TM-0954

Zero-point theorem for the Boolean polynomical ring

by
K. Sakai & Y. Sato

September, 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

Zero-point theorem for the Boolean polynomial ring

Kô Sakai and Yosuke Sato

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

(August 17, 1990)

ABSTRACT

We prove the zero-point theorem for Boolean polynomial rings. This gives us a semantic property of ideals in the polynomial rings. The property is especially important for constraint solving in a Boolean domain.

1. Introduction

"Constraint solving" in a general context can mean various things. However, determination of the validity of a formula under a certain constraint must always be the main purpose of constraint solving.

When we consider a set F of polynomials over a ring as a constraint in the sense that all polynomials in it should have value zero, a valid polynomial can be defined as a polynomial that vanishes on every zero-point of F. To address the problem of determining the validity of a polynomial under F, a purely syntactical characterization of the set $V(F)$ of all valid polynomials is needed.

For ordinary polynomials over an algebraically closed field (such as the complex numbers), a polynomial is valid under F if and only if it is an element of the radical of the ideal generated by F (the Hilbert zero point theorem). We show that, for polynomials over a Boolean ring, a stronger relation holds, that is, in the case that a zero-point of F exists (in other words, F is a satisfiable constraint), a polynomial is valid under F if and only if it is an element of the ideal generated by F. This Boolean version of zero-point theorem gives us the simplest syntactical characterization of valid formulas. Together with the known result concerning solvability of equations of the Boolean polynomial ring (see [SaSa 89], for example), we can handle constraints of this domain completely in terms of ideals.

2. Validity ideal

We assume that the reader is familiar with elementary algebraic notions such as rings and ideals (see [Waerden 37, 40], for example), in particular Boolean rings (see [Halmos 63], for example).

Let B be a Boolean ring, that is, a commutative ring with unit satisfying the follwing property:

$$b^2 = b \quad \text{for any } b \in B.$$

Let us consider a polynomial with elements of B as its coefficients. If it is linear w.r.t. each variable, it is called a **Boolean polynomial**. Let V be a set of variables. The set of all Boolean polynomials over B with variables in V by $B[V]$. The set $B[V]$ forms a Boolean ring by relation $x^2 = x$ for each variable x. Let F be a subset of $B[V]$. We denote the ideal generated from F (i.e. the least ideal including F) by $I(F)$. A **zero-point** of F is a substitution θ which assigns an element of B to each variable such that $\theta(f) = 0$ for every $f \in F$. We denote the set of all zero-points of F by $Z(F)$. A Boolean polynomial f is called **valid** under F if $Z(F) \subset Z(\{f\})$. The set of all polynomials valid under F is denoted by $V(F)$.

Let us summarize known results on ideals and zero-points of Boolean polynomials. Let F be a set of Boolean polynomials,

(B1) $Z(F) = Z(I(F))$,

(B2) $V(F)$ is an ideal and $I(F) \subseteq V(F)$,

(B3) Let f be a Boolean polynomial and let x be a variable occurring in f. We can put $f = f_1 x + f_0$ where f_0 and f_1 are polynomials in which x does not occur. Then f has a zero-point if and only if so does $g = f_1 f_0 + f_0$. In fact, if θ is a zero-point of g, by putting $x = \theta(f_0)$ for example, we can obtain a zero-point of f.

(B4) If F is finite, $Z(F) = \emptyset$ if and only if there is a non-zero constant (a polynomial without variables) in $I(F)$.

3. Zero-point theorem

Theorem 3.1 Zero-point theorem
Let F be a finite subset of $B[V]$. If F has a zero-point, then $V(F) = I(F)$.

For a finite subset $F = \{f_1, f_2, \ldots, f_n\}$ of $B[V]$, if we put $f = f_1 \vee f_2 \vee \cdots \vee f_n$, then it is easily proved that $Z(F) = Z(\{f\})$ (and, therefore, $V(F) = V(\{f\})$) and $I(F) = I(\{f\})$. Hence, we can assume F is a singleton set $\{f\}$ without loss of generality. We also assume that F has a zero-point in the rest of this section.

Before the above theorem, we prove the next two lemmas.

Lemma 3.2
Let a be an atom of B, that is, there exists no $b \in B$ such that $0 < b < a$. Then, for any polynomial g, $ag \in V(F)$ implies $ag \in I(F)$.
Proof: If $ag \in V(F)$, then clearly $\{ag + a, f\}$ does not have zero-points. Therefore, by (B4), there exists a non-zero constant b in $I(\{aP + a, f\})$, that is, there exist Boolean polynomials h, h' such that $b = h(ag + a) + h'f$. Let θ be a zero-point of F, that is, $\theta(f) = 0$. Applying θ from both sides, we have

$$\theta(b) = \theta(h(ag + a) + h'f).$$

Note that $\theta(b) = b$, $\theta(a) = a$, and $\theta(ag) = 0$ since $ag \in V(F)$. Therefore,

$$b = \theta(b) = \theta(h(ag + a) + h'f) = \theta(h)(\theta(ag) + \theta(a)) + \theta(h')\theta(f) = \theta(h)a.$$

Since a is an atom in B and $b \neq 0$, $b = a$. Now we got $a = h(ag + a) + h'f$. Multiplying g from both sides,

$$ag = h(ag + ag) + gh'f = (gh')f \in I(F) \quad \blacksquare$$

Lemma 3.3
Let g be a polynomial and let $b_1, b_2, \ldots, b_n \in B$ be all the coefficients appearing in g. Let $B(b_1, b_2, \ldots, b_n)$ be the Boolean subring of B generated from $b_1, b_2, \ldots, b_n$. Then, g has a zero-point in B if and only if g has a zero-point in $B(b_1, \ldots, b_n)$
Proof: It is clear from (B3). $\blacksquare$

Proof of Theorem 3.1: Suppose $g \in V(F)$. Let $b_1, b_2, \ldots, b_n \in B$ be all the coefficients appearing in mg and f. By Lemma 3.3 F has a zero-point in $B(b_1, b_2, \ldots, b_n)$. Since $B(b_1, b_2, \ldots, b_n) \subseteq B$, $g \in V(F)$ holds also in $B(b_1, b_2, \ldots, b_n)$. Note that $B(b_1, b_2, \ldots, b_n)$ is finite. Let $a_1, a_2, \ldots, a_l$ be all the atoms in $B(b_1, b_2, \ldots, b_n)$. Clearly, $1 = a_1 + a_2 + \cdots + a_l$. Since $a_i g \in V(F)$, $a_i g \in I(F)$ by Lemma 3. 2 for each a_i. Therefore $g = a_1 g + a_2 g + \cdots + a_l g \in I(F)$. It is clear that $g \in I$ holds also in B $\blacksquare$

Example 3.4
When $Z(F) = \emptyset$, clearly $V(F)$ consists of all Boolean polynomials. There exists a finite set F such that $Z(F) = \emptyset$ but $I(F)$ does not consist of all Boolean polynomials. For example, if b is an element of B such that $0 < b < 1$, then $Z(\{b\}) = \emptyset$ but $1 \notin I(\{b\})$.

Example 3.5

When F is not finitely generated, Theorem 3.1 does not necessarily hold. For example, let B be an atomic Boolean ring with infinitely many atoms. Let $x \in V$ and let $F = \{ax \mid a \text{ is an atom in } B\}$. Then, clearly, $x \in V(F)$ but $x \notin I(F)$.

REFERENCES

[Halmos 63] Halmos, P. R. : *Lectures on Boolean Algebras*, D. Van Nostrand Company (1963)

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

[Waerden 37] van der Waerden, B. L. : *Moderne Algebra I*, Berlin-Leipzig (1937)

[Waerden 40] van der Waerden, B. L. : *Moderne Algebra II*, Berlin-Leipzig (1940)