

# **An Overview on Recent Results of Semiautomatic Groups and Semigroups**

**Frank Stephan, Singapore**

**Joint work with**

**Sanjay Jain, Singapore**

**Bakhadyr Khoussainov, Auckland**

**Dan Teng, Singapore**

**Siyuan Zou, Singapore**

# Finite Automata

## Recognising Multiples of Three

Three states: Remainders **0** (initial), **1**, **2**.

Update of state on digit:  $(s, d) \mapsto (s + d) \bmod 3$ ;

for example, state **2** and input **8** give new state **1**.

Accept numbers where final state is **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 $p$

States  $\{0, 1, \dots, p - 1\}$ ; initial state **0**.

Update:  $(s, d) \mapsto ((s \cdot 10) + d) \bmod p$ .

Accept numbers where final state is **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

# 2 3 5 8 . 2 2 5

# 9 1 1 2 . # # #

1 1 4 7 0 . 2 2 5

n c n n c n n n n n

Incorrect Addition

3 3 3 3 . 3 3 #

# # 2 2 . 2 2 2

# 1 5 5 . 5 5 2

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); Bakhtdyr Khoussainov and Anil Nerode (1995); Achim Blumen-sath and Erich Grädel (1999, 2000).

# Characterising automatic functions

**Theorem** [Case, Jain, Seah and Stephan 2013].

A function  $f : \Sigma^* \rightarrow \Sigma^*$  is automatic iff there is a Turing machine with exactly one tape which computes  $f$  in linear time and which lets its output start at the same position where originally the input started.

Turing machine can use tape alphabet  $\Gamma$  much larger than  $\Sigma$ ; 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  $(G, +)$  satisfies the following axioms:

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

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

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

·	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

# Abelian-by-Finite Groups

**Definition.** A group  $(G, +)$  is Abelian-by-Finite iff it has a Abelian subgroup  $(A, +)$  and a finite subset  $F \subseteq G$  such that  $G = \{x + y : x \in A \wedge y \in F\}$ .

**Definition.** A group  $(G, +)$  is finitely generated iff there is a finite set  $F$  such that  $G$  equals to the set of finite sums over the members of  $F$ .

**Theorem** [Oliver and Thomas 2005]. A finitely generated group is automatic iff it is Abelian-by-finite.

**Theorem** [Nies and Thomas 2008]. Every finitely generated subgroup of an automatic group is Abelian-by-finite.

**Question** [Nies 2007]. Is every torsion-free automatic group Abelian-by-finite?

# Groups and Order

An ordered group  $(G, +, <)$  satisfies the group axioms, that  $<$  is transitive, that for each  $x, y \in G$  exactly one of  $x < y$ ,  $x = y$  and  $y < x$  is true, that for each  $x, y, z \in G$  the condition  $x < y$  implies  $x + z < y + z$  and  $z + x < z + y$ . A group is left-ordered if  $x < y$  only implies  $z + x < z + y$  but not the other condition.

**Theorem** [Jain, Khoussainov, Stephan, Teng and Zou 2014]. Every automatic ordered group is Abelian, even if only the group operation and not the ordering is automatic. However, the Klein bottle group with lexicographic order is a left-ordered automatic group.

**Klein bottle group:** Two generators  $a, b$  with  $a \circ b = b^{-1} \circ a$  and  $a^i b^j < a^h b^k \Leftrightarrow i < h \vee (i = h \wedge j < k)$ .



# Two-Dimensional Integer-Groups

**Theorem** [Jain, Khoussainov, Stephan, Teng and Zou 2014]. The ordered group  $(\mathbb{Z} + \sqrt{3} \cdot \mathbb{Z}, +, <)$  is automatic.

**Representation.** Sequences  $a_n \dots a_1 a_0 . a_{-1} \dots a_{-m}$  of coefficients in  $\{-3, -2, -1, 0, 1, 2, 3\}$  representing  $a = \sum_{k=-m, \dots, n} u^k \cdot a_k$  aligned at the dot where  $u = 2 + \sqrt{3}$ .

**Important Equation** is  $4u^k = u^{k+1} + u^{k-1}$ .

**Basic Automatic Algorithm.** (Next Slide) Assume that  $d_k \in \{-9, \dots, 9\}$  for all  $k$ . This algorithm checks whether  $d = \sum_k d_k \cdot u^k$  is negative, zero or positive.

**Comparison.** To check whether  $a < b$ , compute digits  $d_k = b_k - a_k$  and determine the sign of  $d$ .

**Addition.** To check whether  $a + b = c$ , compute all digits  $d_k = a_k + b_k - c_k$  and determine the sign of  $d$ .

# Basic Automatic Algorithm.

Input  $a_n a_{n-1} \dots a_2 a_1 a_0 . a_{-1} a_{-2} \dots a_{-m}$ .

Initialisation  $v = 0$ ;  $w = 0$ ;  $k = n + 1$ .

While  $k > -m$  and  $v, w \in \{-30, -29, \dots, 29, 30\}$

Do Begin  $k = k - 1$ ;  $(v, w) = (4v + w, -v + a_k)$  End;

Represented Value is

$$v \cdot u^{k+1} + w \cdot u^k + \sum_{h < k} a_h \cdot u^h;$$

If  $v > 30$  Then Say “positive”; If  $v < -30$  Then Say “negative”; If  $-30 \leq v \leq +30$  Then Take Sign of  $v \cdot u + w$ .

**Verification.** If  $w$  is out of range then so is  $v$ .

If  $v$  is out of range then  $v$  determines the sign.

**Algorithm** can be carried out by finite automaton as  $v, w$  take only finitely many possible values.

# Does Addition Determine Order?

**Question** [Jain, Khoussainov, Stephan, Teng and Zou 2014]. Is there an automatic copy  $(\mathbf{A}, +)$  of the integers with addition such that  $<$  is not automatic?

**Comment.** This is equivalent to asking whether there is an automatic copy  $(\mathbf{A}, +)$  of the integers such that  $\{\mathbf{x} \in \mathbf{A} : \mathbf{x} \geq \mathbf{0}\}$  is not regular.

**Theorem** [Jain, Khoussainov, Stephan, Teng and Zou 2014]. There is an automatic copy of  $\{\mathbf{x} \cdot 2^{\mathbf{y}} \cdot 3^{\mathbf{z}} : \mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{Z}\}$  in which the addition is automatic but not the order.

The reason is that for every integers  $\mathbf{a}, \mathbf{k}$  there are integers  $\mathbf{b}, \mathbf{c}, \mathbf{d}$  with  $\mathbf{a}/6^{\mathbf{k}} = \mathbf{b}/2^{\mathbf{k}} + \mathbf{c}/3^{\mathbf{k}} + \mathbf{d}$  and  $0 \leq \mathbf{b} < 2^{\mathbf{k}}$  and  $0 \leq \mathbf{c} < 3^{\mathbf{k}}$  where  $\mathbf{b}$  is represented in binary and  $\mathbf{c}$  is represented in ternary. The addition on numbers represented in that way is automatic but the order not.

# 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.

# Semiautomatic Groups and Rings

**Theorem** [Tsankov 2011]. A subring  $(\mathbf{A}, +, =, <; \cdot)$  of the rationals is semiautomatic iff there is a positive natural number  $\mathbf{p}$  such that every element in  $\mathbf{A}$  is of the form  $\mathbf{x} \cdot \mathbf{p}^{\mathbf{y}}$  for some  $\mathbf{x}, \mathbf{y} \in \mathbb{Z}$ .

**Proposition.**

The ordered group  $(\mathbb{Q}, =, <; +)$  is semiautomatic.

The groups  $(\mathbb{Q}, =; \cdot)$  and  $(\mathbb{Z}^{\infty}, =; +)$  are semiautomatic.

**Theorem.**

If  $\mathbf{a}$  is a fixed square-root of an integer then the field  $(\mathbb{Q} + \mathbf{a} \cdot \mathbb{Q}; +, \cdot, =, <)$  is semiautomatic.

**Open Question.**

Are  $(\mathbb{Q}, =, <; +, \cdot)$  and  $(\mathbb{Q}, =; +, \cdot)$  semiautomatic?

# Automatic Group Operation

**Theorem** [Jain, Khoussainov, Stephan, Teng and Zou 2014]. If  $(\mathbf{A}, +; =)$  is a semiautomatic group with automatic group operation then  $(\mathbf{A}, +, =)$  is fully automatic. If  $(\mathbf{A}, +; <, =)$  is an ordered semiautomatic group with automatic group operation then  $(\mathbf{A}, +, <, =)$  is fully automatic ordered group.

Note that  $\mathbf{x} = \mathbf{y} \Leftrightarrow \exists \mathbf{z} [\mathbf{x} + \mathbf{z} = \mathbf{0} \text{ and } \mathbf{y} + \mathbf{z} = \mathbf{0}]$  and therefore comparing with the fixed element  $\mathbf{0}$  is sufficient for testing equality. Similarly, in an ordered group,  $\mathbf{x} < \mathbf{y} \Leftrightarrow \exists \mathbf{z} [\mathbf{x} + \mathbf{z} = \mathbf{0} \text{ and } \mathbf{0} < \mathbf{y} + \mathbf{z}]$ .

**Remark.** This is not true for semigroups. For example, if  $\mathbf{r} > \mathbf{0}$  is a nonrecursive real then  $(\mathbb{N} + \mathbf{r} \cdot \mathbb{N}, +, =; <)$  is semiautomatic but the structure has no automatic copy. There is a semigroup  $(\mathbf{A}, +; =)$  which is not automatic.

# Word Problem of Groups

## Definition.

Let a finite set of generators, say  $A = \{a, b, c, d\}$  of a semigroup be given and let it include the inverses (if they exist). Then  $\{(v, w) : v, w \in A^* \text{ and } v, w \text{ represent the same semigroup element}\}$  is called the word problem of the semigroup.

## Theorem [Based on Known Methods].

The word problem of a finitely generated subgroup of a semiautomatic group is polynomial time decidable.

## Theorem [Jain, Khoussainov, Stephan, Teng, Zou 2015].

There is a semiautomatic monoid where the word problem is undecidable.

# Algorithm for Group

Let  $a, b, c, d$  be the generators. There are automatic functions  $f_a, f_b, f_c, f_d$  mapping representatives  $x$  to representatives of  $x \circ a, x \circ b, x \circ c, x \circ d$ , respectively. Each function has output at most  $k$  symbols longer than input, for some constant  $k$ .

On input  $x, y$ , one checks  $x = y$  by starting with a representative of the neutral element and then applying the functions for the symbols in  $x$  and then the functions for the inverses of symbols in  $y$ , the latter in inverted order.

Then one evaluates the regular language which recognises all representatives of  $0$ .

Each of  $f_a, f_b, f_c, f_d$  runs in linear time and the length of the word in the memory increases at most by  $k \cdot |xy|$ , hence the overall time is quadratic. The final test of being the neutral element is linear.



# Example for Semigroup

Let  $\mathbf{B} \subseteq \{\mathbf{a}\} \cdot \{\mathbf{a}, \mathbf{b}\}^*$  be some set and consider the semigroup of all words  $\{\mathbf{a}, \mathbf{b}, \mathbf{c}\}^*$  with concatenation. Furthermore, let  $\pi$  exchange  $\mathbf{a}, \mathbf{b}$  and leave  $\mathbf{c}$  unchanged. New equality  $\equiv$ : let  $\mathbf{v}_0\mathbf{c}\mathbf{v}_1\mathbf{c}\dots\mathbf{c}\mathbf{v}_k \equiv \mathbf{w}_0\mathbf{c}\mathbf{w}_1\mathbf{c}\dots\mathbf{c}\mathbf{w}_k$  (where  $\mathbf{v}_h, \mathbf{w}_h \in \{\mathbf{a}, \mathbf{b}\}^*$ ) iff  $\mathbf{v}_0 = \mathbf{w}_0$  and  $\mathbf{v}_k = \mathbf{w}_k$  and  $\mathbf{v}_h = \mathbf{w}_h \vee (\mathbf{v}_h = \pi(\mathbf{w}_h) \wedge \mathbf{w}_h \in \mathbf{B}) \vee (\mathbf{v}_h = \pi(\mathbf{w}_h) \wedge \mathbf{v}_h \in \mathbf{B})$  for all other  $h$ .

Now for  $\mathbf{u} \in \{\mathbf{a}\} \cdot \{\mathbf{a}, \mathbf{b}\}^*$ ,  $\mathbf{u} \in \mathbf{B} \Leftrightarrow \mathbf{c}\mathbf{u}\mathbf{c} \equiv \mathbf{c}\pi(\mathbf{u})\mathbf{c}$ .

Similarly equality  $\equiv$  in the semigroup can be mapped back to membership of  $\mathbf{B}$  with a polynomial time truth-table reduction.

All representatives of a semigroup member form a finite set; the semigroup operation with a fixed element can be implemented as concatenation with a fixed word. Thus the monoid is semiautomatic.

# Cayley Automatic Groups

**Definition** [Kharlampovich, Khoussainov and Miasnikov 2011]. A group  $(\mathbf{A}, =; \{x \mapsto x \circ a : a \in \mathbf{A}\})$  is Cayley automatic iff it is finitely generated, the domain is regular, the equality is automatic and for every  $a \in \mathbf{A}$ , the mapping  $x \mapsto x \circ a$  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  $\mathbf{A} = \{(\mathbf{x}, \mathbf{y}) : \mathbf{x} \in \mathbf{B}\}$  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 complement 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  $\{\mathbf{x} : \mathbf{x} \in \mathbf{A} \text{ and } \mathbf{x} = \mathbf{a}\} \cup \{\mathbf{x}' : \mathbf{x} \in \mathbf{A} \text{ and } \mathbf{x} = \mathbf{a}^{-1}\}$ .

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.

# Nilpotent Groups

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

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

**Theorem** [Jain, Khoussainov and Stephan 2016].

If  $(A, \circ)$  is finitely generated, has nilpotency class  $3$  and  $B$  is its commutator subgroup and  $\bullet$  the restriction of  $\circ$  to one operator being from  $B$  then  $(A, B, x \mapsto x^{-1}, \bullet; \circ, =)$  is semiautomatic. For some choices of  $A$ , the structure  $(A, B, =, \bullet; \circ)$  is not semiautomatic.

# Summary

This talk gave an overview of the results from papers at CSR 2014, CCR 2015 and a submitted paper 2016.

For groups and monoids, the complexity of the word problem of finitely generated submonoids was determined; it is in polynomial time for a group and can be arbitrarily complex for monoids.

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

Cailey 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.