Implicit FSM traversal on $F(2^k)$

Xiaojun Sun   Prof. Priyank Kalla
Department of Electrical & Computer Engineering
University of Utah, Salt Lake City
{xiaojun.sun,kalla}@ece.utah.edu

Last Update: Mar 6, 2013

Abstract

N/A

1 Introduction

N/A

2 Theory

BFS traversal

$\underline{\textit{Main Loop:}}$
Input: Δ, S^0
$from^0 = S^0$ =*reached.*
while(1){
  i++;
  $to^i = Img(\Delta, from^{i-1})$
  $new^i = to^i \bigcap \overline{reached}$
  if $new^i == 0$ *then return (reached);*
  $reached = reached \bigcup new^i$
  $from^i = new^i$
}

Image Function

Easy stuff.

Union, Intersect & Complement

- **Theorem 1** If I and J are ideals in $k[x_1, ..., x_n]$, then $V(I + J) = V(I) \bigcap V(J)$.
- **Theorem 2** If I and J are ideals in $k[x_1, ..., x_n]$, then $V(I \cdot J) = V(I) \bigcup V(J)$.
- **Theorem 3** Let V and W be varieties in k^n. Then $I(V) : I(W) = I(V - W)$.

Suppose we take only one polynomial only contains T(next state), like

$$ideal\ G = T^2 + (1 + X) \cdot T + X$$

Since we get G from GB based image function, so G is already a Groebner Basis itself. Considering Theorem 1 $\sim$ 3, it's easy to do ideal operation if its generator is only one polynomial. So using $G + G'$ we can get intersection, using $G \cdot G'$ we can get union. If we take V = Universe = $< vanishing\ polynomial >$, we can get ideal quotient $I(V) : I(W)$ as complementary set for specific varieties.

More about Ideal Quotient

- **Definition 1** If I,J are ideals in $k[x_1, ..., x_n]$, then $I : J$ is the set $\{f \in k[x_1, ..., x_n] : fg \in I\ for\ all\ g \in J\}$

Why we can get complementary set $\overline{reached}$ through this?

First, we only care about varieties. Say we redefine the "equal" as $V(I) == V(J) \Leftrightarrow I == J$.

Second, we only care about the ideal/GB **G** contains only 1 generator f. Say this polynomial f is a function about next state (word level) T, then $f(T = V(\mathbf{G})) == \mathbf{0}$. To ensure then unique of generator f, we'll reduce f (or say **G**) every time.

Third, for ideal quotient $\mathbf{U} : \mathbf{G}$ here, we need to find f from $g\ f == vanish$. This means $< f > \bigcup < g > == < vanish >$. How can we develop a division algorithm to get exactly a factor without any remainders? Let's see

3 examples following:

$$T^2 + (1 + X) \cdot T + X$$

$$T^2 + T$$

$$T^2 + 1$$