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

1 Introduction

2 Regularity Preserving Functions

3 Characterization using Ultimate Periodicity
Show that if $A$ is a regular set, then so is

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

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:

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

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

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

Presence of non linear functions makes regularity counter-intuitive.
Boolean Transition Matrix

For automaton $A = (Q, \Sigma, s, \delta, F)$
Boolean Transition Matrix $\Delta$ is a $|Q| \times |Q|$ 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 $\Delta^n$ gives the $n$-step transition relations.
**Example 1**

$A_{2^n}$

- 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 $\triangle^{2(n+1)} = \triangle^{2^n} \ast \triangle^{2^n}$.
- $\therefore$ Maintain $\triangle$ matrix in the start state.
- As input is scanned, the successive state gets updated matrix, $(C) \rightarrow (C \ast C)$
- $\therefore$ In $n$ steps, $(I) \xrightarrow{n} (\triangle^{2^n})$
- If $\hat{\delta}(s, x) = p$, then accept if $C(p, f) = 1$ for any $f \in F$. Reject otherwise.
Motivation

Example 2

\[ A_{n^2} \]

- 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, \( \triangle^{(n+1)^2} = \triangle^{n^2} \triangle^{2n} \).
- \( \therefore \) 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 \( \hat{\delta}(s, x) = p \), then accept if \( C(p, f) = 1 \) for any \( f \in F \). Reject otherwise.
Overview

1 Introduction

2 Regularity Preserving Functions

3 Characterization using Ultimate Periodicity
Regularity Preserving Functions

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

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

- 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

1 Introduction

2 Regularity Preserving Functions

3 Characterization using Ultimate Periodicity
**Ultimate Periodicity**

**Definition 1**

A set $U \subseteq N$ is called *ultimately periodic (u.p.)* (or *semilinear*) if

$$\exists p \geq 1 \ \forall n \quad n \in U \iff n + p \in U.$$  

More generally, a function $f : N \rightarrow N$ is called *ultimately periodic* if

$$\exists p \geq 1 \ \forall n \quad f(n) = f(n + p).$$

$\forall$ means ”for all but finitely many”.

An example of a u.p. set is $[k]_m$, the congruence class of $k$ modulo $m$

$$[k]_m = \{n|n \text{ modulo } m = k\}$$
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 \(\{ x \mid |x| \in U \}\) is regular.
**Definition 2**

A function $f : N \to N$ is said to preserve ultimate periodicity if $f^{-1}(U)$ 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 $m \geq 1$; and
  2. $f^{-1}(\{x\})$ is ultimately periodic for all $x \in N$

\[A_f = \{ x | \exists y \mid y \models f(|x|) \text{ and } xy \in A \}\]
\[A_{f'} = \{ x | \exists y \mid y \models f(|x|) \text{ and } y \in A \}\]
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 $m$,

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

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

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

$$\iff \exists p \geq 1 \bigwedge_{i=0}^{m-1} \infty \quad \forall n \ n \in f^{-1}([i]_m) \iff n + p \in f^{-1}([i]_m)$$
Proof contd..

\[ \exists p \geq 1 \wedge \forall n \ (f(n) \in [i]_m) \iff f(n + p) \in [i]_m \]

\[ \exists p \geq 1 \forall n \ (f(n) \equiv f(n + p) \mod m) \]

\[ f \text{ is u.p. modulo } m. \]
Theorem

The four conditions \( C1 - C4 \) are equivalent.

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

\[
((a^m)^*a^k)_f = \{ x \mid \exists y \ |y| = f(|x|) \text{ and } xy \in \{a^{mn+k} | n \geq 0\} \}
\]

\[
= \{a^i \mid \exists j \ j = f(i) \text{ and } a^i a^j \in \{a^{mn+k} | n \geq 0\} \}
\]

\[
= \{a^i \mid \exists j \ j = f(i) \text{ and } i + j = k \mod m \}
\]

\[
= \{a^i \mid i + f(i) = k \mod m \},
\]
and by \( \textbf{C1} \), this set is regular, thus

\[
\text{lengths}(((a^m)^*a^k)_{f}) = \text{lengths}\{a^i|i + f(i) = k \mod m\}
\]
\[
= \{i|i + f(i) = k \mod m\}
\]
\[
= f'^{-1}([k]_m)
\]

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 \( \textbf{C4}(i) \implies f'(n) \) is u.p. modulo \( m \) for any \( m \).

Since the function \( n \mapsto (-n) \mod m \) is also u.p., so is the sum

\[
\mod f'(n)m + (-n) \mod m = f'(n) - n \mod m
\]
\[
= f(n) \mod m.
\]
To show $\textbf{C4}$ (ii), consider regular set $a^* ba^k$. Then, $a^* b \cap (a^* ba^k)_f$

$$= \{a^n b \mid \exists y \mid y = f(|a^n b|) \text{ and } a^n b y \in \{a^n ba^k \mid n \geq 0\}\}$$

$$= \{a^n b \mid \exists y \mid y = f(n + 1) \text{ and } y = a^k\}$$

$$= \{a^n b \mid k = f(n + 1)\}$$

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

by $\textbf{C1}$, this set is regular, $\therefore$ lengths(\{a^n b \mid 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.

$$f^{-1}(U) = f^{-1}(F \oplus ([i_1]_p \cup [i_2]_p \cup \ldots \cup [i_k]_p))$$

$$= f^{-1}(F) \oplus (f^{-1}([i_1]_p) \cup f^{-1}([i_2]_p) \cup \ldots \cup f^{-1}([i_k]_p))$$

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

C4, Lemma 1, and closure properties of u.p. sets imply that this set is u.p.
(C3 → C2)

\[ A_f' = \{ x | \exists y \in A \mid y = f(|x|) \} \]

\[ = \{ x | \exists n \in \text{lengths}(A) \mid n = f(|x|) \} \]

\[ = \{ x | f(|x|) \in \text{lengths}(A) \} \]

\[ = \{ x | \mid x \mid \in f^{-1}(\text{lengths}(A)) \} \]

If A is regular

\[ \implies \text{lengths}(A) \text{ is u.p.} \]

\[ \implies f^{-1}(\text{lengths}(A)) \text{ is u.p. by C3} \]

\[ \implies A_f' \text{ is regular.} \]
(C2 → C1) Let $A$ be a regular set and let $M = (Q, \Sigma, \delta, s, F)$ be a deterministic finite automaton with $L(M) = A$. If $p \in Q$ and $G \subseteq Q$, define

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

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

$$= \{x | \exists y \mid y \models f(|x|) \text{ and } \delta(s, xy) \in F\}$$

$$= \{x | \exists y \mid y \models f(|x|) \text{ and } \delta(\delta(s, x), y)\}$$

$$= \bigcup_{p \in Q} \{x | \exists y \mid y \models f(|x|) \text{ and } \delta(s, x) \models p \text{ and } \delta(p, y) \in F\}$$

$$= \bigcup_{p \in Q} \{x \mid \delta(s, x) \models p\} \cap \{x | \exists y \mid y \models f(|x|) \text{ and } \delta(p, y) \in F\}$$

$$= \bigcup_{p \in Q} L(M_s^p) \cap L(M_p^F)'$$

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