Regularity Preserving Functions

Presented By:
Priyanka Bhatt & Surabhi Punjabi

Department of Computer Science and Automation (CSA),
Indian Institute of Science (IISc), Bangalore.

Nov 26, 2013

Overview

Motivation

Show that if A is a regular set, then so is

$$FirstHalves(A) = \{x | \exists y, | y | = | x | \text{ and } xy \in A\}$$

Can be proved using pebbling technique or using a product automaton.

Some more examples

Show that if A is a regular set, then so are the following:

$$A_{n^2} = \{x \mid \exists y, \mid y \mid = \mid x \mid^2 \ and \ xy \in A\}$$

$$A_{2^n} = \{x \mid \exists y, \mid y \mid = 2^{|x|} and \ xy \in A\}$$

$$A_{2^{2^n}} = \{x \mid \exists y, \mid y \mid = 2^{2^{|x|}} and \ xy \in A\}$$

Presence of **non linear functions** makes regularity counter-intuitive.

Boolean Transition Matrix

For automaton A = (Q,Σ,s,δ, F)
Boolean Transition Matrix Δ is a $\mid Q \mid \times \mid Q \mid$ matrix where

$$\Delta(u, v) = \begin{cases} 1 & \text{if } \exists a \in \Sigma \text{ s.t.} \delta(u, a) = v \\ 0, & \text{otherwise} \end{cases}$$

Power Δ^n gives the n-step transition relations.

Example1

A_{2^n}

- Create a Boolean transition matrix $\triangle$ (as described).
- Basic problem to be solved in this : How to get $\triangle^{2^{n+1}}$ from $\triangle^{2^n}$?
- Observe that $\triangle^{2^{(n+1)}} = \triangle^{2^n} * \triangle^{2^n}$.
- $\therefore$ Maintain $\triangle$ matrix in the start state.
- As input is scanned, the successive state gets updated matrix, $(C) \rightarrow (C * C)$
- $\therefore$ In n steps, $(I) \xrightarrow{n} (\triangle^{2^n})$
- If $\widehat{\delta}(s, x) =$ p, then accept if $C($p,f$) = 1$ for any $f \in F$. Reject otherwise.

Example2

A_{n^2}

- Create a Boolean transition matrix $\triangle$ (as described).
- Basic problem to be solved in this : How to get $\triangle^{(n+1)^2}$ from $\triangle^{(n)^2}$?
- Now, $\triangle^{(n+1)^2} = \triangle^{n^2}\triangle^{2n}\triangle$.
- $\therefore$ Maintain (I, I) matrices in start state.
- As input is scanned, the successive state gets updated matrices $(C, D) \rightarrow (CD\triangle, D\triangle^2)$
- $\therefore$ In n steps, $(I, I) \xrightarrow{n} (\triangle^{n^2}, \triangle^{2n})$
- If $\widehat{\delta}(s, x) =$ p, then accept if $C($p,f$) = 1$ for any $f \in F$. Reject otherwise.

Overview

Regularity Preserving Functions

- General class of functions for which the following theorem holds. If A is regular, then so is

$$A_f = \{x \mid \exists y \mid y \mid = f(\mid x \mid) \text{ and } xy \in A\}$$

- The class is closed under addition, multiplication, exponentiation, composition and contains arbitrarily fast growing functions.
- Next, we look at the how to characterize this class in terms of the concept of ultimate periodicity.

Overview

Ultimate Periodicity

Definition 1

A set $U \subseteq N$ is called *ultimately periodic (u.p.)* (or *semilinear*) if
$\exists p \geqslant 1 \quad \overset{\infty}{\forall} n \quad n \in U \longleftrightarrow n + p \in U.$
More generally, a function $f : N \rightarrow N$ is called *ultimately periodic* if
$\exists p \geqslant 1 \quad \overset{\infty}{\forall} n \quad f(n) = f(n + p).$

$\overset{\infty}{\forall}$ means "for all but finitely many".
An example of a u.p. set is $[k]_m$, the congruence class of k modulo m

$$[k]_m = \{n | \text{n modulo m} = \text{k}\}$$

Properties of Ultimately Periodic Sets

Family of u.p. sets is closed under boolean operations.

- If U,V are u.p. with periods p, q respectively, then U $\bigcup$ V is u.p. with period lcm(p,q).
- For any regular set A, the set lengths(A) is u.p.
- For a u.p. set U, the set $\{x \mid \mid x \mid \in U\}$ is regular.

Definition 2

A function $f : N \to N$ is said to *preserve ultimate periodicity* if $f^{-1}(\mathrm{U})$ is u.p. whenever U is.

Definition 3

A function $f : N \to N$ is said to be *ultimately periodic modulo m*(u.p. mod m) if the function n $\mapsto f(n)$ mod m is ultimately periodic.

Conditions

- **C1 :** A_f is regular whenever A is.
- **C2 :** A'_f is regular whenever A is.
- **C3 :** f preserves ultimate periodicity.
- **C4 :**
  1. f is ultimately periodic modulo m for all $m \geqslant 1$; and
  2. $f^{-1}(\{x\})$ is ultimately periodic for all $x \in N$

$$A_f = \{x \mid \exists y \mid y \mid = f(\mid x \mid) \text{ and } xy \in A\}$$

$$A_{f'} = \{x \mid \exists y \mid y \mid = f(\mid x \mid) \text{ and } y \in A\}$$

Lemma 1

Lemma 1 The statement **C4** (i) is equivalent to the statement that $f^{-1}([i]_m)$ is ultimately periodic for all i and m.

Proof.

For all m,

$$f^{-1}([i]_m) \text{is u.p., } 0 \leqslant i \leqslant m-1$$

$$\longleftrightarrow \bigwedge_{i=0}^{m-1} \exists p_i \geqslant 1 \;\; f^{-1}([i]_m) \text{is u.p. with period } p_i$$

$$\longleftrightarrow \exists p \geqslant 1 \bigwedge_{i=0}^{m-1} f^{-1}([i]_m) \text{ is u.p. with period p (take p} = \text{lcm}_i \; p_i)$$

$$\longleftrightarrow \exists p \geqslant 1 \bigwedge_{i=0}^{m-1} \overset{\infty}{\forall} n \;\; n \in f^{-1}([i]_m) \longleftrightarrow n+p \in f^{-1}([i]_m)$$

Proof contd..

$$\longleftrightarrow \exists p \geqslant 1 \bigwedge_{i=0}^{m-1} \overset{\infty}{\forall} n \;\; f(n) \in [i]_m \longleftrightarrow f(n+p) \in [i]_m$$

$$\longleftrightarrow \exists p \geqslant 1 \overset{\infty}{\forall} n \bigwedge_{i=0}^{m-1} f(n) \in [i]_m \longleftrightarrow f(n+p) \in [i]_m$$

$$\longleftrightarrow \exists p \geqslant 1 \overset{\infty}{\forall} n \; f(n) = f(n+p) \bmod m$$

$\longleftrightarrow f$ is u.p. modulo m.

Theorem

Theorem

The four conditions **C1** - **C4** are equivalent.

Proof. (**C1** → **C4**) To show **C4**(i), let $0 \leqslant k \leqslant m-1$, and consider the regular set $(a^m)^*a^k$. We have

$$\begin{aligned} ((a^m)^*a^k)_f &= \{x \mid \exists y \; |y| = f(|x|) \text{ and } xy \in \{a^{mn+k} \mid n \geqslant 0\}\} \\ &= \{a^i \mid \exists j \; j = f(i) \text{ and } a^i a^j \in \{a^{mn+k} \mid n \geqslant 0\}\} \\ &= \{a^i \mid \exists j \; j = f(i) \text{ and } i + j = k \bmod m\} \\ &= \{a^i \mid i + f(i) = k \bmod m\}, \end{aligned}$$

Proof Contd..

and by **C1**, this set is regular, thus

$$\begin{aligned} \text{lengths}(((a^m)^* a^k)_f) &= \text{lengths}(\{a^i | i + f(i) = k \text{ mod } m\}) \\ &= \{i | i + f(i) = k \text{ mod } m\} \\ &= f'^{-1}([k]_m) \end{aligned}$$

is u.p., where $f'(n) = n + f(n)$.
Since this holds for arbitrary k and m, it follows from Lemma 1 that $f'(n)$ satisfies **C4**(i) $\Longrightarrow$ $f'(n)$ is u.p. modulo m for any m.
Since the function $n \mapsto (-n)$ mod m is also u.p., so is the sum

$$\begin{aligned} \text{mod } f'(n) m + (-n) \text{ mod } m &= f'(n) - n \text{ mod } m \\ &= f(n) \text{ mod } m. \end{aligned}$$

To show **C4**(ii), consider regular set a^*ba^k. Then, $a^*b \cap (a^*ba^k)_f$

$$= \{a^nb \mid \exists y \mid y \mid = f(\mid a^nb \mid) \text{ and } a^nby \in \{a^nba^k \mid n \geqslant 0\}\}$$
$$= \{a^nb \mid \exists y \mid y \mid = f(n+1) \text{ and } y = a^k\}$$
$$= \{a^nb \mid \text{k} = f(n+1)\}$$
$$= \{a^nb \mid \text{n+1} \in f^{-1}(\{k\})\},$$

by **C1**, this set is regular, ∴ lengths($\{a^nb \mid \text{n+1} \in f^{-1}(\{k\})\}$)

$$= \{n+1 \mid n+1 \in f^{-1}(\{k\})\}$$
$$= f^{-1}(\{k\}) - \{0\}$$

is u.p.. $\implies f^{-1}(k)$ is u.p.

(**C4** → **C3**) Let U be a u.p. set with period p.
U can be expressed as a Boolean combination of a finite set F and sets of form $[i]_p$:

$$U = F \oplus ([i_1]_p \cup [i_2]_p \cup \ldots \cup [i_k]_p),$$

$\oplus$ denotes symmetric difference of sets.

$$\begin{aligned} f^{-1}(U) &= f^{-1}(F \oplus ([i_1]_p \cup [i_2]_p \cup \ldots \cup [i_k]_p)) \\ &= f^{-1}(F) \oplus (f^{-1}([i_1]_p) \cup f^{-1}([i_2]_p) \cup \ldots \cup f^{-1}([i_k]_p)) \\ &= (\bigcup_{x \in F} f^{-1}(x)) \oplus (f^{-1}([i_1]_p) \cup f^{-1}([i_2]_p) \cup \ldots \cup f^{-1}([i_k]_p)) \end{aligned}$$

C4, Lemma 1, and closure properties of u.p. sets imply that this set is u.p.

(**C3** → **C2**)

$$\begin{aligned} A'_f &= \{x \mid \exists y \in A \mid y \mid = f(\mid x \mid)\} \\ &= \{x \mid \exists n \in lengths(A) \text{ n} = f(\mid x \mid)\} \\ &= \{x \mid f(\mid x \mid) \in lengths(A)\} \\ &= \{x \mid \ \mid x \mid \in f^{-1}(lengths(A))\} \end{aligned}$$

If A is regular

$\implies$ lengths(A) is u.p.

$\implies$ $f^{-1}(lengths(A))$ is u.p. by **C3**

$\implies$ A'_f is regular.

(**C2** → **C1**) Let A be a regular set and let M = (Q, Σ, δ, s, F) be a deterministic finite automaton with L(M)=A.
If p ∈ Q and G ⊆ Q, define

$$M_p^G = (Q, \Sigma, \delta, p, G)$$

$$\begin{aligned}
A_f &= \{x \mid \exists y \mid y \mid = f(\mid x \mid) \text{ and } xy \in A\} \\
&= \{x \mid \exists y \mid y \mid = f(\mid x \mid) \text{ and } \widehat{\delta}(s, xy) \in F\} \\
&= \{x \mid \exists y \mid y \mid = f(\mid x \mid) \text{ and } \widehat{\delta}(\widehat{\delta}(s, x), y))\} \\
&= \bigcup_{p \in Q} \{x \mid \exists y \mid y \mid = f(\mid x \mid) \text{ and } \widehat{\delta}(s, x) = \text{p and } \widehat{\delta}(p, y) \in F\} \\
&= \bigcup_{p \in Q} \{x \mid \widehat{\delta}(s, x) = \text{p}\} \cap \{x \mid \exists y \mid y \mid = f(\mid x \mid) \text{ and } \widehat{\delta}(p, y) \in F\} \\
&= \bigcup_{p \in Q} L(M_s^p) \cap L(M_p^F)'_f.
\end{aligned}$$

By **C2** and closure of regular sets under the boolean set operations, this is a regular set.

Thank You!