Automata and Logic

Aart Middeldorp and Samuel Frontull

Outline

Definition

formulas of Presburger arithmetic

$$\varphi \ ::= \ \bot \mid \neg\varphi \mid \varphi_1 \vee \varphi_2 \mid \exists\, x.\, \varphi \mid t_1 = t_2 \mid t_1 < t_2$$

$$t \ ::= \ 0 \mid 1 \mid t_1 + t_2 \mid x$$

Abbreviations

$$\varphi \wedge \psi \ := \ \neg(\neg\varphi \vee \neg\psi) \qquad \varphi \to \psi \ := \ \neg\varphi \vee \psi \qquad \top \ := \ \neg\bot$$

$$\forall\, x.\, \varphi \ := \ \neg\exists\, x.\, \neg\varphi \qquad t_1 \leqslant t_2 \ := \ t_1 < t_2 \vee t_1 = t_2$$

$$\mathrm{n} \ := \ \underbrace{1 + \cdots + 1}_{n} \qquad \mathrm{n}\, x \ := \ \underbrace{x + \cdots + x}_{n} \quad \text{for } n > 1$$

Definitions

- assignment α is mapping from first–order variables to $\mathbb{N}$
- extension to terms: $\alpha(0) = 0 \qquad \alpha(1) = 1 \qquad \alpha(t_1 + t_2) = \alpha(t_1) + \alpha(t_2)$

Definition

assignment α satisfies formula φ ($\alpha \vDash \varphi$):

$$
\begin{array}{lcl}
\alpha \nvDash \bot & & \\
\alpha \vDash \neg\varphi & \iff & \alpha \nvDash \varphi \\
\alpha \vDash \varphi_1 \vee \varphi_2 & \iff & \alpha \vDash \varphi_1 \text{ or } \alpha \vDash \varphi_2 \\
\alpha \vDash \exists x.\, \varphi & \iff & \alpha[x \mapsto n] \vDash \varphi \text{ for some } n \in \mathbb{N} \\
\alpha \vDash t_1 = t_2 & \iff & \alpha(t_1) = \alpha(t_2) \\
\alpha \vDash t_1 < t_2 & \iff & \alpha(t_1) < \alpha(t_2)
\end{array}
$$

Remark

every $t_1 = t_2$ can be written as $a_1x_1 + \cdots + a_nx_n = b$ with $a_1, \ldots, a_n, b \in \mathbb{Z}$

Theorem (Presburger 1929)

Presburger arithmetic is decidable

Decision Procedures

- quantifier elimination
- automata techniques
- translation to WMSO

Definition (Representation)

- sequence of n natural numbers is represented as string over

$$\Sigma_n = \{(b_1 \cdots b_n)^\mathsf{T} \mid b_1, \ldots, b_n \in \{0,1\}\}$$

- $x = \begin{pmatrix} b_1^1 \\ \vdots \\ b_n^1 \end{pmatrix} \begin{pmatrix} b_1^2 \\ \vdots \\ b_n^2 \end{pmatrix} \cdots \begin{pmatrix} b_1^m \\ \vdots \\ b_n^m \end{pmatrix} \in \Sigma_n^*$ represents $x_1 = (b_1^m \cdots b_1^2 b_1^1)_2, \ldots, x_n = (b_n^m \cdots b_n^2 b_n^1)_2$
- $\underline{x} = (x_1, \ldots, x_n)$

Definition

for Presburger arithmetic formula φ with $\mathrm{FV}(\varphi) = (x_1, \ldots, x_n)$

$$L(\varphi) = \{x \in \Sigma_n^* \mid \underline{x} \vDash \varphi\}$$

Theorem (Presburger 1929)

Presburger arithmetic is decidable

Proof Sketch

- construct finite automaton A_φ for every Presburger arithmetic formula φ
- induction on φ
- $L(A_\varphi) = L(\varphi)$

Definition (Automaton for Atomic Formula)

finite automaton $A_\varphi = (Q, \Sigma_n, \delta, s, F)$ for $\varphi(x_1, \dots, x_n)$: $a_1x_1 + \cdots + a_nx_n = b$

- $Q \subseteq \{i \mid |i| \leqslant |b| + |a_1| + \cdots + |a_n|\} \cup \{\bot\}$
- $\delta(i, (b_1 \cdots b_n)^\mathsf{T}) = \begin{cases} \dfrac{i - (a_1b_1 + \cdots + a_nb_n)}{2} & \text{if } i - (a_1b_1 + \cdots + a_nb_n) \text{ is even} \\ \bot & \text{if } i - (a_1b_1 + \cdots + a_nb_n) \text{ is odd or } i = \bot \end{cases}$
- $s = b$
- $F = \{0\}$

Lemma

if $\delta(i, (b_1 \cdots b_n)^\mathsf{T}) = j$ then $a_1x_1 + \cdots + a_nx_n = j \iff a_1(2x_1 + b_1) + \cdots + a_n(2x_n + b_n) = i$

Theorem

- A_φ is well–defined
- $L(A_\varphi) = L(\varphi)$

Boolean Operations

boolean operation	automata construction	
$\neg$	complement	C
$\wedge$	intersection	I
$\vee$	union	U

Definition (Cylindrification)

$\mathsf{C}_i(R) \subseteq \Sigma_{n+1}^*$ is defined for $R \subseteq \Sigma_n^*$ and index $1 \leqslant i \leqslant n+1$ as

$$\mathsf{C}_i(R) = \left\{ x_1 \cdots x_m \in \Sigma_{n+1}^* \;\middle|\; \mathsf{drop}_i(x_1) \cdots \mathsf{drop}_i(x_m) \in R \right\}$$

with $\mathsf{drop}_i\big((b_1 \cdots b_{n+1})^\mathsf{T}\big) = (b_1 \cdots b_{i-1} b_{i+1} \cdots b_{n+1})^\mathsf{T}$

Lemma

if $R \subseteq \Sigma_n^*$ is regular then $\mathsf{C}_i(R) \subseteq \Sigma_{n+1}^*$ is regular for every $1 \leqslant i \leqslant n+1$

Definition (Projection)

$\Pi_i(R) \subseteq \Sigma_n^*$ is defined for $R \subseteq \Sigma_{n+1}^*$ and index $1 \leqslant i \leqslant n+1$ as

$$\Pi_i(R) = \{\mathrm{drop}_i(x_1) \cdots \mathrm{drop}_i(x_m) \in \Sigma_n^* \mid x_1 \cdots x_m \in R\}$$

Lemma

if $R \subseteq \Sigma_{n+1}^*$ is regular then $\Pi_i(R) \subseteq \Sigma_n^*$ is regular for every $1 \leqslant i \leqslant n+1$

Translation from Presburger Arithmetic to WMSO

- map variables in Presburger arithmetic formula to second−order variables in WMSO
- n is represented as set of "1" positions in reverse binary notation of n
- 0 and 1 in Presburger arithmetic formulas are translated into ZERO and ONE with

$$\forall x.\, \neg \mathrm{ZERO}(x) \qquad\qquad \forall x.\, \mathrm{ONE}(x) \leftrightarrow x = 0$$

- $+$ in Presburger arithmetic formula is translated into ternary predicate P_+ with

$$\begin{aligned} P_+(X,Y,Z) \;:=\; \exists\, C.\, \neg C(0) \wedge {} & \big(\forall x.\, C(x+1) \leftrightarrow X(x) \wedge Y(x) \vee X(x) \wedge C(x) \vee Y(x) \wedge C(x)\big) \wedge \\ & \big(\forall x.\, Z(x) \leftrightarrow X(x) \wedge Y(x) \wedge C(x) \vee X(x) \wedge \neg Y(x) \wedge \neg C(x) \vee \\ & \qquad \neg X(x) \wedge Y(x) \wedge \neg C(x) \vee \neg X(x) \wedge \neg Y(x) \wedge C(x)\big) \end{aligned}$$

Automata

- (deterministic, nondeterministic, alternating) finite automata
- regular expressions
- (alternating) Büchi automata

Logic

- (weak) monadic second–order logic
- Presburger arithmetic
- linear–time temporal logic

Outline

Definitions

- infinite string over alphabet Σ is function $x\colon \mathbb{N} \to \Sigma$
- Σ^ω denotes set of all infinite strings over Σ
- $|x|_a$ for $x \in \Sigma^\omega$ and $a \in \Sigma$ denotes number of occurrences of a in x

Example

$$x(i) = \begin{cases} a & \text{if } i \text{ is even} \\ b & \text{if } i \text{ is odd} \end{cases} \qquad x = ababab\cdots = (ab)^\omega$$

Remarks

- infinite string x is identified with infinite sequence $x(0)x(1)x(2)\cdots$
- $|x|_a = \infty$ for at least one $a \in \Sigma$

Definitions

- left–concatenation of $u \in \Sigma^*$ and $v \in \Sigma^\omega$ is denoted by $u \cdot v \in \Sigma^\omega$
- left–concatenation of $U \subseteq \Sigma^*$ and $V \subseteq \Sigma^\omega$

$$U \cdot V = \{u \cdot v \mid u \in U \text{ and } v \in V\}$$

- $\sim V = \Sigma^\omega - V$ is complement of $V \subseteq \Sigma^\omega$
- $U^\omega = \{u_0 \cdot u_1 \cdot \cdots \mid u_i \in U - \{\epsilon\} \text{ for all } i \in \mathbb{N}\}$ is ω–iteration of $U \subseteq \Sigma^*$

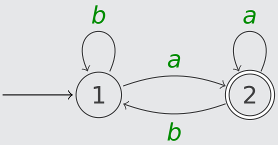
Outline

Definitions

- nondeterministic Büchi automaton (NBA) is NFA $M = (Q, \Sigma, \Delta, S, F)$ operating on Σ^ω
- run of M on input $x = a_0 a_1 a_2 \cdots \in \Sigma^\omega$ is infinite sequence $q_0, q_1, \ldots$ of states such that $q_0 \in S$ and $q_{i+1} \in \Delta(q_i, a_i)$ for $i \geqslant 0$
- run $q_0, q_1, \ldots$ is accepting if $q_i \in F$ for infinitely many i
- $L(M) = \{x \in \Sigma^\omega \mid x \text{ admits accepting run}\}$

Example

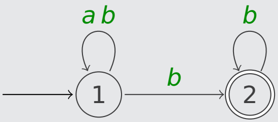
- NBA M



- $(ab)^\omega \in L(M)$
- $aab^\omega \notin L(M)$
- $L(M) = \{x \in \{a, b\}^\omega \mid |x|_a = \infty\}$

Example

- NBA M



- $L(M) = \{x \in \{a, b\}^\omega \mid |x|_a \neq \infty\} = (a + b)^* b^\omega$
- M is not deterministic

Definitions

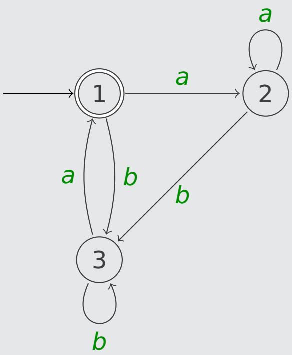
- set $A \subseteq \Sigma^\omega$ is **ω–regular** if $A = L(M)$ for some NBA M
- **deterministic Büchi automaton** (**DBA**) is NBA $(Q, \Sigma, \Delta, S, F)$ with

  ① $|S| = 1$

  ② $|\Delta(q, a)| = 1$ for all $q \in Q$ and $a \in \Sigma$

Example

$\{x \in \{a, b\}^\omega \mid |x|_a = |x|_b = \infty\}$ is accepted by DBA



Theorem

not every ω–regular set is accepted by DBA

Proof

$L = \{x \in \{a,b\}^\omega \mid |x|_a \neq \infty\}$ is ω–regular but not accepted by DBA:

- suppose $L = L(M)$ for DBA $M = (Q,\Sigma,\Delta,S,F)$

  $x_0 = b^\omega \in L \implies \exists$ accepting run $q_0, q_1, \dots \implies \exists\, i_0 \geqslant 0$ with $q_{i_0} \in F$

  $x_1 = b^{i_0} a b^\omega \in L \implies \exists$ accepting run $q_0, q_1, \dots \implies \exists\, i_1 > i_0 + 1$ with $q_{i_1} \in F$

  let $l_1 = i_1 - i_0 - 1$

  $x_2 = b^{i_0} a b^{l_1} a b^\omega \in L \implies \exists$ accepting run $q_0, q_1, \cdots \implies \exists\, i_2 > i_1 + 1$ with $q_{i_2} \in F$

  $\dots$

  $\exists\, j < k$ such that $q_{i_j} = q_{i_k}$

- $x = b^{i_0} a b^{l_1} \cdots a b^{l_j} (a b^{l_j+1} \cdots a b^{l_k})^\omega$ admits accepting run but $x \notin L$ ↯

Lemma

every ω–regular set is accepted by NBA with one start state

Proof

- $A = L(M)$ for NBA $M = (Q, \Sigma, \Delta, S, F)$
- define NBA $N = (Q', \Sigma, \Delta', \{s\}, F)$ with $Q' = Q \uplus \{s\}$ and

$$\Delta'(p, a) = \begin{cases} \Delta(p, a) & \text{if } p \neq s \\ \{q \in Q \mid q \in \Delta(p', a) \text{ for some } p' \in S\} & \text{if } p = s \end{cases}$$

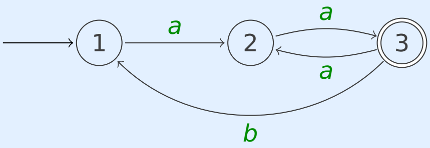
- $L(N) = A$:

$$\begin{aligned} x \in A \quad & \iff \quad \exists \text{ run } q_0, q_1, q_2, \dots \text{ in } M \text{ with } q_0 \in S \text{ and } q_i \in F \text{ for infinitely many } i \geqslant 0 \\ & \iff \quad \exists \text{ run } q_0, q_1, q_2, \dots \text{ in } M \text{ with } q_0 \in S \text{ and } q_i \in F \text{ for infinitely many } i > 0 \\ & \iff \quad \exists \text{ run } s, q_1, q_2, \dots \text{ in } N \text{ with } q_i \in F \text{ for infinitely many } i > 0 \\ & \iff \quad x \in L(N) \end{aligned}$$

Outline

Question

Which statement about the following NBA M is true ?



A $L(M) = \varnothing$

B $(b^*aa)^\omega \in L(M)$

C $L(M) = \{x \mid |x|_a = \infty \text{ and } |x|_b \neq \infty\}$

D $L(M) = \{x \in \{a,b\}^\omega \mid \text{every } b \text{ follows an even number of } a\text{'s}\}$

Outline

Theorem

ω–regular sets are effectively closed under union

Proof (construction)

- $A = L(M_1)$ for NBA $M_1 = (Q_1, \Sigma, \Delta_1, S_1, F_1)$
  $B = L(M_2)$ for NBA $M_2 = (Q_2, \Sigma, \Delta_2, S_2, F_2)$
- without loss of generality $Q_1 \cap Q_2 = \varnothing$
- $A \cup B = L(M)$ for NBA $M = (Q, \Sigma, \Delta, S, F)$ with
  1. $Q = Q_1 \cup Q_2$
  2. $S = S_1 \cup S_2$
  3. $F = F_1 \cup F_2$
  4. $\Delta(q, a) = \begin{cases} \Delta_1(q, a) & \text{if } q \in Q_1 \\ \Delta_2(q, a) & \text{if } q \in Q_2 \end{cases}$

Theorem

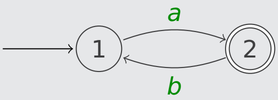
ω–regular sets are effectively closed under intersection

Remark

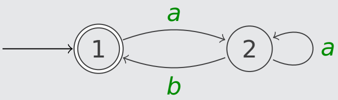
product construction needs to be modified

Example

M_1 :

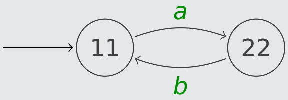


M_2 :



$L(M_1) = a(ba)^\omega = (ab)^\omega$ $\quad L(M_2) = (aa^*b)^\omega$ $\quad L(M_1) \cap L(M_2) = (ab)^\omega$

$M_1 \times M_2$:



Theorem

ω–regular sets are effectively closed under intersection

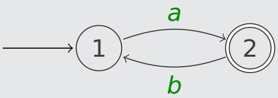
Proof (modified product construction)

- $A = L(M_1)$ for NBA $M_1 = (Q_1, \Sigma, \Delta_1, S_1, F_1)$ and $B = L(M_2)$ for NBA $M_2 = (Q_2, \Sigma, \Delta_2, S_2, F_2)$
- $A \cap B = L(M)$ for NBA $M = (Q, \Sigma, \Delta, S, F)$ with
  1. $Q = Q_1 \times Q_2 \times \{0, 1, 2\}$
  2. $S = S_1 \times S_2 \times \{0\}$
  3. $F = Q_1 \times Q_2 \times \{2\}$
  4. $\Delta((p, q, i), a) = \{(p', q', j) \mid p' \in \Delta_1(p, a) \text{ and } q' \in \Delta_2(q, a)\}$ with

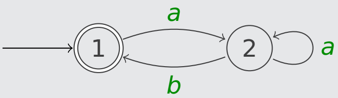
$$j = \begin{cases} 1 & \text{if } i = 0 \text{ and } p' \in F_1 \text{ or } i = 1 \text{ and } q' \notin F_2 \\ 2 & \text{if } i = 1 \text{ and } q' \in F_2 \\ 0 & \text{otherwise} \end{cases}$$

Example

$M_1:$

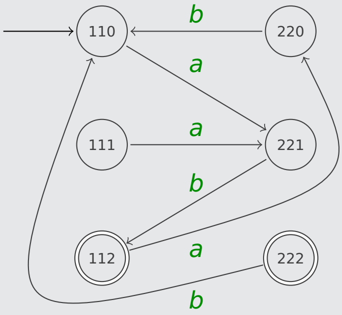


$M_2:$



$$L(M_1) = a(ba)^\omega = (ab)^\omega \qquad L(M_2) = (aa^*b)^\omega \qquad L(M_1) \cap L(M_2) = (ab)^\omega$$

$M:$



Theorem

left–concatenation of regular set and ω–regular set is ω–regular

Proof (construction)

- $A = L(M_1)$ for NFA $M_1 = (Q_1, \Sigma, \Delta_1, S_1, F_1)$ and $B = L(M_2)$ for NBA $M_2 = (Q_2, \Sigma, \Delta_2, S_2, F_2)$
- without loss of generality $Q_1 \cap Q_2 = \varnothing$
- $A \cdot B = L(M)$ for NBA $M = (Q, \Sigma, \Delta, S, F)$ with

  ① $Q = Q_1 \cup Q_2$

  ② $S = \begin{cases} S_1 & \text{if } F_1 \cap S_1 = \varnothing \\ S_1 \cup S_2 & \text{otherwise} \end{cases}$

  ③ $F = F_2$

  ④ $\Delta = \Delta_1 \cup \Delta_2 \cup \{(p, a, q) \mid (p, a, f) \in \Delta_1 \text{ for some } f \in F_1 \text{ and } q \in S_2\}$

Theorem

ω–iteration of regular set is ω–regular

Proof (construction)

- $A = L(M)$ for NFA $M = (Q, \Sigma, \Delta, S, F)$
- without loss of generality $\epsilon \notin A$
- NFA $M' = (Q \cup \{s\}, \Sigma, \Delta', \{s\}, F)$ with

$$\Delta' = \Delta \cup \{(s, a, q) \mid (p, a, q) \in \Delta \text{ for some } p \in S\}$$

- $L(M') = L(M)$
- NBA $M'' = (Q \cup \{s\}, \Sigma, \Delta'', \{s\}, \{s\})$ with

$$\Delta'' = \Delta' \cup \{(p, a, s) \mid (p, a, q) \in \Delta' \text{ for some } q \in F\}$$

- $L(M'') = L(M')^\omega$

Theorem

set $A \subseteq \Sigma^\omega$ is ω–regular $\iff$ $A = U_1 \cdot V_1^\omega \cup \cdots \cup U_n \cdot V_n^\omega$ for some $n \geqslant 0$ and regular $U_1, \dots, U_n, V_1, \dots, V_n \subseteq \Sigma^*$

Proof ($\Longleftarrow$)

A is ω–regular using closure properties: ω–iteration, left–concatenation, union

Proof ($\Longrightarrow$)

- $A = L(M)$ for some NBA $M = (Q, \Sigma, \Delta, S, F)$
- L_{pq} for $p, q \in Q$ is set of strings $x \in \Sigma^*$ such that $q \in \widehat{\Delta}(\{p\}, x)$
- L_{pq} is regular for all $p, q \in Q$
- $A = \displaystyle\bigcup_{p \in S,\, q \in F} L_{pq} \cdot L_{qq}^\omega$

Outline

Hofmann and Lange

- Chapter 5 of Automatentheorie und Logik (Springer 2011)

Esparza and Blondin

- Chapter 10 of Automata Theory: An Algorithmic Approach (MIT Press 2023)

Important Concepts

- Büchi automaton
- left−concatenation
- NBA
- ω−iteration
- DBA
- Σ^ω
- ω−regular

homework for November 28