ICOT Technical Memorandom: TM-0962

TM-0962

Universal Boolean Grobner base

by

Y. Sato

October, 1990

ICOT

Mita Kokusai Bldg. 21F
4-28 Mita 1-Chome
Minato-ku Tokyo 108 Japan

(03)3456-3191~5
Telex ICOT J32964

Institute for New Generation Computer Technology

Universal Boolean Gröbner base

Yosuke Sato

ICOT Research Center
1-4-28, Mita, Minato-ku, Tokyo 108, JAPAN

ABSTRACT

In [1], we showed how to construct a Boolean Gröbner base of a finitely generated ideal in a Boolean polynomial ring. A Boolean polynomial in $B(X_1, \ldots, X_m, Y_1, \ldots, Y_n)$ is also considered as a Boolean polynomial in $B(X_1, \ldots, X_m)(Y_1, \ldots, Y_n)$ with variables $Y_1, \ldots, Y_n$ over a coefficient Boolean ring $B(X_1, \ldots, X_m)$. Let I be an ideal in $B(X_1, \ldots, X_m, Y_1, \ldots, Y_n)$ and G be its Boolean Gröbner base. For any substitution θ of elements of B to the variables $X_1, \ldots, X_m$, $I\theta$ forms an ideal in $B(Y_1, \ldots, Y_n)$. In this paper, we prove (i) $G\theta$ is also a Boolean Gröbner base of $I\theta$ and (ii) for any Boolean polynomial f in $B(X_1, \ldots, X_m, Y_1, \ldots, Y_n)$ $f\theta{\downarrow_{G\theta}} = (f{\downarrow_G})\theta$.

1. Introduction

We assume that the reader is familiar with the theory of Boolean Gröbner base which is described in [1].

Let B be any Boolean ring. A Boolean polynomial in a Boolean polynomial ring $B(X_1, \ldots, X_m, Y_1, \ldots, Y_n)$ with variables $X_1, \ldots, X_m, Y_1, \ldots, Y_n$ can be considered as a Boolean polynomial in a Boolean polynomial ring with variables $Y_1, \ldots, Y_n$ over a coefficient Boolean ring $B(X_1, \ldots, X_m)$, which is expressed as $B(X_1, \ldots, X_m)(Y_1, \ldots, Y_n)$.

Lemma 1.1
Let I be an ideal in $B(X_1, \ldots, X_m, Y_1, \ldots, Y_n)$ and θ be a substitution of elements of B to the variables $X_1, \ldots, X_m$. Then $\{f\theta | f \in I\}$ forms an ideal in $B(Y_1, \ldots, Y_n)$ which is denoted by $I\theta$.

Proof: Easy to check. ∎

In the rest of the paper, we fix an admissible total ordering on monomials consisting of variables $Y_1, \ldots, Y_n$.

2. Universal Boolean Gröbner base

Definition 2.1
Let $G = \{g_1 A_1 \oplus t_1, \ldots, g_k A_k \oplus t_k\}$ be a Boolean Gröbner base in $B(X_1, \ldots, X_m)(Y_1, \ldots, Y_n)$ and θ be a substitution of elements of B to variables $X_1, \ldots, X_m$.

We define $G\theta \stackrel{\text{def}}{=} \{(g_i\theta)A_i \oplus (t_i\theta) | g_i\theta \neq 0\}$

Theorem 2.2
Let G be a Boolean Gröbner base of a finitely generated ideal I in $B(X_1, \ldots, X_m)(Y_1, \ldots, Y_n)$. Then $G\theta$ is also a Boolean Gröbner base of $I\theta$ in $B(Y_1, \ldots, Y_n)$.

Theorem 2.3
For any Boolean polynomial f in $B(X_1, \ldots X_m, Y_1, \ldots, Y_n)$, $(f\theta)\downarrow_{G\theta} = (f\downarrow_G)\theta$.

In order to prove these theorems, we need the following lemmas.

Lemma 2.4
For any Boolean polynomial f in $B(X_1, \ldots, X_m, Y_1, \ldots, Y_n)$, if f is irreducible by $\Rightarrow_G$, then $f\theta$ is also irreducible by $\Rightarrow_{G\theta}$ for any substitution θ.

Proof:

Let $f = f_0 + f_1 A_1 + \ldots + f_l A_l$, where A_i is a monomial of $Y_1, \ldots, Y_n$ and $f_i \in B(X_1, \ldots, X_m)$. If f is irreducible by $\Rightarrow_G$, then for each $gB \oplus t \in G$ $gf_i = 0$ for any i such that $B \subseteq A_i$. Since $gf_i = 0$ implies $(g\theta)(f_i\theta) = 0$, $f\theta$ is also irreducible by $G\theta$. ∎

Lemma 2.5
For any Boolean polynomial f in $B(X_1, \ldots, X_m, Y_1, \ldots, Y_n)$, $(f\theta)\downarrow_{G\theta} = (f\downarrow_G)\theta$.

Proof:

Since we have not proved that $G\theta$ is a Gröbner base, $(f\theta)\downarrow_{G\theta}$ denotes one of irreducible forms of $f\theta$ by $\Rightarrow_{G\theta}$. Given a reduction $f \Rightarrow_{g_1} f_1 \Rightarrow_{g_2} \ldots \Rightarrow_{g_r} f_r$ by $g_1, \ldots, g_r$ in G where

f_r is irreducible by $\Rightarrow_G$. Let $f_i = p(X_1,\ldots,X_m)AB + S$ and $g_{i+1} = q(X_1,\ldots,X_m)A \oplus T$, where $p(X_1,\ldots,X_m), q(X_1,\ldots,X_m) \in B(X_1,\ldots,X_m)$, $S,T \in B(X_1,\ldots,X_m,Y_1,\ldots,Y_n)$, A, B are monomials of $Y_1,\ldots Y_m$ and $p(X_1,\ldots,X_m)q(X_1,\ldots,X_m) \neq 0$. By the definition of $\Rightarrow_{g_{i+1}}$, $f_{i+1} = p(X_1,\ldots,X_m)(q(X_1,\ldots,X_m)+1)AB+p(X_1,\ldots,X_m)q(X_1,\ldots,X_m)BT+S$. There are two cases to be considered.

Case 1: $(p(X_1,\ldots,X_m)\theta)(q(X_1,\ldots,X_m)\theta) = 0$

In this case, $f_i\theta = f_{i+1}\theta$

Case 2: $(p(X_1,\ldots,X_m)\theta)(q(X_1,\ldots,X_m)\theta) \neq 0$

In this case, $f_i\theta \Rightarrow_{g_{i+1}\theta} f_{i+1}\theta$

Therefore we have a reduction from $f\theta$ to $f_n\theta$ by using $\Rightarrow_{G\theta}$.(If Case 1 occurs for each i, $f\theta = f_n\theta$.) By Lemma 2.4, $f_n\theta$ is irreducible by $\Rightarrow_{G\theta}$. Hence $f_n\theta = (f\theta)\downarrow_{G\theta}$,i.e. $(f\downarrow_G)\theta = (f\theta)\downarrow_{G\theta}$.

∎

Proof: of Theorem 2.2

Note that it suffices to show the following.

(i) $I\theta = (G\theta)$ where $(G\theta)$ denotes an ideal generated by $G\theta$

(ii) For each different g and h in $G\theta$, g is irreducible by $\Rightarrow_h$.

(iii) For each different g and h in $G\theta$, $cp(g,h)\downarrow_{G\theta} = 0, vsc(g)\downarrow_{G\theta} = 0$ and $csc(g)\downarrow_{G\theta} = 0$, where $cp(g,h)$ denotes a critical pair of g and h ,$vsc(g)$ and $csc(g)$ denote a variable and a coefficient self-critical pair of g respectively.

By the definition of Boolean Gröbner base, we can get (ii) by Lemma 2.4, and (iii) by Lemma 2.5 directly.

Let $G_1 = \{g_i \oplus t_i | g_i\theta = 0\}$, and $G_1^\theta = \{t_i\theta | g_i\theta = 0\}$. Since $I = (G)$, $I\theta = (G\theta \cup G_1^\theta)$. Therefore in order to see (i), it suffices to show $G_1^\theta \subseteq (G\theta)$, i.e. $t_i\theta \in (G\theta)$ for any i such that $g_i\theta = 0$. Note that $scp(g_iA_i \oplus t_i) = g_it_i + t_i$. Hence,$(scp(g_iA_i \oplus t_i))\theta = t_i\theta$. Since $(scp(g_iA_i \oplus t_i))\downarrow_G = 0$, $(scp(g_iA_i \oplus t_i))\theta\downarrow_{G\theta} = 0$ by Lemma 2.5, i.e. $(t_i\theta)\downarrow_{G\theta} = 0$. By the definition of $\Rightarrow_{G\theta}$, it is clear that $t_i\theta \in (G\theta)$.

∎

Proof: of Theorem 2.3

This is exactly same as Lemma 2.5. ∎

REFERENCES

[1] Sakai,K. Sato,Y. Menju,S.: *Boolean Gröbner base(revised)*, to appear (1990)

[2] Sakai,K. Sato,Y.: *A note on solvability of Boolean equations* , IEICE Technical Report, Vol.89,No.276,pp.41-44 (1989)

[3] Sakai, K. and Sato, Y.: *Zero-point theorem for Boolean polynomial ring*, to appear (1990)

[4] Sato, Y. Sakai, K. Menju,S: *SetCAL - a solver of set constraint in CAL system*, to appear (1990)

[5] Sato, Y.: *Quantifier elimination for atomic Boolean constraint*, to appear (1990)