Examples are integers, rationals and reals with addition as well as finite groups (remainder groups):

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Semiautomatic Structures

Automatic structures are quite restrictive and many structures cannot be represented.

Theorem [Tsankov 2011]. The additive group of the rationals is not automatic.

Semiautomatic structures try to represent more structures using automata. Idea: Instead of requiring that a function is an automatic function in all inputs, one requires only that the projected functions obtained by fixing all but one inputs by constants are automatic; similarly for relations including equality.

More formally, a structure like $(\mathbb{Q}, =, <; +)$ is semiautomatic if the sets and relations and functions before the semicolon are automatic and those after the semicolon are only semiautomatic.

Cayley Automatic Groups

Definition [Kharlampovich, Khoussainov and Miasnikov 2011]. A group $(\mathbf{A}, =; \{\mathbf{x} \mapsto \mathbf{x} \circ \mathbf{a} : \mathbf{a} \in \mathbf{A}\})$ is Cayley automatic iff it is finitely generated, the domain is regular, the equality is automatic and for every $\mathbf{a} \in \mathbf{A}$, the mapping $\mathbf{x} \mapsto \mathbf{x} \circ \mathbf{a}$ is automatic. If a finitely generated group satisfies that $(\mathbf{A}, =; \circ)$ is semiautomatic then it is called Cayley biautomatic.

Theorem [Miasnikov and Šunić 2012].
There are Cayley automatic groups which are not Cayley biautomatic.
The conjugacy problem and the first-order theory of some Cayley automatic groups are undecidable.

Theorem [Jain, Khoussainov and Stephan 2016].
If $(\mathbf{A}, \circ)$ is a Cayley automatic group then $(\mathbf{A}; \circ, =)$ is semiautomatic.

Implication

Let a Cayley automatic representation $(\mathbf{B}, =; \{\mathbf{x} \mapsto \mathbf{x} \circ \mathbf{a} : \mathbf{a} \in \mathbf{A}\})$ be given.

Now $\mathbf{A} = \{(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in \mathbf{B}\}$ with $(\mathbf{x}, \mathbf{y})$ representing $\mathbf{x}^{-1} \circ \mathbf{y}$.

Inversion: $(\mathbf{x}, \mathbf{y}) \mapsto (\mathbf{y}, \mathbf{x})$.
Group operation with constants:
$(\mathbf{x}, \mathbf{y}) \mapsto (\mathbf{x}, \mathbf{y} \circ \mathbf{a})$ represents $(\mathbf{x}^{-1} \circ \mathbf{y}) \circ \mathbf{a}$;
$(\mathbf{x}, \mathbf{y}) \mapsto (\mathbf{x} \circ \mathbf{a}^{-1}, \mathbf{y})$ represents $\mathbf{a} \circ (\mathbf{x}^{-1} \circ \mathbf{y})$.
$(\mathbf{x}, \mathbf{y})$ equals $\mathbf{a}$ iff $\mathbf{x} \circ \mathbf{a}^{-1} = \mathbf{y}$ what can be checked for every fixed $\mathbf{a} \in \mathbf{B}$.

In summary: $(\mathbf{A}, \mathbf{x} \mapsto \mathbf{x}^{-1}; \circ, =)$ is semiautomatic and equals the given Cayley automatic group.

Separation: Open Problem for Finitely Generated Groups. There are semiautomatic groups which are not finitely generated and thus not Cayley automatic.

Inversion

Proposition.
If $(\mathbf{A};\circ,=)$ is semiautomatic, so is $(\mathbf{B},\mathbf{x}\mapsto\mathbf{x}^{-1};\circ,=)$ for a suitably coded copy $\mathbf{B}$ of $\mathbf{A}$.

Here $\mathbf{B}=\{\mathbf{x},\mathbf{x}':\mathbf{x}\in\mathbf{A}\}$ consist of two regular copies of $\mathbf{A}$ where for each $\mathbf{x}\in\mathbf{A}$, $\mathbf{x}'$ denotes the inverse of $\mathbf{x}$.
The mappings $\mathbf{x}\mapsto\mathbf{x}\circ\mathbf{a}$ and $\mathbf{x}\mapsto\mathbf{a}\circ\mathbf{x}$ are extended from domain $\mathbf{A}$ to domain $\mathbf{B}$ by defining $\mathbf{x}'\circ\mathbf{a}=(\mathbf{a}^{-1}\circ\mathbf{x})'$ and $\mathbf{a}\circ\mathbf{x}'=(\mathbf{x}\circ\mathbf{a}^{-1})'$.
Furthermore, one tests whether $\mathbf{x}'=\mathbf{a}$ by testing whether $\mathbf{x}=\mathbf{a}^{-1}$, so the representatives of $\mathbf{a}$ form the regular set $\{\mathbf{x}:\mathbf{x}\in\mathbf{A}$ and $\mathbf{x}=\mathbf{a}\}\cup\{\mathbf{x}':\mathbf{x}\in\mathbf{A}$ and $\mathbf{x}=\mathbf{a}^{-1}\}$.
The inversion maps $\mathbf{x}\in\mathbf{A}$ to $\mathbf{x}'$ and $\mathbf{x}'$ with $\mathbf{x}\in\mathbf{A}$ to $\mathbf{x}$. So $'$ is appended if it is not there and deleted if it is at the end of $\mathbf{x}$. The special symbol $'$ is at the end of $\mathbf{x}$ or absent.

Semidirect Products

Let $(\mathbf{A}, \circ, =)$ be an automatic group and $(\mathbf{B}; \circ, =)$ be a semiautomatic group. Furthermore, let $\varphi_{\mathbf{b}}$ for every $\mathbf{b} \in \mathbf{B}$ be an automatic group automorphism $\mathbf{A} \to \mathbf{A}$ such that $\varphi_{\mathbf{b} \circ \mathbf{b}'}(\mathbf{a}) = \varphi_{\mathbf{b}}(\varphi_{\mathbf{b}'}(\mathbf{a}))$ for all $\mathbf{a} \in \mathbf{A}, \mathbf{b}, \mathbf{b}' \in \mathbf{B}$. Now one defines for $\mathbf{a}, \mathbf{b}$ that $\mathbf{b} \circ \mathbf{a} = \varphi_{\mathbf{b}}(\mathbf{a}) \circ \mathbf{b}$ and extends so $\circ$ to the set of all $\{\mathbf{a} \circ \mathbf{b} : \mathbf{a} \in \mathbf{A}, \mathbf{b} \in \mathbf{B}\}$. The so obtained group is called the semidirect product $\mathbf{A} \rtimes_{\varphi} \mathbf{B}$ of $\mathbf{A}$ and $\mathbf{B}$.

The set $\{(\mathbf{a}, \mathbf{b}, \mathbf{a}') : \mathbf{a}, \mathbf{a}' \in \mathbf{A}, \mathbf{b} \in \mathbf{B}\}$ permits to define a semiautomatic group operation, where $(\mathbf{a}, \mathbf{b}, \mathbf{a}')$ stands for $\mathbf{a} \circ \mathbf{b} \circ \mathbf{a}'$.

One can show that the restriction $\bullet$ of $\circ$ to one operand being from $\mathbf{A} \circ \{\varepsilon\} \circ \mathbf{A}$ is automatic. Furthermore, equality is semiautomatic and for each fixed $\mathbf{b} \in \mathbf{B}$, equality restricted to $\{(\mathbf{a}, \mathbf{b}, \mathbf{a}') : \mathbf{a}, \mathbf{a}' \in \mathbf{A}\}$ is automatic.

Nilpotent Groups

A finitely generated group has nilpotency class $\mathbf{k}$ iff for all elements $\mathbf{a_0, a_1, a_2, \ldots, a_k}$ the sequence $\mathbf{b_0 = a_0}$ and $\mathbf{b_{h+1} = b_h^{-1} \circ a_h^{-1} \circ b_h \circ a_h}$ ends in a $\mathbf{b_k}$ such that $\mathbf{b_k}$ is the neutral element ε. Here $\mathbf{b_h \circ a_h = a_h \circ b_h \circ b_{h+1}}$ and therefore one calls $\mathbf{b_{h+1}}$ also the communitator of $\mathbf{a_h, b_h}$; groups of nilpotency class $\mathbf{1}$ are Abelian.

Theorem [Kharlampovich, Khoussainov and Miasnikov 2011]. Finitely generated groups of nilpotency class $\mathbf{2}$ are Cayley automatic.

Theorem [Jain, Khoussainov and Stephan 2016]. Every finitely generated group of nilpotency class $\mathbf{3}$ is semiautomatic.

Question.
Is there a finitely generated group of nilpotency class $\mathbf{3}$ which is not Cayley automatic?

Examples and Facts

The class of all upper unitriangular $\mathbf{n} \times \mathbf{n}$ matrices like

1	a	b	c		1	0	b	c
0	1	d	e	or	0	1	0	e
0	0	1	f		0	0	1	0
0	0	0	1		0	0	0	1

has nilpotency class $\mathbf{n-1}$, the one in the picture nilpotency class $\mathbf{3}$. A communicator of $\mathbf{m}$ elements has $\mathbf{0}$ in the first $\mathbf{m-1}$ semidiagonals above the diagonal; thus if $\mathbf{m=n}$ then it is the unit matrix which is the neutral element. In the above example, the matrices on the right side form a commutative subgroup of the group.

Direct products of nilpotent groups are nilpotent groups.

A group is Abelian iff it has nilpotency class $\mathbf{1}$.

Main Result

Let $(\mathbf{A}, \circ)$ be finitely generated and have nilpotency class $\mathbf{3}$.

The set $\mathbf{B}$ of the subgroup generated by elements of the form $\mathbf{x}^{-1} \circ \mathbf{y}^{-1} \circ \mathbf{x} \circ \mathbf{y}$ is called the commutator subgroup; it is an Abelian subgroup.

The set $\mathbf{C}$ generated by $\{\mathbf{x}^{-1} \circ \mathbf{y}^{-1} \circ \mathbf{x} \circ \mathbf{y} : \mathbf{x} \in \mathbf{A}, \mathbf{y} \in \mathbf{B}\}$ commutes with all elements of $\mathbf{A}$.

Theorem [Jain, Khoussainov and Stephan 2016]
(a) Let $\bullet$ the restriction of $\circ$ to one input being from $\mathbf{B}$. The structure $(\mathbf{A}, \mathbf{B}, \mathbf{x} \mapsto \mathbf{x}^{-1}, \bullet; \circ, =)$ is semiautomatic.

(b) For some choices of $\mathbf{A}$, the structure $(\mathbf{A}, \mathbf{B}, =, \bullet; \circ)$ is not semiautomatic, as one can code NP-complete problems or even undecidable problems into the theory of the structure.

Construction of (a)

The quotient group $\mathbf{A}/\mathbf{B}$ is Abelian, thus one has finitely many generators $\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n}$ and each of them can occur in form $\mathbf{a_k^{m_k}}$ with either $\mathbf{m_k} \in \mathbb{Z}$ or $\mathbf{m_k} \in \{\mathbf{0}, \mathbf{1}, \ldots, \mathbf{p_k} - \mathbf{1}\}$ for some $\mathbf{p_k} \geq \mathbf{2}$.

Furthermore, $\mathbf{B}$ is Abelian and one can find generators $\mathbf{b_1}, \ldots, \mathbf{b_{n'}}, \mathbf{c_1}, \ldots, \mathbf{c_{n''}}$ of $\mathbf{B}$ where the subgroup $\mathbf{C}$ generated by $\mathbf{c_1}, \ldots, \mathbf{c_{n''}}$ only consists of commutators of three elements and commutes with all members of $\mathbf{A}$.

One represents all members of $\mathbf{A}$ by a triple $(\mathbf{b}, \mathbf{a}, \mathbf{b'})$ with $\mathbf{a} \in \mathbf{A}/\mathbf{B}$ and $\mathbf{b}, \mathbf{b'} \in \mathbf{B}$. The members in $\mathbf{a}$ are represented by $\mathbf{a_1^{m_1}} \circ \ldots \circ \mathbf{a_n^{m_n}}$ with the vector $(\mathbf{m_1}, \ldots, \mathbf{m_n})$ used in the representation; similarly vectors of the form $(\mathbf{m'_1}, \ldots, \mathbf{m'_{n'}}, \mathbf{m''_1}, \ldots, \mathbf{m''_{n''}})$ are used to represent $\mathbf{b}, \mathbf{b'}$.

Construction of (a) Continued

The m''_k cannot be represented as single numbers, as moving an a_i over an $a_j^{m_j}$ might generate not only $b_k^{m_j}$ but also some $c_\ell^{m_j(m_j-1)/2}$ or the like and therefore one stores the coordinates for the m''_ℓ in form $h_0 + h_1 \cdot m_1 + \ldots + h_n \cdot m_n$ which will be updated whenever some m_i changes.

Furthermore, one has some fixed linear combinations which give 0, for example, $20 \cdot m'_1 - 30 \cdot m''_2$, one can take these into account and nevertheless test, for all fixed values of $m_1, \ldots, m_n$, automatically whether some vectors $b, \tilde{b}$ are equal. Furthermore, for fixed $m_1, \ldots, m_n$, one can automatically compute the coordinates of the b-part when moving the b over the a and so automatically compare whether two vectors of the form $b \circ a \circ b'$ and $\tilde{b} \circ a \circ \tilde{b}'$ are equal.

Construction of (a) Continued

The numbers collaps to $\mathbf{h_0}$ when $\mathbf{m_1, \ldots, m_n}$ are all $\mathbf{0}$. The members of $\mathbf{A}$ which are actually in $\mathbf{B}$ have that the $\mathbf{m_1, \ldots, m_n}$ are all $\mathbf{0}$ and that therefore only the $\mathbf{h_0}$-entries of the $\mathbf{m''_k}$ are relevant in $\mathbf{b}$ and $\mathbf{b'}$; these can then simply be added to determine their value. This permits to automatically multiply any element from $\mathbf{A}$ of the form $\mathbf{b \circ a \circ b'}$ with with any element from $\mathbf{B}$ from either side.

When multiplying from the front, one has then only to update the entries $\mathbf{m'_k}$ and the $\mathbf{h_0}$-entries for the $\mathbf{m''_\ell}$ in $\mathbf{b}$ by adding the values of the corresponding coordinates in $\mathbf{B}$; similarly, when multiplying from the other side, one updates the values in $\mathbf{b'}$.

Construction of (b)

Construction of group to code the NP-hard problem

$$\mathbf{S} = \{(\alpha, \beta, \gamma) : \exists \mu, \nu \in \mathbb{Z}\, [\mu^{\mathbf{2}} \leq \gamma^{\mathbf{2}} \wedge \mu^{\mathbf{2}} + \nu \cdot \beta = \alpha]\}$$

which can be solved in polynomial time when group is semiautomatic as indicated; more involved constrution would permit to code undecidable problems.

One chooses $\mathbf{A}, \mathbf{B}$ such that $\mathbf{A}/\mathbf{B}$ is generated by $\mathbf{a_1}, \ldots, \mathbf{a_7}$, $\mathbf{B}$ is generated by $\mathbf{b_1}, \ldots, \mathbf{b_6}, \mathbf{c_1}, \mathbf{c_2}$ and satisfies

$$\begin{aligned}
&\mathbf{a_7 \circ a_1 = a_1 \circ a_7 \circ b_1}, \ldots, \mathbf{a_7 \circ a_6 = a_6 \circ a_7 \circ b_1}, \\
&\mathbf{b_1 \circ a_1 = a_1 \circ b_1 \circ c_1}, \mathbf{b_2 \circ a_2 = a_2 \circ b_2 \circ c_1 \circ c_2}, \\
&\mathbf{b_3 \circ a_3 = a_3 \circ b_3 \circ c_2}, \mathbf{b_4 \circ a_4 = a_4 \circ b_4 \circ c_2}, \\
&\mathbf{b_5 \circ a_5 = a_5 \circ b_5 \circ c_2}, \mathbf{b_6 \circ a_6 = a_6 \circ b_6 \circ c_2}.
\end{aligned}$$

If $\mathbf{i}, \mathbf{j} < \mathbf{7}$ then $\mathbf{a_i}, \mathbf{b_j}$ commute. Also commutators of three different $\mathbf{a_i}, \mathbf{a_j}, \mathbf{a_k}$ are ε.

Construction of (b) continued

$(\alpha, \beta, \gamma) \in \mathbf{S}$ iff there are $\mathbf{x}, \mathbf{x_1}, \mathbf{x_2} \in \mathbf{A}$, $\mathbf{y}, \mathbf{y_1}, \mathbf{y_2} \in \mathbf{B}$ with

$$\mathbf{b_1^\beta \bullet y_2 \bullet x = x \bullet b_1^\beta \bullet y_2 \bullet c_1^\alpha \bullet c_2^{\gamma^2}}$$

and the following side conditions are satisfied:

$$\mathbf{a_7 \circ x = x \circ a_7 \circ y,\ a_7 \circ x_1 = x_1 \circ a_7 \circ y_1,}$$
$$\mathbf{a_7 \circ x_2 = x_2 \circ a_7 \circ y_2,}$$
$$\mathbf{y = y_1 \bullet y_2,}$$
$$\mathbf{a_1 \circ y_2 = y_2 \circ a_1,\ a_2 \circ y_1 = y_1 \circ a_2,\ a_3 \circ y_1 = y_1 \circ a_3,}$$
$$\mathbf{a_4 \circ y_1 = y_1 \circ a_4,\ a_5 \circ y_1 = y_1 \circ a_5,\ a_6 \circ y_1 = y_1 \circ a_6}$$

and, for $\mathbf{i = 1, \ldots, 6}$ and $\mathbf{\tilde{x} = x, x_1, x_2}$ and for all $\mathbf{\tilde{y} \in B}$,

if $\mathbf{a_i \circ \tilde{x} = (\tilde{x} \circ a_i) \bullet \tilde{y}}$ then $\mathbf{a_7 \circ \tilde{y} = \tilde{y} \circ a_7}$.

Here $\mathbf{c_1^\alpha}$, $\mathbf{b_1^\beta}$, $\mathbf{c_2^{\gamma^2}}$ can be computed in polynomial time and the subsequent test is automatic.

Summary

For finitely generated groups, one has the implications

automatic $\Rightarrow$ Cayley biautomatic $\Rightarrow$ Cayley automatic $\Rightarrow$ semiautomatic

and for all groups one has the implications

Cayley biautomatic $\Rightarrow$ Cayley automatic $\Rightarrow$ semiautomatic $\Leftarrow$ automatic

where no further arrow holds. It is open whether every finitely generated semiautomatic group is Cayley automatic.

One can represent semiautomatic groups such that the inversion is automatic.

All finitely generated groups of nilpotency class $\mathbf{3}$ are semiautomatic.