Advanced Automata Theory 9 Automatic Structures in General

Frank Stephan

Department of Computer Science

Department of Mathematics

National University of Singapore

fstephan@comp.nus.edu.sg

Repetition: Automatic Functions

Convolution

The convolution of two strings is formed by making pairs of characters in matching positions; the shorter string is padded with a special character, if needed.

$$\mathbf{conv}(001, 110011) = \binom{0}{1}\binom{0}{1}\binom{1}{0}\binom{\#}{0}\binom{\#}{1}\binom{\#}{1}$$

More precisely, the convolution of a $\mathbf{k}$-tuples $(\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_k})$ consists of characters in the alphabet $(\mathbf{\Sigma} \cup \{\#\})^{\mathbf{k}}$ and has length $\max\{|\mathbf{x_1}|, |\mathbf{x_2}|, \ldots, |\mathbf{x_k}|\}$ where the $\mathbf{m}$-th symbol $(\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_k})$ contains as $\mathbf{a_i}$ the $\mathbf{m}$-th symbol of $\mathbf{x_i}$ if that exists and $\#$ if $\mathbf{m} > |\mathbf{x_i}|$.

A relation $\mathbf{R} \subseteq (\mathbf{\Sigma}^*)^{\mathbf{k}}$ is automatic iff $\{\mathbf{conv}(\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_k}) : (\mathbf{x_1}, \mathbf{x_2}, \ldots, \mathbf{x_k}) \in \mathbf{R}\}$ is regular as a set of strings.

Groups, Monoids and Semigroups

Groups, monoids and semigroups are mathematical objects related to automata theory in two ways:

- The derivations of a regular language can be made into a monoid, leading to the definition of a syntactic monoid and characterisation of regular languages by congruence relations;
- Many groups, monoids and semigroups can be represented by automata in various ways.

There are prominent examples of groups: the integers $(\mathbb{Z}, +, \mathbf{0})$ and the rationals $(\mathbb{Q}, +, \mathbf{0})$; furthermore, permutation groups or the group of all possible move-sequences on Rubik's cube (modulo equivalence).

Definition of Groups

Let $\mathbf{G}$ be a set and $\circ$ be an operation mapping $\mathbf{G} \times \mathbf{G}$ to $\mathbf{G}$.
(a) The structure $(\mathbf{G}, \circ)$ is called a semigroup iff $\circ$ is associative, that is, iff $\mathbf{x} \circ (\mathbf{y} \circ \mathbf{z}) = (\mathbf{x} \circ \mathbf{y}) \circ \mathbf{z}$ for all $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbf{G}$.
(b) The structure $(\mathbf{G}, \circ, \mathbf{e})$ is called a monoid iff $(\mathbf{G}, \circ)$ is a semigroup and $\mathbf{e} \in \mathbf{G}$ and $\mathbf{e}$ satisfies $\mathbf{x} \circ \mathbf{e} = \mathbf{e} \circ \mathbf{x} = \mathbf{x}$ for all $\mathbf{x} \in \mathbf{G}$.
(c) The structure $(\mathbf{G}, \circ, \mathbf{e})$ is called a group iff $(\mathbf{G}, \circ, \mathbf{e})$ is a monoid and for each $\mathbf{x} \in \mathbf{G}$ there is an $\mathbf{y} \in \mathbf{G}$ with $\mathbf{x} \circ \mathbf{y} = \mathbf{e}$.
(d) A semigroup $(\mathbf{G}, \circ)$ is called finitely generated iff there is a finite subset $\mathbf{F} \subseteq \mathbf{G}$ such that for each $\mathbf{x} \in \mathbf{G}$ there are $\mathbf{n}$ and $\mathbf{y_1}, \mathbf{y_2}, \ldots, \mathbf{y_n} \in \mathbf{F}$ with $\mathbf{x} = \mathbf{y_1} \circ \mathbf{y_2} \circ \ldots \circ \mathbf{y_n}$.
(e) A semigroup $(\mathbf{G}, \circ)$ is finite iff $\mathbf{G}$ is finite as a set.

Automaticity of Groups & Semigroups

Let $(\mathbf{G}, \circ)$ be a semigroup.

Model of Epstein, Cannon, Holt, Levy, Paterson and Thurston

- $\mathbf{G}$ is chosen as regular set of words over finite set $\mathbf{F}$ of generators;
- Mapping $\mathbf{x} \mapsto \mathbf{x} \circ \mathbf{y}$ is automatic for fixed $\mathbf{y}$ (where $\mathbf{x} \circ \mathbf{y}$ stands for the unique element in $\mathbf{G}$ representing this value).

Model of Hodgson, Khousssainov and Nerode (fully automatic)

- Representatives $\mathbf{G}$ are given as arbitrary regular set;
- Mapping $\mathbf{x}, \mathbf{y} \mapsto \mathbf{x} \circ \mathbf{y}$ is automatic as function of two inputs.

Automatic Structures

A structure $(\mathbf{A}, \mathbf{R_1}, \ldots, \mathbf{R_m}, \mathbf{f_1}, \ldots, \mathbf{f_n}, \mathbf{c_1}, \ldots, \mathbf{c_h})$ is automatic iff $\mathbf{A}$ is a regular set and each relation $\mathbf{R_k}$ is an automatic relation with domain $\mathbf{A}^{\ell_\mathbf{k}}$ and each function $\mathbf{f_k}$ is an automatic function mapping $\mathbf{A}^{\ell'_\mathbf{k}}$ to $\mathbf{A}$; the constants $\mathbf{c_1}, \ldots, \mathbf{c_h}$ are specific members of $\mathbf{A}$.

Examples of automatic structures

$(\mathbb{N}, +, <, \mathbf{0}, \mathbf{1})$ is a monoid with order.

$(\mathbb{Z}, +, \mathbf{0}, \mathbf{POT})$ is a group with powers of $\mathbf{2}$.

Indeed, every fully automatic group is by definition an automatic structure.

$(\mathbb{Q}, +, \mathbf{0})$ is not an automatic structure.

Automatic Monoids and Structures

The monoid $(\{0,1\}^*, \circ, \varepsilon)$ with $\circ$ being the concatenation is automatic and has no representation as an automatic structure.

However, if one just uses instead of $\circ$ the mappings $x \mapsto x0$ and $x \mapsto x1$ then one gets a structure which is automatic.

The structure $(\{0,1\}^*, x \mapsto x0, x \mapsto x1, \varepsilon)$ is automatic.

There is a finitely generated group $(G, \circ)$ with generators a, b and the rule $aab = ba$ which is not automatic though the there is an automatic structure representing $(G, x \mapsto x \circ a, x \mapsto x \circ \overline{a}, x \mapsto x \circ b, x \mapsto x \circ \overline{b}, \varepsilon)$.

In this structure, G is not represented as a set of words over generators but as the convolution of a dyadic rationals i and 2^j representing $a^i b^j$, where $a^{1/2^n}$ stands for $\overline{b}^n a b^n$.

Definability and Automaticity

Khoussainov and Nerode showed that whenever in an automatic structure a relation or function is first-order definable from other automatic relations or functions then it is automatic.

$(\mathbf{0}^*, \mathbf{Succ})$ with $\mathbf{Succ(w) = w0}$ is isomorphic to the structure $(\mathbb{N}, \mathbf{x \mapsto x + 1})$. The addition is not automatic in this structure, hence addition cannot be first-order defined from the successor-relation.

If $(\mathbf{A}, +, \mathbf{0})$ is isomorphic to $(\mathbb{N}, +, \mathbf{0})$ then one can define the order $<$ by $\mathbf{x < y \Leftrightarrow x \neq y \wedge \exists z\,[x + z = y]}$.
Also the subsets of even and odd numbers are definable: $\mathbf{x}$ is even iff $\mathbf{\exists y\,[x = y + y]}$; $\mathbf{x}$ is odd iff $\mathbf{\forall y\,[x \neq y + y]}$.

In $(\mathbb{Z}, +)$, the order is not first-order definable and also not the set $\mathbb{N}$; it is an open problem whether for all fully automatic models of $(\mathbb{Z}, +)$, $\mathbb{N}$ is a regular subset.

Example 9.2, Definability

Consider the structure $(\{0,1\}^*, \{0\}^*, <_{\mathbf{sh}}, <_{\mathbf{ll}})$ where the relation $<_{\mathbf{sh}}$ says $\mathbf{x} <_{\mathbf{sh}} \mathbf{y} \Leftrightarrow |\mathbf{x}| < |\mathbf{y}|$.

One can define $<_{\mathbf{sh}}$ in $(\{0,1\}^*, \{0\}^*, <_{\mathbf{ll}})$ as follows:

$$|\mathbf{x}| <_{\mathbf{sh}} |\mathbf{y}| \Leftrightarrow \exists \mathbf{z} \in \{0\}^* [\mathbf{x} <_{\mathbf{ll}} \mathbf{z} \wedge (\mathbf{z} = \mathbf{y} \vee \mathbf{z} <_{\mathbf{ll}} \mathbf{y})].$$

One can define $\{0\}^*$ in $(\{0,1\}^*, <_{\mathbf{sh}}, <_{\mathbf{ll}})$:

$$\mathbf{x} \in \{0\}^* \Leftrightarrow \forall \mathbf{y} <_{\mathbf{ll}} \mathbf{x} [\mathbf{y} <_{\mathbf{sh}} \mathbf{x}].$$

Quiz

How can one define $\{1\}^*$ in $(\{0,1\}^*, <_{\mathbf{sh}}, <_{\mathbf{ll}})$?
Are $\{0\}^*$ and $\{1\}^*$ definable in $(\{0,1\}^*, <_{\mathbf{ll}})$?

Rings and Semirings

A structure $(\mathbf{A}, \oplus, \otimes, \mathbf{0}, \mathbf{1})$ is called a semiring with $\mathbf{1}$ iff it satisfies the following conditions:

1. $(\mathbf{A}, \oplus, \mathbf{0})$ is a commutative monoid;
2. $(\mathbf{A}, \otimes, \mathbf{1})$ is a monoid;
3. $\forall \mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbf{A} \left[\mathbf{x} \otimes (\mathbf{y} \oplus \mathbf{z}) = (\mathbf{x} \otimes \mathbf{y}) \oplus (\mathbf{x} \otimes \mathbf{z})\right]$ and $\forall \mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbf{A} \left[(\mathbf{x} \oplus \mathbf{y}) \otimes \mathbf{z} = (\mathbf{x} \otimes \mathbf{z}) \oplus (\mathbf{y} \otimes \mathbf{z})\right]$;
4. $\forall \mathbf{x} \in \mathbf{A} \left[\mathbf{x} \otimes \mathbf{0} = \mathbf{0}\right.$ and $\left.\mathbf{0} \otimes \mathbf{x} = \mathbf{0}\right]$.

If, furthermore, $(\mathbf{A}, \oplus, \mathbf{0})$ is a group then $(\mathbf{A}, \oplus, \otimes, \mathbf{0}, \mathbf{1})$ is called a ring with $\mathbf{1}$. Note that the first three properties plus invertability of $\oplus$ imply the fourth that everything times $\mathbf{0}$ is $\mathbf{0}$.

A semiring / ring is called commutative iff $\forall \mathbf{x}, \mathbf{y} \left[\mathbf{x} \otimes \mathbf{y} = \mathbf{y} \otimes \mathbf{x}\right]$.

Examples

$(\mathbb{Z}, +, *, \mathbf{0}, \mathbf{1})$ is the ring of integers.
Every field like $(\mathbb{Q}, +, *, \mathbf{0}, \mathbf{1})$ is a ring.

If $(\mathbf{A}, \oplus_{\mathbf{A}}, \otimes_{\mathbf{A}}, \mathbf{0_A}, \mathbf{1_A})$ and $(\mathbf{B}, \oplus_{\mathbf{B}}, \otimes_{\mathbf{B}}, \mathbf{0_B}, \mathbf{1_B})$ are rings then one can also define a ring $(\mathbf{A} \times \mathbf{B}, \oplus, \otimes, (\mathbf{0_A}, \mathbf{0_B}), (\mathbf{1_A}, \mathbf{1_B}))$ with the componentwise operations $(\mathbf{x}, \mathbf{y}) \oplus (\mathbf{x'}, \mathbf{y'}) = (\mathbf{x} \oplus_{\mathbf{A}} \mathbf{x'}, \mathbf{y} \oplus_{\mathbf{B}} \mathbf{y'})$ and $(\mathbf{x}, \mathbf{y}) \otimes (\mathbf{x'}, \mathbf{y'}) = (\mathbf{x} \otimes_{\mathbf{A}} \mathbf{x'}, \mathbf{y} \otimes_{\mathbf{B}} \mathbf{y'})$.

There is a finite ring $\mathbf{F}$ of operations modulo a number $\mathbf{r} \in \{\mathbf{2}, \mathbf{3}, \ldots\}$, here for $\mathbf{r} = \mathbf{4}$:

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

$*$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Infinite Automatic Ring

Assume that $(\mathbf{F}, +, *, 0, 1)$ is a finite ring. Let $\mathbf{G}$ contain those elements $\mathbf{x_1 x_2 \ldots x_n}$ in $\mathbf{F^*}$ which either satisfy $\mathbf{n = 1}$ or $\mathbf{n > 1 \wedge x_{n-1} \neq x_n}$. Intuitively, $\mathbf{02112}$ stands for $\mathbf{021122222\ldots}$ where the last symbol repeats forever.

Now let $\mathbf{x_1 x_2 \ldots x_n + y_1 y_2 \ldots y_m = z_1 z_2 \ldots z_h}$ if for all $\mathbf{k > 0}$, $\mathbf{x_{\min\{n,k\}} + y_{\min\{m,k\}} = z_{\min\{h,k\}}}$. Similarly for multiplication.

Now the member $\mathbf{0}$ of $\mathbf{F}$ is also the additive neutral element in $\mathbf{G}$ and $\mathbf{1}$ is also the multiplicative neutral element in $\mathbf{G}$.

The so generated $(\mathbf{G}, +, *, 0, 1)$ is an example of an infinite automatic ring and represents the ring of the eventually constant functions $\mathbf{f : \mathbb{N} \to F}$ with pointwise operations.

Example

For $\mathbf{F} = \{\mathbf{0}, \mathbf{1}\}$, the ring $\mathbf{G}$ can also be viewed as the set of all finite and cofinite subsets of $\mathbb{N}$; the intersection $\cap$ is the ring multiplication and the symmetric difference $\oplus$ is the addition. Note that when using $\cup$ in place of $\oplus$, the resulting structure is only a semiring and not a ring, as the union does not have for any nonempty set an inverse.

Coding. One identifies a subset $\mathbf{A} \subseteq \mathbb{N}$ with $\mathbf{f} : \mathbb{N} \to \{\mathbf{0}, \mathbf{1}\}, \mathbf{f}(\mathbf{n}) = \mathbf{A}(\mathbf{n})$ and then uses the definitions from the last slide. So $\mathbf{0110110}$ stands for $\{\mathbf{1}, \mathbf{2}, \mathbf{4}, \mathbf{5}\}$.

Quiz. Now match the following strings representing finite or cofininte sets in $\mathbf{G}$ to the subsets of $\mathbb{N}$ listed below:

$\mathbf{01}$, $\mathbf{0110}$, $\mathbf{101010}$, $\mathbf{011101}$, $\mathbf{1}$, $\mathbf{0}$, $\mathbf{01010}$.

$\mathbb{N}$, $\mathbb{N} - \{\mathbf{0}\}$, $\mathbb{N} - \{\mathbf{0}, \mathbf{4}\}$, $\{\mathbf{0}, \mathbf{2}, \mathbf{4}\}$, $\{\mathbf{1}, \mathbf{2}\}$, $\{\mathbf{1}, \mathbf{3}\}$, $\emptyset$.

Partial and Linear Orders

An ordering $\sqsubset$ on a set $\mathbf{A}$ is a relation satisfying the following two axioms:

1. $\forall \mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbf{A} \left[\mathbf{x} \sqsubset \mathbf{y} \wedge \mathbf{y} \sqsubset \mathbf{z} \Rightarrow \mathbf{x} \sqsubset \mathbf{z} \right]$;
2. $\forall \mathbf{x} \left[\mathbf{x} \not\sqsubset \mathbf{x} \right]$.

Well-known automatic orderings are $<_{\mathbf{lex}}$, $<_{\mathbf{ll}}$, $<_{\mathbf{sh}}$ and $\prec$.

An ordering is called linear iff

3. $\forall \mathbf{x}, \mathbf{y} \in \mathbf{A} \left[\mathbf{x} \sqsubset \mathbf{y} \vee \mathbf{x} = \mathbf{y} \vee \mathbf{y} \sqsubset \mathbf{x} \right]$.

The orderings $<_{\mathbf{lex}}$ and $<_{\mathbf{ll}}$ are linear, the orderings $<_{\mathbf{sh}}$ and $\prec$ are not linear.

Quiz

Let $\sqsubset$ be the componentwise comparison given by $(\mathbf{x}, \mathbf{y}) \sqsubset (\mathbf{x}', \mathbf{y}') \Leftrightarrow \mathbf{x} < \mathbf{x}' \wedge \mathbf{y} < \mathbf{y}'$ on $\mathbb{N} \times \mathbb{N}$. Is $\sqsubset$ a linear ordering?

Exercise 9.6

Consider $(\{\mathbf{0}\} \cdot \{\mathbf{0},\mathbf{1}\}^* \cup \{\mathbf{1}\}, \max_{\mathbf{lex}}, \min_{\mathbf{lex}}, \mathbf{0}, \mathbf{1})$. Show that this structure is an automatic semiring and verify the corresponding properties as well as the automaticity.

Does this work for the minimum and maximum of any automatic linear ordering $\sqsubset$ when the least element $\mathbf{0}$ and greatest element $\mathbf{1}$ exist?

Given the commutative automatic semiring $(\mathbf{R}, +, *, \mathbf{0}, \mathbf{1})$, consider the extension on $\mathbf{R} \times \mathbf{R} \times \mathbf{R}$ with the componentwise operation $+$ and the new multiplication $\odot$ given by $(\mathbf{x},\mathbf{y},\mathbf{z}) \odot (\mathbf{x}',\mathbf{y}',\mathbf{z}') = (\mathbf{x} * \mathbf{x}', \mathbf{y} * \mathbf{y}', \mathbf{x} * \mathbf{z}' + \mathbf{z} * \mathbf{y}')$? Is this a semiring? Is $\odot$ commutative? What are the neutral elements for $+$ and $\odot$ in this ring? Prove your answer.

Automatic Fields

Let $(\mathbf{A}, +, *, \mathbf{0}, \mathbf{1})$ be a ring with $\mathbf{1}$. $(\mathbf{A}, +, *, \mathbf{0}, \mathbf{1})$ is called a field iff $*$ can be inverted on every nonzero element: $\forall \mathbf{x} \in \mathbf{A}\, \exists \mathbf{y}\, [\mathbf{x} = \mathbf{0} \vee \mathbf{x} * \mathbf{y} = \mathbf{1}]$.

Examples of fields: $(\mathbb{Q}, +, *, \mathbf{0}, \mathbf{1})$, $(\mathbb{R}, +, *, \mathbf{0}, \mathbf{1})$.

The ring $(\{\mathbf{0}, \mathbf{1}, \ldots, \mathbf{r} - \mathbf{1}\}, +, *, \mathbf{0}, \mathbf{1})$ with operations modulo $\mathbf{r}$ is a field iff $\mathbf{r}$ is a prime number.

Theorem

There is no infinite automatic field.

No Infinite Automatic Field

Assume that $(\mathbf{A}, +, *, \mathbf{0}, \mathbf{1})$ is an automatic field and $<_{\mathbf{ll}}$ is the length-lexicographic order on $\mathbf{A}$.

Let $\mathbf{f(x)} = \min_{\mathbf{ll}}\{\mathbf{y} \in \mathbf{A} : \forall \mathbf{a}, \mathbf{a'}, \mathbf{b}, \mathbf{b'} \in \mathbf{A}$ with $\mathbf{a}, \mathbf{a'}, \mathbf{b}, \mathbf{b'} \leq_{\mathbf{ll}} \mathbf{x}\,[\mathbf{a} \neq \mathbf{a'} \Rightarrow (\mathbf{a} - \mathbf{a'}) * \mathbf{y} \neq \mathbf{b} - \mathbf{b'}]\}$.

Let $\mathbf{g(x)} = \max_{\mathbf{ll}}\{\mathbf{a} * \mathbf{f(x)} + \mathbf{b} : \mathbf{a}, \mathbf{b} \in \mathbf{A} \wedge \mathbf{a}, \mathbf{b} \leq_{\mathbf{ll}} \mathbf{x}\}$.

There is a constant $\mathbf{k}$ such that $\mathbf{A}$ has at least two elements shorter than $\mathbf{k}$ and $|\mathbf{g(x)}| \leq |\mathbf{x}| + \mathbf{k}$ for all $\mathbf{x} \in \mathbf{A}$.

If $\mathbf{A}$ has $\mathbf{m}$ elements of length up to $\mathbf{r} \cdot \mathbf{k}$ then $\mathbf{A}$ has $\mathbf{m^2}$ elements of length up to $(\mathbf{r} + \mathbf{1}) \cdot \mathbf{k}$.

This constradicts the fact that the number of words up to length $\mathbf{r} \cdot \mathbf{k}$ grows only exponentially in $\mathbf{r}$ and not doubleexponentially.

Ordinals

A linearly ordered set $(\mathbf{A}, <)$ is called an ordinal iff every nonempty subset $\mathbf{B}$ of $\mathbf{A}$ has a least element $\mathbf{b}$.

Two ordinals $(\mathbf{A}, <)$ and $(\mathbf{B}, <')$ are considered to be the same iff there is an orderpreserving bijective mapping $\mathbf{f}$ from $\mathbf{A}$ to $\mathbf{B}$.

The ordinal represented by $(\mathbb{N}, <)$ is called ω.

One can add ordinals: Given $(\mathbf{A}, <)$ and $(\mathbf{B}, <)$, one considers the set $\mathbf{C} = \{(\mathbf{0}, \mathbf{a}) : \mathbf{a} \in \mathbf{A}\} \cup \{(\mathbf{1}, \mathbf{b}) : \mathbf{b} \in \mathbf{B}\}$ with $(\mathbf{x}, \mathbf{y}) < (\mathbf{x}', \mathbf{y}')$ iff $\mathbf{x} < \mathbf{x}'$ or $\mathbf{x} = \mathbf{x}' \wedge \mathbf{y} < \mathbf{y}'$.

The ordinal $\omega + \mathbf{1}$ is obtained by putting one element behind all natural numbers, $\omega + \mathbf{1} \neq \omega$.

The sets $(\{\mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots\}, <)$, $(\{-\mathbf{1}, \mathbf{0}, \mathbf{1}, \mathbf{2}, \ldots\}, <)$ are isomorphic, so $\mathbf{1} + \omega = \omega$.

Cantor Normal Form

Cantor designed a way to represent small ordinals as sums of descending chains of ω-powers: $\omega^4 + \omega^2 + \omega^2 + \omega$. Here ω^{k+1} is the first ordinal which cannot be written as a finite sum of ordinals up to ω^k; ω is the first ordinal which cannot be written as $1 + 1 + \ldots + 1$.

Write $\omega^3 \cdot 2 + \omega \cdot 3 + 4$ instead of $\omega^3 + \omega^3 + \omega + \omega + \omega + 1 + 1 + 1 + 1$.

When adding ordinals, determine the highest power ω^k in the second term and add the coefficients of ω^k and take the higher powers from the first term and the lower powers from the second term.

Example:
$(\omega^8 \cdot 5 + \omega^7 \cdot 2 + \omega^4) + (\omega^7 + \omega^6 + \omega + 1) = \omega^8 \cdot 5 + \omega^7 \cdot 3 + \omega^6 + \omega + 1$.

Quiz

Form the following sums:

$$\begin{aligned}
(\omega^{5}+\omega^{3}) &+ (\omega^{4}+\omega^{2})\\
(\omega^{18}\cdot 18+\omega^{5}\cdot 5) &+ (\omega^{5}\cdot 5+\omega^{4}\cdot 4)\\
(\omega^{22}+\omega^{11}+\omega^{2}) &+ (\omega^{11}+\omega^{8}+\omega^{2}+\omega+8)\\
(\omega^{\omega+3}+\omega^{\omega}+\omega^{33}) &+ (\omega^{\omega}+\omega^{22})\\
(\omega^{2222}\cdot 1234) &+ (\omega^{\omega}+\omega^{132}\cdot 22)
\end{aligned}$$

Which is the largest of the following ordinals?

1. $\omega^{5}+\omega^{2}+\omega\cdot 12345678+23456789$,
2. $\omega^{4}\cdot 444+\omega^{3}\cdot 33+\omega^{2}\cdot 88+\omega\cdot 12+6$,
3. $\omega^{\omega+3}\cdot 22+\omega^{11}\cdot 111+\omega^{8}\cdot 88+\omega\cdot 8$,
4. $\omega^{\omega\cdot 2+12}\cdot 25+\omega^{222}\cdot 22+\omega^{2}$,
5. $\omega^{\omega\cdot 2+12}\cdot 25+\omega^{222}\cdot 22+25$,
6. $\omega^{257}\cdot 5+\omega^{256}\cdot 28+\omega^{255}\cdot 555$.

Example 9.9

The ordinals below ω^3 are automatic. One uses that $(\mathbb{N}, +, 0)$ is automatic and represents ordinals by tuples of natural numbers.

Represent $\omega^2 \cdot a_2 + \omega \cdot a_1 + a_0$ by $\mathbf{conv}(a_0, a_1, a_2)$.

$\mathbf{conv}(a_0, a_1, a_2) + \mathbf{conv}(b_0, b_1, b_2)$ is
$\mathbf{conv}(a_0 + b_0, a_1, a_2)$ if $b_1 = 0, b_2 = 0$;
$\mathbf{conv}(b_0, a_1 + b_1, a_2)$ if $b_1 > 0, b_2 = 0$;
$\mathbf{conv}(b_0, b_1, a_2 + b_2)$ if $b_2 > 0$.

$\mathbf{conv}(a_0, a_1, a_2) < \mathbf{conv}(b_0, b_1, b_2)$ iff
$a_2 < b_2 \vee (a_1 < b_1 \wedge a_2 = b_2) \vee (a_0 < b_0 \wedge a_1 = b_1 \wedge a_2 = b_2)$.

More general: The ordered monoid $(A, +, <, 0)$ of the ordinals below ω^k with $k \in \mathbb{N}$ can be represented by an automatic structure.

Theorem of Delhommé

The Ordinals below ω^ω (as a well-ordered set) do not have an automatic presentation.

Assume that $(\mathbf{A}, <)$ is a linearly ordered set such that its "bottom part" are the ordinals below ω^ω.

Let $\mathbf{u_k}$ represent $\omega^{\mathbf{k}}$ in the set $\mathbf{A}$.

For each $\mathbf{v} \in \mathbf{\Sigma}^{|\mathbf{u_k}|}$, let $\mathbf{V_{v,k}}$ be all $\mathbf{w} \succeq \mathbf{v}$ with $\mathbf{w} < \mathbf{u_k}$.

One can ignore the fixed prefix $\mathbf{v}$ of these sets and show that the set $\{\tilde{\mathbf{w}} : \mathbf{v} \cdot \tilde{\mathbf{w}} \in \mathbf{W}\}$ and the ordering on it are recognised by finite automata with $\mathbf{c}$ states for some constant $\mathbf{c}$.

Hence there are only finitely many sets $\mathbf{V_{v,k}}$; however each ordinal $\omega^{\mathbf{k}}$ is order-isomorphic to such a set, a contradiction.

Exercise 9.11

Prove this statement

If $\{\beta : \beta < \omega^{\mathbf{n}}\}$ is the union of finitely many sets $\mathbf{A_1}, \mathbf{A_2}, \ldots, \mathbf{A_m}$ then there is $\mathbf{k} \in \{\mathbf{1}, \mathbf{2}, \ldots, \mathbf{m}\}$ with $(\mathbf{A_k}, <)$ being order-isomorphic to the ordinals below $\omega^{\mathbf{n}}$.

For $\mathbf{n = 1}$: This follows from the fact that every infinite subset $\mathbf{A} \subseteq \mathbb{N}$ with ordering $<$ is orderisomorphic to ω.

For $\mathbf{n = 2}$: Let

$$\tilde{\mathbf{A}}_{\mathbf{k}} = \{\mathbf{i} : \exists^{\infty}\mathbf{j}\,[\omega \cdot \mathbf{i} + \mathbf{j} \in \mathbf{A_k}]\}$$

and then each $\mathbf{i}$ is in some $\tilde{\mathbf{A}}_{\mathbf{k}}$ and one $\tilde{\mathbf{A}}_{\mathbf{k}}$ is infinite. For this $\mathbf{k}$, show that $(\mathbf{A_k}, <)$ is isomorphic to $\omega^{\mathbf{2}}$.

Generalise this to larger $\mathbf{n}$.

Further Non-Automatic Structures

The following algebraic structures do not have any automatic presentation.

- $(\{1, 2, 3, \ldots\}, *, 1)$;
- $(\{q \in \mathbb{Q} : q > 0\}, *, 1)$ and $(\{q \in \mathbb{Q} : q \neq 0\}, *, 1)$;
- $(\mathbb{Q}, +, 0)$;
- if $(F, +, *, 0, 1)$ is a finite ring with 1 then the polynomial ring $(F[x], +, *, 0, 1)$ over F in one variable x does not have an automatic presentation.

Graphs

An undirected graph $(\mathbf{V}, \mathbf{E})$ is a set of vertices and edges between the vertices where $(\mathbf{x}, \mathbf{y}) \in \mathbf{E}$ iff $(\mathbf{y}, \mathbf{x}) \in \mathbf{E}$ for all $\mathbf{x}, \mathbf{y} \in \mathbf{V}$.

A graph is automatic iff $\mathbf{V}$ is regular and $\mathbf{E}$ is an automatic relation on $\mathbf{V}$. Two graphs $(\mathbf{V}, \mathbf{E})$ and $(\mathbf{V}', \mathbf{E}')$ are isomorphic iff there is a bijection $\mathbf{f} : \mathbf{V} \to \mathbf{V}'$ such that for all $\mathbf{x}, \mathbf{y} \in \mathbf{V}$: $(\mathbf{x}, \mathbf{y}) \in \mathbf{E} \Leftrightarrow (\mathbf{f}(\mathbf{x}), \mathbf{f}(\mathbf{y})) \in \mathbf{E}'$.

An undirected graph is called “a random graph” iff $\mathbf{V}$ is countable and infinite and for every two finite disjoint sets $\mathbf{A}, \mathbf{B}$ there is a node $\mathbf{x}$ such that $(\mathbf{x}, \mathbf{y}) \in \mathbf{E}$ for all $\mathbf{y} \in \mathbf{A}$ and $(\mathbf{x}, \mathbf{y}) \notin \mathbf{E}$ for all $\mathbf{y} \in \mathbf{B}$. All random graphs are isomorphic.

Theorem [Delhommé]. No random graph is automatic.

Proof of Delhommé's Theorem

Assume that $(\mathbf{V}, \mathbf{E})$ would be an automatic copy of the random graph. Furthermore, let $<_{\mathbf{ll}}$ be the automatic length-lexicographic order on $\mathbf{V}$.

Now define a relation $\mathbf{R}(\mathbf{x}, \mathbf{y})$ as there is no $\mathbf{z} <_{\mathbf{ll}} \mathbf{y}$ with $\forall \mathbf{u} \leq_{\mathbf{ll}} \mathbf{x} [(\mathbf{u}, \mathbf{z}) \in \mathbf{E} \Leftrightarrow (\mathbf{u}, \mathbf{y}) \in \mathbf{E}]$. As $\mathbf{R}$ is first-order defined with automatic parameters, $\mathbf{R}$ is automatic. Furthermore, $\mathbf{f_R}(\mathbf{x}) = \mathbf{max_{ll}}\{\mathbf{y} : \mathbf{R}(\mathbf{x}, \mathbf{y})\}$ is an automatic function; thus there is constant $\mathbf{c}$ with $|\mathbf{f_R}(\mathbf{x})| \leq |\mathbf{x}| + \mathbf{c}$ for all $\mathbf{x}$ and $\mathbf{c} \geq |\mathbf{min_{ll}}(\mathbf{V})|$.

Let $\mathbf{g}(\mathbf{n})$ be the number of element of $\mathbf{V}$ up to length $\mathbf{c} \cdot \mathbf{n}$. Now $\mathbf{g}(\mathbf{1}) \geq \mathbf{1}$ and $\mathbf{g}(\mathbf{n+1}) \geq \mathbf{2^{g(n)}}$, as for each splitting $(\mathbf{A}, \mathbf{B})$ of the elements of $\mathbf{V}$ up to length $\mathbf{c} \cdot \mathbf{n}$ there is an $\mathbf{y}$ connecting to those in $\mathbf{A}$ and not to those in $\mathbf{B}$. On one hand $\mathbf{g}(\mathbf{n})$ grows superexponentially and on the other hand there are only exponentially many elements up to length $\mathbf{c} \cdot \mathbf{n}$. Thus $(\mathbf{V}, \mathbf{E})$ cannot be automatic.

Exercise 9.13

Let $(\mathbf{G}, \circ)$ be a fully automatic group and $\mathbf{F}$ be a regular subset of $\mathbf{G}$. Is the graph $(\mathbf{G}, \mathbf{E})$ with $\mathbf{E} = \{(\mathbf{x}, \mathbf{y}) : \exists \mathbf{z} \in \mathbf{F} \, [\mathbf{x} \circ \mathbf{z} = \mathbf{y}]\}$ automatic?

To which extent can the result be transferred to automatic groups? Consider the special cases for $\mathbf{F}$ being finite and $\mathbf{F}$ being infinite. In which cases are there automatic groups $(\mathbf{G}, \circ)$ in the sense of Epstein, Cannon, Holt, Levy, Paterson and Thurston such that for given $\mathbf{F}$ the graph $(\mathbf{G}, \mathbf{E})$ is automatic?

Exercise 9.14

Consider the following structure: For $\mathbf{a} = (\mathbf{a_0}, \mathbf{a_1}, \ldots, \mathbf{a_n}) \in \mathbb{N}^{\mathbf{n+1}}$, let

$$\mathbf{f_a(x)} = \sum_{\mathbf{m=0}}^{\mathbf{n}} \mathbf{a_m} \cdot \binom{\mathbf{x}}{\mathbf{m}}$$

and let $\mathbf{F}$ be the set of all so defined $\mathbf{f_a}$ (where $\mathbf{n}$ is not fixed). For which of the following orderings $<_\mathbf{k}$ is $(\mathbf{F}, <_\mathbf{k})$ an automatic partially ordered set?

(1) $\mathbf{a} <_\mathbf{1} \mathbf{b} \Leftrightarrow \mathbf{f_a} \neq \mathbf{f_b}$ and $\mathbf{f_a(x)} < \mathbf{f_b(x)}$ for the first $\mathbf{x}$ where they differ;

(2) $\mathbf{a} <_\mathbf{2} \mathbf{b} \Leftrightarrow \exists^\infty \mathbf{x} \, [\mathbf{f_a(x)} < \mathbf{f_b(x)}]$;

(3) $\mathbf{a} <_\mathbf{3} \mathbf{b} \Leftrightarrow \forall^\infty \mathbf{x} \, [\mathbf{f_a(x)} < \mathbf{f_b(x)}]$.

Explicit Automatic Relations

For the following exercises, let the binary string $\mathbf{val(a_0 a_1 \ldots a_n)}$ denote $\sum_{\mathbf{m}} \mathbf{2^m \cdot a_m}$ where $\mathbf{a_m} \in \{0, 1\}$ and allow leading zeroes. For convolutions, there is in this specific case no need to distinguish $\#$ and 0.

Exercise 9.15 Construct a two-state dfa which checks whether $\mathbf{val(x)} \leq \mathbf{val(y)}$ for binary strings $\mathbf{x}, \mathbf{y}$.

Exercise 9.16 Construct a dfa which checks whether $\mathbf{val(x)} < \mathbf{val(y)} + \mathbf{val(z)}$ for binary strings $\mathbf{x}, \mathbf{y}, \mathbf{z}$.

Exercise 9.17 Construct a dfa which checks whether $\max\{\mathbf{val(x)}, \mathbf{val(y)}\} \leq \mathbf{val(z)} + \mathbf{val(z)}$ for binary strings $\mathbf{x}, \mathbf{y}, \mathbf{z}$.

Exercise 9.18 Construct a dfa which checks whether $\max\{\mathbf{val(x)}, \mathbf{val(y)}\} \leq \min\{\mathbf{val(y)}, \mathbf{val(z)}\}$ for binary strings $\mathbf{x}, \mathbf{y}, \mathbf{z}$.

Automaticity and Non-Automaticity

Exercise 9.19: The structure $(\{0,1\}^*, \mathbf{Pal}, \mathbf{u} \mapsto \mathbf{u0}, \mathbf{u} \mapsto \mathbf{u1})$ is not automatic in the current representations, as the set $\mathbf{Pal}$ of all palindromes is not regular. Is there any other automatic presentation of this structure? Prove the answer.

Yuri Matiyasevich showed that there is a polynomial $\mathbf{p}(\mathbf{x}, \mathbf{y_1}, \ldots, \mathbf{y_9})$ with integer coefficients such that one cannot decide whether for given $\mathbf{x} \in \mathbb{N}$ one can find $\mathbf{y_1}, \ldots, \mathbf{y_9} \in \mathbb{N}$ with $\mathbf{p}(\mathbf{x}, \mathbf{y_1}, \ldots, \mathbf{y_9}) = \mathbf{0}$.

Exercise 9.20: Show that the ring $(\mathbb{Z}, +, \cdot, <, \mathbf{0}, \mathbf{1})$ is not automatic.

Exercise 9.21: Show that the structure $(\mathbb{Z}, +, \mathbf{S}, <, \mathbf{0}, \mathbf{1})$ is not automatic, where $\mathbf{S}$ is the set of square numbers.

Additional Exercises

Exercise 9.22: Call a subset $\mathbf{A} \subseteq \mathbb{N}$ eventually $\mathbf{k}$-periodic, iff there are $\mathbf{i}, \mathbf{j}$ with $\mathbf{1} \leq \mathbf{j} \leq \mathbf{k}$ such that, for all $\mathbf{x} \geq \mathbf{i}$, $\mathbf{A}(\mathbf{x}) = \mathbf{A}(\mathbf{x} + \mathbf{j})$. Prove that for each $\mathbf{k} \in \mathbb{N}$ with $\mathbf{k} > \mathbf{0}$ there is an automatic representation of all eventually $\mathbf{k}$-periodic sets such that union, intersection and symmetric difference are fully automatic.

Exercise 9.23: Call a function $\mathbf{f} : \mathbb{Z} \to \mathbb{Z}$ to be a $\mathbf{k}$-step function iff there are at most $\mathbf{k}$ vaues $\mathbf{x}$ with $\mathbf{f}(\mathbf{x}) \neq \mathbf{f}(\mathbf{x} + \mathbf{1})$. Construct an automatic structure of all $\mathbf{k}$-step functions which has a two-place automatic function $\mathbf{F_k} : \mathbf{e}, \mathbf{x} \to \mathbf{f_e}(\mathbf{x})$ mapping $\mathbf{x} \in \mathbb{Z}$ to the value $\mathbf{f_e}(\mathbf{x})$ for the $\mathbf{e}$-th $\mathbf{k}$-step function.

Exercise 9.24: Prove that one can define $\mathbf{F_k}$, $\mathbf{F_{2k}}$ from Exercise 9.23 such that there is an automatic function $\mathbf{g_k}$ mapping each two indices $\mathbf{i}, \mathbf{j}$ of $\mathbf{k}$-step functions to an index $\mathbf{g_k}(\mathbf{i}, \mathbf{j})$ of a $\mathbf{2k}$-step function with $\forall \mathbf{x} \left[\mathbf{f_{g_k(i,j)}}(\mathbf{x}) = \mathbf{f_i}(\mathbf{x}) + \mathbf{f_j}(\mathbf{x})\right]$.