Logic and Automata I: Automata on Infinite Words

Wolfgang Thomas

RWTH AACHEN

Computability in Europe, Budapest, June 2014

The Plan

We present automata theory as a tool to make logic effective.

Three parts:

1. **Automata on infinite words**
2. **Infinite games**
3. **Tree automata and decidability of monadic theories**

Background: MSO Logic

Why MSO-Logic? Tarski's Problem

Gödel's and Turing's results implied:

The first-order theory of $(\mathbb{N}, +, \cdot, 0, 1)$ is undecidable.

If we use second-order logic, we get undecidability even for $(\mathbb{N}, +1, 0)$.

Define addition (and similarly multiplication):

$x + y = z$ iff each binary relation that contains $(0, x)$ and is closed under $(m, n) \mapsto (m + 1, n + 1)$ contains also (y, z)

Alfred Tarski asked:

Is the monadic second-order theory of $(\mathbb{N}, +1, 0)$ decidable?

Alfred Tarski (1901 - 1983)

“Model-Checking”

Today we call this a model-checking problem:

Is the model-checking problem

$(\mathbb{N}, +1, 0) \models \varphi$**?**

w.r.t. MSO -logic decidable?

Other names: S1S, SC, Büchi’s arithmetic

In computer science, the emphasis has shifted:

Does a system model G **satisfy a specification** φ**?**

G **is often a transition graph:** $G = (V, (E_a)_{a \in \Sigma}, (P_b)_{b \in \Gamma})$

MSO Logic over $(\mathbb{N}, +1, 0)$

We have

- **first-order variables $x, y, z, \ldots$ ranging over natural numbers**
- **set variables $X, Y, Z, \ldots$ ranging over sets of natural numbers**
- **terms formed from first-order variables and 0 by application of "$+1$"**
- **atomic formulas $s = t$ and $X(t)$ for terms s, t and set variables X**
- **connectives $\neg, \vee, \wedge, \rightarrow, \leftrightarrow$ and quantifiers $\exists$, $\forall$**

Example Formulas

- **Over $(\mathbb{N}, +1, 0)$ the induction axiom:**

  $\forall X (X(0) \wedge \forall y (X(y) \rightarrow X(y+1)) \ \rightarrow \ \forall z X(z))$

- **Over graphs (V, E) 3-colorability:**

  $\exists X_1 \exists X_2 \exists X_3 (\text{Partition}(X_1, X_2, X_3)$
  $\wedge \forall x \forall y (E(x,y) \rightarrow \bigvee_{i \neq j} (X_i(x) \wedge X_j(y))))$

- **Over $(\mathbb{N}, +1, 0)$ the existence of automaton runs (e.g., for three states):**

  $\exists X_1 \exists X_2 \exists X_3$
  $(\text{Partition}(X_1, X_2, X_3)$
  $\wedge$ **transition and acceptance condition**$)$

Transitive Closure

We have $x \leq y$ iff for all sets X containing x and closed under successor, $X(y)$ holds.

For any MSO-formula $\varphi(z, z')$, we write

$$\varphi^*(x, y) \;:=$$

$$\forall X(X(x) \wedge \forall z, z'(X(z) \wedge \varphi(z, z') \rightarrow X(z')) \;\rightarrow\; X(y))$$

Another shortwriting:

$\exists^\omega y \ldots$... **for** $\forall x \exists y(x < y \wedge \ldots$

Example

“Each set with two successive elements contains an even number”

First define “y is even”:

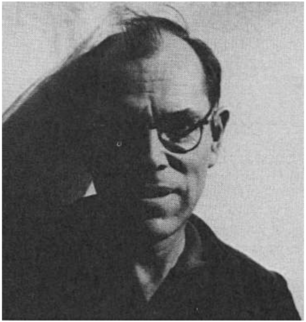
Set $\varphi_2(z, z') \;:=\; (z+1)+1 = z'$

$\mathrm{Even}(y) := \varphi_2^*(0, y)$

Then we take the following formula:

$$\forall X(\exists x(X(x) \wedge X(x+1)) \rightarrow \exists y(X(y) \wedge \mathrm{Even}(y)))$$

Büchi's Theorem



Richard J. Büchi (1924 - 1984)

The MSO-theory of $(\mathbb{N}, +1, 0)$ is decidable.

MSO-formulas can be translated into "Büchi automata".

SECTION

I

MATHEMATICAL

LOGIC

Symposium on Decision Problems

ON A DECISION METHOD IN RESTRICTED SECOND ORDER ARITHMETIC

J. RICHARD BÜCHI

University of Michigan, Ann Arbor, Michigan, U.S.A.

Let SC be the interpreted formalism which makes use of individual variables t, x, y, z, . . . ranging over natural numbers, monadic predicate variables q( ), r( ), s( ), i( ), . . . ranging over arbitrary sets of natural numbers, the individual symbol 0 standing for zero, the function symbol ′ denoting the successor function, propositional connectives, and quantifiers for both types of variables. Thus SC is a fraction of the restricted second order theory of natural numbers, or of the first order theory of real numbers. In fact, if predicates on natural numbers are interpreted as binary expansions of real numbers, it is easy to see that SC is equivalent to the first order theory of [Re, +, Pw, Nn], whereby Re, Pw, Nn are, respectively, the sets of non-negative reals, integral powers of 2, and natural numbers.

The purpose of this paper is to obtain a rather complete understanding of definability in SC, and to outline an effective method for deciding truth

This work was done under a grant from the National Science Foundation to the Logic of Computers Group, and with additional assistance through contracts with the Office of Naval Research, Office of Ordnance Research, and the Army Signal Corps.

First Step: MSO over Finite Words

Words coded by Sets

Consider $w = \binom{0}{1}\binom{0}{0}\binom{0}{0}\binom{1}{1}\binom{1}{0}$

Domain of letter positions: $D = \{0, 1, 2, 3, 4\}$

For an infinite word this domain is $\mathbb{N}$.

w is identified with a pair of sets: $K_1 = \{3, 4\}$, $K_2 = \{0, 3\}$

A word over $\{0, 1\}^n$ with domain D can be identified with an n-tuple $(K_1, \ldots, K_n)$ of subsets of D.

A Definable Language

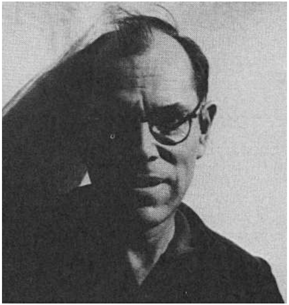
Consider the regular language L_0 over $\{0,1\}^2$ containing the words where

between any two letters $\binom{*}{1}$ there is a letter $\binom{0}{*}$

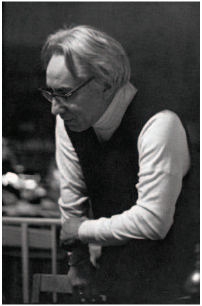
$w = \binom{0}{1}\binom{0}{0}\binom{0}{0}\binom{1}{1}\binom{1}{0}$ **satsfies this.**

$$\begin{aligned}\varphi(X_1, X_2) \;\; = \;\; & \forall x \forall y (x < y \wedge X_2(x) \wedge X_2(y) \;\rightarrow \\ & \quad \exists z\ (x < z \wedge z < y \wedge \neg X_1(z)))\end{aligned}$$

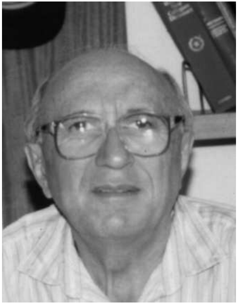
BET Theorem



J.R. Büchi



C.C. Elgot



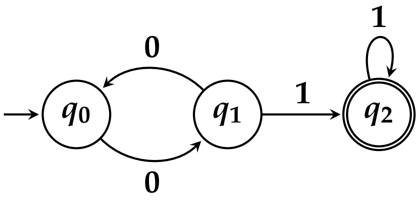
B.A. Trakhtenbrot

Theorem of Büchi-Elgot-Trakhtenbrot (1960):

Finite automata and monadic second-order fomulas can express the same properties of finite words.

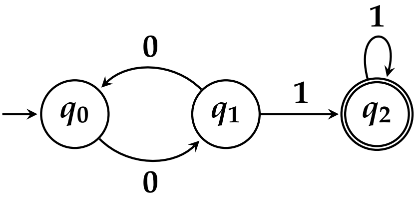
From Automata to MSO-Logic

$\mathcal{A}_0$:



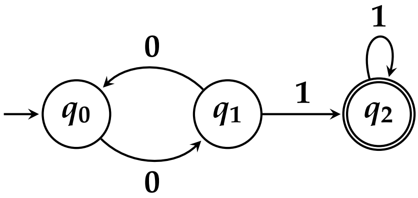
We look for an MSO-formula φ "equivalent" to $\mathcal{A}_0$

It should express over w that $\mathcal{A}_0$ accepts w.



An input word and an accepting run:

$$
\begin{array}{cccccc}
0 & 0 & 0 & 1 & 1 & \\
\begin{pmatrix}1\\0\\0\end{pmatrix} & \begin{pmatrix}0\\1\\0\end{pmatrix} & \begin{pmatrix}1\\0\\0\end{pmatrix} & \begin{pmatrix}0\\1\\0\end{pmatrix} & \begin{pmatrix}0\\0\\1\end{pmatrix} & \begin{pmatrix}0\\0\\1\end{pmatrix}
\end{array}
$$



$$
\begin{aligned}
&\varphi(X) := \\
&\exists Y_0 \exists Y_1 \exists Y_2 (\text{Partition}(Y_0, Y_1, Y_2) \wedge Y_0(\min) \\
&\qquad \wedge \forall x ((Y_0(x) \wedge \neg X(x) \wedge Y_1(x+1)) \\
&\qquad\qquad \vee (Y_1(x) \wedge \neg X(x) \wedge Y_0(x+1)) \\
&\qquad\qquad \vee (Y_1(x) \wedge X(x) \wedge Y_2(x+1)) \\
&\qquad\qquad \vee (Y_2(x) \wedge X(x) \wedge Y_2(x+1))) \\
&\qquad \wedge (Y_1(\max) \vee Y_2(\max)) \wedge X(\max))
\end{aligned}
$$

Preparing MSO for Easy Induction

Work with a dialect of MSO in which the first-order variables are cancelled.

Simulate x by a singleton variable $\{x\}$.

Atomic formulas: $X \subseteq Y$, Sing(X), Succ(X, Y), $X < Y$.

Example

$$\varphi(X_1, X_2) \;=\; \forall x \forall y (x < y \wedge X_2(x) \wedge X_2(y) \;\rightarrow\; \exists z \neg X_1(z))$$

$$\varphi'(X_1, X_2) \;=\; \forall X \forall Y (X < Y \wedge X \subseteq X_2 \wedge Y \subseteq X_2(y) \;\rightarrow$$

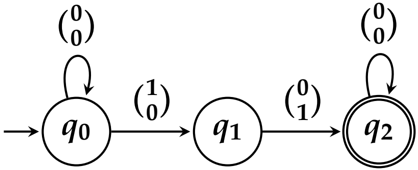
$$\exists Z(\mathrm{Sing}(Z) \wedge \neg Z \subseteq X_1))$$

Task: Find for any $\varphi(X_1, \ldots, X_n)$ a corresponding automaton over $\{0,1\}^n$.

From MSO to Automata (Finite Words)

Proceed by induction on formulas.

Example: $\mathrm{Succ}(X_1, X_2)$



Use nondeterministic automata:

Then atomic formulas, $\vee, \exists$ are easy.

For complementation use the subsetset construction to obtain a deterministic automaton which is easily complementable.

On Complexity

The number of states of finite automata for MSO-formulas of length n cannot be bounded by an elementary function in n (Stockmeyer, Meyer, STOC 1973)

Question: Is there a class of formulas sufficient for "practice" that escapes this non-elementary blow-up?

Some references:

Klaus Reinhardt: The Complexity of Translating Logic to Finite Automata, in: Automata, Logics, and Infinite Games, Springer LNCS 2500 (2001) 231-238.

David A. Basin, Nils Klarlund: Hardware Verification using Monadic Second-Order Logic. CAV 1995: 31-41.

Christos A. Kapoutsis, Nans Lefebvre: Analogs of Fagin's Theorem for Small Nondeterministic Finite Automata. Developments in Language Theory 2012: 202-213

Büchi Automata

Definition

A Büchi automaton (NBA) has the form $\mathcal{A} = (Q, \Sigma, q_0, \Delta, F)$ with

- finite state-set Q, initial state q_0, set $F \subseteq Q$ of final states,
- transition relation $\Delta \subseteq Q \times \Sigma \times Q$

$\mathcal{A}$ accepts the input word $\alpha \in \Sigma^\omega$ if there is a run ϱ of $\mathcal{A}$ on α such that $\exists^\omega i \; \varrho(i) \in F$

$L(\mathcal{A}) := \{\alpha \in \Sigma^\omega \mid \mathcal{A} \text{ accepts } \alpha\}$
is the ω-language recognized by $\mathcal{A}$.

L is called Büchi recognizable if $L = L(\mathcal{A})$ for some Büchi automaton $\mathcal{A}$.

Büchi's Version of "Büchi Automaton"

$$\Sigma_1^\omega : (\exists r) \cdot A[r(0)] \wedge \forall t\ B[i(t), r(t), r(t')] \wedge (\exists^\omega t)\ C[r(t)]$$

This formula type is motivated by a representation of Σ_1^1-sets in the Cantor space.

Büchi showed closure properties of this formula class and derived that this is a normal form of formulas of S1S.

This was new kind of "quantifier elimination".

Periodicity

Given $\mathcal{A} = (Q, \Sigma, q_0, \Delta, F)$ define

$W_{pq} = \{w \in \Sigma^* \mid \mathcal{A} : p \xrightarrow{w} q\}$

Then $L(\mathcal{A}) \; = \; \bigcup_{q \in F} \; W_{q_0 q} \cdot (W_{q,q})^\omega$

An ω-language is Büchi recognizable iff it is a finite union of ω-languages $U \cdot V^\omega$ with regular $U, V \subseteq \Sigma^*$

Consequence: A nonempty Büchi-recognizable ω-language contains an ultimately periodic ω-word.

Büchi's Theorem

An ω-language is MSO-definable iff it is Büchi recognizable

- From automata to MSO: as over finite words.
- From MSO to automata: Proceed again by induction.
  Only complementation is difficult.

Complementation

Idea: Represent also the complement-ω-language as a finite union of sets $U \cdot V^\omega$ with regular U, V.

As U, V use equivalence classes of an equivalence relation:

$$u \sim_{\mathcal{A}} v \;\; :\Leftrightarrow \mathcal{A} : p \xrightarrow{u} q \Leftrightarrow \mathcal{A} : p \xrightarrow{v} q$$

$$\text{and } \mathcal{A} : p \xrightarrow{u} q \text{ via } F \;\Leftrightarrow\; \mathcal{A} : p \xrightarrow{v} q \text{ via } F$$

This is an equivalence relation of finite index.

The $\sim_{\mathcal{A}}$-class of u is captured by two lists of edges (p, q):

- **those (p, q) with $\mathcal{A} : p \xrightarrow{u} q$**
- **those (p, q) with $\mathcal{A} : p \xrightarrow{u} q$ via F**

Each $\sim_{\mathcal{A}}$-class is regular!

A Crucial Property

Assume $\alpha \in U \cdot V^\omega \cap L(\mathcal{A})$, where U, V are $\sim_\mathcal{A}$-classes.

Then $U \cdot V^\omega \subseteq L(\mathcal{A})$.

By assumption we have:

$\mathcal{A} : q_0 \xrightarrow{u} p_1 \xrightarrow{v_1} p_2 \xrightarrow{v_2} p_3 \xrightarrow{v_3} \ldots$ **with** $u \in U, v_i \in V$
where via infinitely many v_i a final state is passed.

Consider $\beta = u'v_1'v_2'v_3' \ldots$ in $U \cdot V^\omega$ with $u' \in U, v_i' \in V$.

Apply $u \sim_\mathcal{A} u'$ and $v_i \sim_\mathcal{A} v_i'$:

$$\mathcal{A} : q_0 \xrightarrow{u'} p_1 \xrightarrow{v_1'} p_2 \xrightarrow{v_2'} p_3 \xrightarrow{v_3'} \ldots$$

where via infinitely many v_i' a final state is passed.

Last Missing Step

We want to show:

$$\overline{L(\mathcal{A})} = \bigcup \{U \cdot V^\omega | U \cdot V^\omega \cap L(\mathcal{A}) = \emptyset\}$$

Missing step: Show that each α belongs to some $U \cdot V^\omega$ where U, V are $\sim_\mathcal{A}$-classes.

Ramsey's Theorem: Given a coloring of all pairs (i, j) of natural numbers with $i < j$, there is an infinite "homogeneous" set $H \subseteq \mathbb{N}$ and a fixed color c such that each pair (i, j) with $i, j \in H, i < j$ is colored with c.

Take as color for (i, j) the $\sim_\mathcal{A}$-class of $\alpha[i, j)$

Consequences

1. **The MSO-theory of $(\mathbb{N}, +1, 0)$ is decidable.**
   Proof: Transform a sentence φ into a Büchi automaton over $\{0,1\}^0$ (i.e. with unlabelled transitions) and check whether there is a reachable $q \in F$ with a loop back to q.

2. **MSO-formulas over $(\mathbb{N}, +1, 0)$ can be rewritten as EMSO-formulas.**

3. **Model checking:**
   Check whether for each path of a transition system $\mathcal{S}$ a formula φ holds.
   Check whether the intersection automaton of $\mathcal{S}$ and $\mathcal{A}_{\neg\varphi}$ accepts some ω-word.

Determinization

Deterministic Büchi Automata (DBA)

are of the form $\mathcal{A} = (Q, \Sigma, q_0, \delta, F)$ with $\delta : Q \times \Sigma \to Q$

$\mathcal{A}$ accepts α if its unique run on α visits F infinitely often.

This means: The DFA $\mathcal{A}$ accepts infinitely many prefixes of α

Let $\varphi(X_1, \ldots, X_n)$ be a formula equivalent to the DFA $\mathcal{A}$

Modify $\varphi(X_1, \ldots, X_n)$ to a formula $\varphi'(X_1, \ldots, X_n, y)$ saying "the segment up to position y satisfies φ"

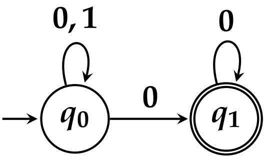
Then the DBA $\mathcal{A}$ is equivalent to the formula

$\forall x \exists y \ (x < y \land \varphi'(X_1, \ldots, X_n, y))$ where φ' is bounded in y.

So: DBA-recognizable ω-languages are Π^0_2-sets of the Borel hierarchy (as opposed to Σ^1_1 sets for NBA).

Weakness of DBA

Consider the ω-language $(0+1)^*0^\omega$, recognized by an NBA:



Assume the DBA $\mathcal{A}$ recognizes $(0+1)^*0^\omega$.

- **Reading 0^ω it will reach a final state after 0^{n_0}**
- **Reading $0^{n_0}10^\omega$ it will reach a final state after $0^{n_0}10^{n_1}$**
- **etc.**

So on $0^{n_0}10^{n_1}10^{n_2}1\ldots$ $\mathcal{A}$ will visit final states infinitely often, contradiction.

Muller Automata

are a form of ω-automata that recognize the Boolean combinations of DBA-recognizable sets.

Format: $\mathcal{A} = (Q, \Sigma, q_0, \delta, \mathcal{F})$
with $\delta : Q \times \Sigma \to Q$, $\mathcal{F} = \{F_1, \dots, F_k\}$ **where** $F_i \subseteq Q$

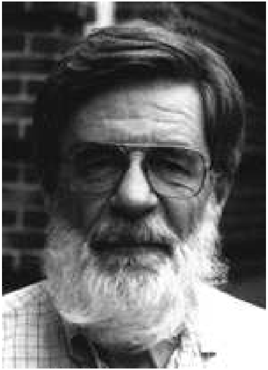
Acceptance: $\mathcal{A}$ **accepts** α **iff for the unique run** ϱ **we have**

$$\bigvee_{i=1}^{k} \Big(\bigwedge_{q \in F_i} \exists^\omega m\ \varrho(m) = q \wedge \bigwedge_{q \in Q \setminus F_i} \neg \exists^\omega m\ \varrho(m) = q \Big)$$

Write $\mathcal{A}_q$ **for the det. Büchi automaton** $(Q, \Sigma, q_0, \delta, \{q\})$**.**

$$L(\mathcal{A}) = \bigcup_{i=1}^{k} \Big(\bigcap_{q \in F_i} L(\mathcal{A}_q) \cap \bigcap_{q \in Q \setminus F_i} \overline{L(\mathcal{A}_q)} \Big)$$

McNaughton's Theorem



R. McNaughton (1924 - 2014)

Each Büchi automaton an be transformed into a (deterministic) Muller automaton.

Constructions of Automata

- **Muller (1963), with a flaw**
- **McNaughton (1966)**
- **Choueka (1974)**
- **Safra (1988)**
  with optimal growth rate $2^{O(n \log n)}$ for number of states
- **Muller and Schupp (1995)**
- **Fogharty, Kähler, Vardi, Wilke (2013)**

One can give a more abstract and “conceptual” proof (Ths., Inf and Control 1981), avoiding “programming”.

McNaughton's Theorem Logically

The ω-language defined by a Büchi automaton can be defined by a Boolean combination of formulas

$\forall x \exists y (x < y \wedge \varphi(y))$ **where** $\varphi(y)$ **is bounded in** y

In logical terminology we are reducing a Σ^1_1-statement to a Boolean combination of Π^0_2-statements.

In other words: The Büchi recognizable ω-languages are all included in a low level of the Borel hierarchy (of the Cantor space).

Three Problems

Problem 1. Let SC^2 be like SC, except that the functions $2x+1$ and $2x+2$ are taken as primitives in place of $x+1$. Is SC^2 decidable?

This is of some interest, because the functions $2x+1$ and $2x+2$ can be interpreted as the right-successor functions x1 and x2 on the set of all words on two generators 1 and 2.

Problem 2. Let $SC(\alpha)$ be like SC, except that the domain of individuals is the ordinal α, and the well ordering on α is added as a primitive. Is $SC(\omega^2)$ decidable?

As outlined in the introduction, Theorem 2 may be interpreted as a method for deciding whether or not a given finite automaton satisfies a given condition in SC.

Problem 3. Is there a solvability algorithm for SC, i.e., is there a method which applies to any formula $C(\mathbf{i}, \mathbf{u})$ of SC and decides whether or not there is a finite automata recursion $A(\mathbf{i}, \mathbf{r}, \mathbf{u})$ which satisfies the condition C (i.e., $A(\mathbf{i}, \mathbf{r}, \mathbf{u}) \supset C(\mathbf{i}, \mathbf{u})$)?