TR-613

Boolean Gröbner Bases (revised)

by
K. Sakai, Y. Satoh, & S. Menju

January, 1991

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

Boolean Gröbner Bases (revised)

Kô Sakai, Yosuke Sato, Satoshi Menju

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

ABSTRACT

We studied several important properties of Boolean polynomial rings in [SaSa 90]. Especially we saw ideal plays a central role for solving a Boolean constraint. This paper gives an algorithm which produces a rewriting system for a given finitely generated ideal in the ring of Boolean polynomials. The rewriting system reduces all Boolean polynomials that are equivalent under the ideal to the same normal form.

1. Boolean polynomial ring

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 algebras (see [Halmos 63], for example), and the terminology of rewriting systems (see [Huet 80], for example).

For a Boolean algebra $\langle \vee, \wedge, \neg, 0, 1, \rangle$, define $a + b =_{\text{def}} (a \wedge \neg b) \vee (\neg a \wedge b)$ and $a \times b =_{\text{def}} a \wedge b$ for each a, b in B, then $\langle B, \times, + \rangle$ is known to form a Boolean ring, namely, a commutative ring with a unit with the following properties.

(B1) $\quad \forall a \in B \quad a + a = 0$

(B2) $\quad \forall a \in B \quad a \times a = a$

In what follows, let B be a fixed Boolean ring. Elements of B are denoted by typed variables $a, b, c, \ldots$ (possibly with suffix). As usual, we omit symbols $\times$, i.e. $a \times b$ is denoted by ab, for example.

The following notions may intuitively clear to the reader. However, we give a formal definitions to them for ease of later discussion.

First, assume that we have a denumerable set V of **variables**. We denote variables by typed variables $X, Y, Z, \ldots$ (possibly with suffix). A **power product** is a finite sequence

$$X_1 X_2 \ldots X_n \quad (n \geq 0)$$

of variables. We do not distinguish two power products that contain the same number of the same variables in different order. Therefore, a power product can be regarded as a finite multiset [Dershowitz 79] of variables. The empty power product is denoted by 1. Power products are expressed by typed variables $\alpha, \beta, \gamma, \ldots$ (possibly with suffix).

A **polynomial** is a function ψ from the set of all power products to B such that $\psi(\alpha) = 0$ for every but a finite number of power products α. The value $\psi(\alpha)$ is called the **coefficient** of α. As usual, we express a polynomial in the following way:

$$a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n \quad (n \geq 0),$$

which means the coefficient of α_i is a_i and the coefficients of all the power products other than a_is are 0. When $a_i = 1$, the coefficient a_i is often ommited. It is called a **monomial** if $n = 1$, and it is denoted by 0 if $n = 0$. Polynomials are expressed by typed variables $\psi, \phi, \varphi, \ldots$ (possibly with suffix).

We define operations $+$ and $\times$ on polynomials as follows:

$$(\psi + \phi)(\alpha) = \psi(\alpha) + \phi(\alpha), \quad (\psi \times \phi)(\alpha) = \sum_{\beta\gamma=\alpha} \psi(\beta) \times \phi(\gamma),$$

where $\beta\gamma$ denotes the concatenation of β and γ as strings (or the union as multisets). As is well-known, the set of all polynomials forms a ring w. r. t. the operations $+$ and $\times$. We denote this ring by $B[V]$. We omit $\times$ symbols also for polynomials.

A function θ from V to B is called a **substitution**. A substitution θ is extended to a function from power products and polynomials homomorphically in the following way.

(1) $\theta(X_1X_2\ldots X_n) = \theta(X_1)\theta(X_2)\ldots\theta(X_n)$

(2) $\theta(a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n) = a_1\theta(\alpha_1) + a_2\theta(\alpha_2)\cdots + a_n\theta(\alpha_n)$

2. Reduction

In the rest of the paper we often denote a polynomial in the additive form $a\alpha + \phi$ (i.e. a sequence of a monomial, a $+$ symbol and another polynomial in this order). In this case, we assume that $a \neq 0$ and $\phi(\alpha) = 0$ unless otherwise stated.

Let $\rightarrow_\times$ denote rewriting over polynomials which reduces the order of a monomial by using the property (B2) of a Boolean ring once. More precisely, $aXX\alpha + \psi \rightarrow_\times aX\alpha + \psi$ for any variable X. For example,

$$aX^2YZ + bXYZ + cXZ^2 \rightarrow_\times (a+b)XYZ + cXZ^2.$$

It is clear that the following holds:

Proposition 2.1
The rewriting system $\{\rightarrow_\times\}$ is confluent and terminating.

For a polynomial ϕ, $\phi\downarrow$ expresses the canonical form of ϕ by the rewriting system $\{\rightarrow_\times\}$.

Let $B(V)$ denote the set of all polynomials in canonical form. If we define a new operation $\times'$ by $\psi \times' \phi = (\psi \times' \phi)\downarrow$, then $B(V)$ forms a Boolean ring w. r. t. the operations $+$ and $\times'$. We call this the **Boolean polynomial ring**. For convenience, let us call an element of $B(V)$ a **Boolean polynomial**. Similarly, a monomial in canonical form is called **Boolean monomial**. We omit $\times'$ symbols also for Boolean polynomials. Therefore, in what follows, $\psi\phi$ stands for $\psi \times' \phi$ if both ψ and ϕ are Boolean polynomials and $\psi \times \phi$ otherwise.

For a finite set $F = \{\phi_1, \ldots, \phi_n\}$ of Boolean polynomials, let $I(F)$ denote the ideal over $B(V)$ generated by F, i.e.

$$I(F) = \{\psi_1\phi_1 + \cdots + \psi_n\phi_n | \psi_1, \ldots, \psi_n \in B(V)\}$$

Let $\geq$ be an ordering on power products. The ordering is said to be **admissible** if the following hold:

(1) $\alpha \geq \beta$ for any power product α and β such that $\alpha \supseteq \beta$ in the sense of multiset inclusion.

(2) If $\alpha \geq \beta$, then $\alpha\gamma \geq \beta\gamma$ for any power product α, β, and γ.

Let S be a fixed finite set of variables. The fact that an admissible ordering on power products consisting only of the variables in S is well-founded is well known as Dickson's lemma [Dickson 13], or easily proven as its corollary.

In what follows, let $\geq$ be a fixed admissible ordering on power products. Moreover, we assume that $\geq$ is total.

The **leading power product** of a polynomial is the greatest power product with non-zero coefficient. Let a notation $a\alpha \oplus \phi$ express polynomial $a\alpha + \phi$ with α as its leading power product, that is, $\alpha > \beta$ for any β such that $\phi(\beta) \neq 0$. Note that every non-zero polynomial is uniquely expressed in the above form.

We extend the ordering $\geq$ to polynomials in the following lexicographic way. First, we define $0 \geq \psi$ for any polynomial ψ. Next, we define $a\alpha \oplus \psi \geq b\beta \oplus \phi$ if and only if one of the following conditions holds:

(1) $\alpha > \beta$

(2) $\alpha = \beta$ and $a > b$ by the natural ordering in Boolean algebra B.

(3) $\alpha = \beta$, $a = b$, and $\psi \geq \phi$ in the recursive sense.

Now, we define reduction by a Boolean polynomial $a\alpha \oplus \phi$. Let φ be a Boolean polynomial such that $b\alpha\beta + \psi$, and φ' is a Boolean polynomial such that $\varphi' = \psi + b(1+a)\alpha\beta + ab\beta\phi$. Then, if $ab \neq 0$, we write $\varphi \Rightarrow_{a\alpha\oplus\phi} \varphi'$. Similarly, if φ is a polynomial such that $\varphi = b\alpha\beta + \psi$, $ab \neq 0$, and φ' is a polynomial such that $\varphi' = \psi + b(1+a)\alpha\beta + ab\beta\phi$, we write $\varphi \rightarrow_{a\alpha\oplus\phi} \varphi'$.

These mean φ' is obtained from φ by substituting $a\alpha$ for ϕ by using equation $a\alpha = a\phi$. That is, $b\alpha\beta$ is splitted to $b(1+a)\alpha\beta + ba\alpha\beta$ first, and then $a\alpha$ is replaced by $a\phi$. The condition $ab \neq 0$ is indispensable in order to make the reduction terminate.

Let R be a set of Boolean polynomials. We write $\phi \Rightarrow_R \psi$ if there exists $\varphi \in R$ such that $\phi \Rightarrow_\varphi \psi$, and $\phi \overset{*}{\Rightarrow}_R \psi$ if there exists a sequence $\phi_0, \phi_1, \ldots, \phi_m (m \geq 0)$. of Boolean polynomials such that $\phi = \phi_0 \Rightarrow_R \phi_1 \Rightarrow_R \ldots \Rightarrow_R \phi_m = \psi$. That is $\overset{*}{\Rightarrow}_R$ is the reflexive transitive closure of $\Rightarrow_R$. We write $\phi \rightarrow_R \psi$ if $\phi \rightarrow_\times \psi$ or $\phi \rightarrow_\varphi \psi$ for some $\varphi \in R$. $\overset{*}{\rightarrow}_R$ is defined as the reflexive and transitive closure of $\rightarrow_R$, and $\overset{*}{\leftrightarrow}_R$ as the symmetric, reflexive and transitive closure.

Lemma 2.2
Let R be a set of Boolean polynomials. If $\phi \rightarrow_R \psi$, then $\phi > \psi$ for any polynomials ϕ and ψ. If $\phi \Rightarrow_R \psi$, then $\phi > \psi$ for any Boolean polynomials ϕ and ψ.
Proof: Easy to check. ∎

Corollary 2.3
Both of $\rightarrow_R$ and $\Rightarrow_R$ have a termination property. That is, there exist no infinite reductions such as $\phi_0 \rightarrow_R \phi_1 \rightarrow_R \phi_2 \rightarrow_R \ldots$ or $\varphi_0 \Rightarrow_R \varphi_1 \Rightarrow_R \varphi_2 \Rightarrow_R \ldots$.

3. Boolean Gröbner base

In what follows, we will discuss ideals in Boolean polynomial ring. Intuitively, an ideal can be regarded as the set of all Boolean polynomials of value 0 under a certain constraint. (See [SaSa 90])

Let I be an ideal of the Boolean polynomial ring. A subset R of I is called a **Boolean Gröbner base** for I if it has the following two conditions.

(1) If $\phi + \psi \in I$ (or $\phi \equiv \psi \pmod{I}$), then there exists a Boolean polynomial, φ, such that $\psi \overset{*}{\Rightarrow}_R \varphi$ and $\psi \overset{*}{\Rightarrow}_R \varphi$.

(2) Any $\varphi \in R$ is not reducible by $\Rightarrow_\psi$ for any $\psi \in R$ which is distinct from φ.

Moreover if R has the following property, it is called **normal**.

(3) Elements of R have no common leading power products, i.e. if $a\alpha \oplus \phi$, $a'\alpha' \oplus \phi'$ are distinct elements of R, then $\alpha \neq \alpha'$.

Theorem 3.1
Let E be an arbitrary finite set of Boolean polynomials, then a Boolean Gröbner base for the ideal generated by E exists and, furthermore, we have an algorithm to construct it from E.

Intuitively, an element of the generated ideal is a Boolean polynomial of value 0 under the constraint that all elements in E have value 0. A Gröbner base can be viewed as a mechanism to determine whether a certain polynomial is in the ideal. First, we give an algorithm, then show its correctness. We need to define several notations.

Definition 3.2
Let R be a set of Boolean polynomials. For each Boolean polynomial ϕ, $\phi{\downarrow_R}$ denotes a Boolean polynomial, ψ, such that $\phi \overset{*}{\Rightarrow}_R \psi$ and ψ is irreducible by $\Rightarrow_R$, i.e., there exists no Boolean polynomial φ, such that $\psi \Rightarrow_R \varphi$, and called a normal form of ϕ by $\Rightarrow_R$. (Note that Corollary 2.3 assures the existence of such ψ. However, it may not be unique. $\phi{\downarrow_R}$ denotes one such ψ.)

Definition 3.3
Let $a\alpha \oplus \phi$ be a Boolean polynomial. Then a Boolean polynomial $a\phi + \phi$ is called a **coefficient self-critical pair** of $a\alpha \oplus \phi$ denoted by $csc(a\alpha \oplus \phi)$, and a Boolean polynomial $X\phi + \phi$ for any Boolean variable X in α is called a **variable self-critical pair** of $a\alpha \oplus \phi$ denoted by $vsc(a\alpha \oplus \phi)$. (Note that this is not determined unique.)

If $a\alpha \oplus \phi$ is in an ideal, I, then so are all the coefficient self-critical pairs and variable self-critical pairs of $a\alpha \oplus \phi$.

In fact, let $X \in \alpha$, i.e., $\alpha = X\beta$ for some (possibly empty) power product, β. Then, $aX\beta \oplus \phi \in I$ implies $(a+1)(aX\beta \oplus \phi) = a\phi + \phi \in I$, and $(X+1)(aX\beta \oplus \phi) = X\phi + \phi \in I$.

Example 3.4
Let $a\alpha \oplus \phi$ be $aXY \oplus bY$. Then, its coefficient self-critical pair is $(ab+b)Y$. The variable self-critical pairs are $bXY + bX$ and $0 (= bYY + bY)$.

Definition 3.5

Let $a\alpha \oplus \phi$ and $b\beta \oplus \psi$ be Boolean polynomials, and γ the intersection of α and β as sets. According to tradition, let us call γ the GCD (greatest common divisor) of α and β. Suppose that $\gamma \neq 1, ab \neq 0, \alpha = \gamma\alpha'$ and $\beta = \gamma\beta'$. Then, a Boolean polynomial $b\beta'\phi + a\alpha'\psi$ is called the critical pair between $a\alpha \oplus \phi$ and $b\beta \oplus \psi$, and denoted by $cp(a\alpha \oplus \phi, b\beta \oplus \psi)$.

If $a\alpha \oplus \phi$ and $b\beta \oplus \psi$ are in an ideal, I, then so is the critical pair between $a\alpha \oplus \phi$ and $b\beta \oplus \psi$. In fact, $b\beta'(a\alpha \oplus \phi) + a\alpha'(b\beta \oplus \psi) = b\beta'\phi + a\alpha'\psi \in I$.

Example 3.6

Let $a\alpha \oplus \phi = aXY \oplus bX$ and $b\beta \oplus \psi = bYZ \oplus aY$ where $ab \neq 0$, then $(bZ)(bX) + (aX)(aY) = bZX + aXY$. Therefore, $bZX + aXY$ is the critical pair between $aXY \oplus bX$ and $bYZ \oplus aY$.

Definition 3.7

Let ϕ be a Boolean polynomial and R be a finite set of Boolean polynomials, then $CP(\phi, R)$ denotes the set consisting of all the non-zero critical pairs between ϕ and each element of R and all the variable self-critical pairs of ϕ.

Definition 3.8

Let R be a finite set of Boolean polynomials, $Glue(R)$ is a finite set of Boolean polynomials defined as follows. For each power product α which is the Boolean power product of some Boolean polynomial in R, let $\{a_1\alpha \oplus \phi_1, \ldots, a_n\alpha \oplus \phi_n\}$ be the set of all Boolean polynomials in R which have α for the largest power product. Then $(a_1 + \ldots + a_n)\alpha \oplus (\phi_1 + \ldots + \phi_n) \in Glue(R)$. All the elements of $Glue(R)$ are such Boolean polynomials.

Example 3.9

Let $R = \{aXY \oplus X, bXY \oplus Y, bXZ \oplus X, XZ \oplus Z\}$, then $Glue(R) = \{(a+b)XY \oplus (X + Y), (b+1)XZ \oplus (X+Z)\}$.

Now the algorithm can be presented.

input E
$R \longleftarrow \emptyset$
while $E \neq \emptyset$
  choose $\phi \in E$
  $E \longleftarrow (E - \{\phi\}) \cup \{csc(\phi)\}$ and $\phi' \longleftarrow \phi\downarrow_R$
  if $\phi' \neq 0$ **then**
    for every $a\alpha \oplus \psi \in R$
      if $a\alpha \Rightarrow_{\phi'} \varphi$
      then $E \longleftarrow E \cup \{(\varphi + \psi)\downarrow\}$ and $R \longleftarrow R - \{a\alpha \oplus \psi\}$
      else $R \longleftarrow (R - \{a\alpha \oplus \psi\}) \cup \{a\alpha \oplus (\psi\downarrow_{R\cup\{\phi'\}})\}$
      end-if
    end-for
    $E \longleftarrow E \cup CP(\phi', R)$ and $R \longleftarrow R \cup \{\phi'\}$
  end-if
end-while
output $Glue(R)$ ($Glue(R)$ is a normal Gröbner base)

(In this algorithm, the choice of an element in E should be fair. That is, any element of E should be chosen at some stage in the outermost **while** loop.)

This algorithm terminates and returns a Gröbner base. To prove the correctness of the algorithm, we study a more general form of the algorithm.

Definition 3.10
We define inference rules on pairs (E, R) of finite sets of Boolean polynomials.

Rule 1
$$\frac{E \cup \{\psi\}, R}{E \cup \{\varphi\}, R} \quad \text{where } \psi \Rightarrow_R \varphi$$

Rule 2
$$\frac{E \cup \{0\}, R}{E, R}$$

Rule 3
$$\frac{E, R \cup \{a\alpha \oplus \psi\}}{E, R \cup \{a\alpha \oplus \varphi\}} \quad \text{where } \psi \Rightarrow_R \varphi$$

Rule 4 $$\frac{E, R \cup \{b\alpha\beta \oplus \psi\}}{E \cup \{b(1+a)\alpha\beta + ab\beta\phi + \psi\}, R} \quad \text{where } a\alpha \oplus \phi \in R, ab \neq 0 \text{ and } \alpha \neq \emptyset$$

Rule 5 $$\frac{E \cup \{\psi\}, R}{E \cup \{csc(\psi)\}, R \cup \{\psi\}}$$

Rule 6 $$\frac{E, R}{E \cup \{cp(\psi, \varphi)\}, R} \quad \text{where } \psi, \varphi \in R \text{ and } cp(\psi, \varphi) \neq \emptyset \quad \text{(critical pair)}$$

Rule 7 $$\frac{E, R}{E \cup \{vsc(\psi)\}, R} \quad \text{where } \psi \in R \quad \text{(variable self-critical pair)}$$

Definition 3.11 (General form of the algorithm)
Let $E_0 = E, R_0 = \emptyset$. For each i, let E_{i+1} and R_{i+1} be obtained from E_i and R_i by one of the above rules. In the following, $\cup_{n=1}^{\infty} \cap_{i=n}^{\infty} E_i$ is denoted by E^{∞} and $\cup_{n=1}^{\infty} \cap_{i=n}^{\infty} R_i$ by R^{∞}. We give priority to Rules 1 and 2. We need two restrictions to make the algorithm correct.

(i) The algorithm must be fair, i.e., $E^{\infty} = \emptyset$.

(ii) Any possible critical pair or variable self-critical pair must be taken, i.e., for each $\psi \in R^{\infty}$, any $vsc(\psi)$ must be put in some E_i by Rule 7 and for each $\psi, \varphi \in R^{\infty}$, $cp(\psi, \varphi)$ must be put in some E_i by Rule 6.

Then for some i, E_i is empty and $Gluc(R_i)$ is a Gröbner base. (Note that the previous algorithm takes the form defined here.)

To prove the last statement, we need some more definitions.

Definition 3.12
Let φ and ψ be arbitrary polynomials such that $\varphi - \psi = b\beta\phi$ for $\phi \in E_i$. We associate this equation with an ordered pair $(\{\varphi, \psi\}, \phi)$, where $\{\varphi, \psi\}$ is a multiset. Similarly, we associate the reduction $\varphi \rightarrow_{\phi} \psi$ for $\phi \in R_i$ with an ordered pair $(\{\varphi\}, \phi)$. We also associate the rewriting $\varphi \rightarrow_{\times} \psi$ with an ordered pair $(\{\varphi\}, \bullet)$, where $\bullet$ is a special constant. We introduce an ordering on the above ordered pair defined as follows. The first component is compared by the multiset ordering induced by the ordering on polynomials and the second component is compared as a Boolean polynomial. We define $\bullet$ as bigger than any Boolean polynomial. Finally, we define an ordering on ordered pairs lexicographically by the components. We denote this ordering $\geq$. Note that this is well-founded.

Definition 3.13
Let φ and ψ be arbitrary polynomials. If there is a sequence $\Xi_1, \Xi_2, \ldots, \Xi_m$ such that each Ξ_j is an equation $\zeta_j - \zeta_{j+1} = b_j\beta_j\phi_j$ for $\phi_j \in E_i$ (which is denoted by $\zeta_j =_{\phi_j} \zeta_{j+1}$) or a reduction from ζ_j to ζ_{j+1} or from ζ_{j+1} to ζ_j by $\rightarrow_{\phi_j}$ for $\phi_j \in R_i$ or by $\rightarrow_\times$ where $\zeta_1 = \varphi$ and $\zeta_{m+1} = \psi$, we write $\varphi \overset{*}{\leftrightarrow}_{(E_i,R_i)} \psi$, and the sequence is called its **evidence**. Note that there might be many evidences of $\varphi \overset{*}{\leftrightarrow}_{(E_i,R_i)} \psi$ in general. We define an ordering on evidences as the multiset ordering induced by the ordering on equations and reductions defined above. Note that this is also well-founded.

Note that the definition of the ordering does not depend on i. Therefore, we can compare an evidence of $\varphi \overset{*}{\leftrightarrow}_{(E_i,R_i)} \psi$ and an evidence of $\varphi \overset{*}{\leftrightarrow}_{(E_j,R_j)} \psi$, even if i and j are different.

We write $\varphi \overset{*}{\leftrightarrow}_{(E,R)} \psi$, if there exists i such that $\varphi \overset{*}{\leftrightarrow}_{(E_i,R_i)} \psi$.

In the Definition 2.6, $\varphi = \varphi'$ if $ab = 0$. In order to make the following proofs simpler, in this case we also abuse the notation $\varphi \rightarrow_{a\alpha\oplus\phi} \varphi'$ as an dummy reduction in an evidence. That is, the evidence actually does not include this dummy reduction.

Lemma 3.14
Suppose that Rule 1, 3, 4, or 5 is applied in the i-th step and a Boolean polynomial in E_i or R_i, say ψ, is eliminated. Any equation using φ or reduction using $\rightarrow_\varphi$ can be replaced by a smaller evidence in (E_{i+1}, R_{i+1}).

Proof:

Rule 1: Let $\psi = b\alpha\beta + \varphi \in E_i$. Let $a\alpha \oplus \phi \in R_i$, $\psi \Rightarrow_{a\alpha\oplus\varphi} \psi'$, and $\psi' \in E_{i+1}$. Given an equation $\zeta =_\psi \xi$. Let $\zeta \rightarrow_{a\alpha\oplus\phi} \zeta'$ and $\xi \rightarrow_{a\alpha\oplus\phi} \xi'$. Then $\zeta \rightarrow_{a\alpha\oplus\phi} \zeta' \overset{*}{\rightarrow}_\times \zeta'\downarrow =_{\psi'} \xi'\downarrow_\times \overset{*}{\leftarrow} \xi'_{a\alpha\oplus\phi} \leftarrow \xi$. It is easy to see that this evidence is smaller than $\zeta -_\psi \xi$. (Note that there are several cases this evidence includes dummy reductions such as when $abc = 0$. In this case the evidence is nothing but $\zeta =_{\psi'} \xi$.)

Rule 3: Let $a\alpha \oplus \psi \subset R_i$ and $\psi \Rightarrow_\phi \varphi \in R_{i+1}$ for $\phi \in R_i$. Given a reduction $\zeta \rightarrow_{a\alpha\oplus\psi} \xi$. Then $\xi \rightarrow_\phi \xi' \leftarrow_{a\alpha\oplus\varphi} \zeta$. It is easy to see that this evidence is smaller than $\zeta \rightarrow_{a\alpha\oplus\psi} \xi$.

Rule 4: Let $b\alpha\beta\oplus\psi \in R_i$, $a\alpha\oplus\phi \in R_i$ and $b\alpha\beta+\psi \Rightarrow_{a\alpha\oplus\phi} (b(1+a)\alpha\beta+ab\beta\phi+\psi)\downarrow \in E_{i+1}$. Given a reduction $\zeta \rightarrow_{b\alpha\beta\oplus\psi} \xi$. Then $\xi \rightarrow_{a\alpha\oplus\phi} \xi' \overset{*}{\rightarrow}_\times \xi'\downarrow =_{(b(1+a)\alpha\beta+ab\beta\phi+\psi)\downarrow} \zeta'\downarrow \overset{*}{\leftarrow}_\times \zeta' \leftarrow_{a\alpha\oplus\phi} \zeta$. It is easy to see that this evidence is smaller than $\zeta \rightarrow_{b\alpha\beta\oplus\psi} \xi$.

Rule 5: Let $\psi = a\alpha \oplus \varphi \in E_i$, $\psi \in R_{i+1}$ and $csc(\psi) = ((a+1)\varphi)\downarrow \in E_{i+1}$. Given an equation $\zeta =_\psi \xi$. Then $\zeta \rightarrow_\psi \zeta' \overset{*}{\rightarrow}_\times \zeta'\downarrow =_{csc(\psi)} \xi'\downarrow \overset{*}{\leftarrow}_\times \xi' \leftarrow_\psi \xi$. It is easy to see that this evidence is smaller than $\zeta =_\psi \xi$. ∎

Corollary 3.15
If $i \leq j$, $\varphi \overset{*}{\leftrightarrow}_{(E_i,R_i)} \psi \Longrightarrow \varphi \overset{*}{\leftrightarrow}_{(E_j,R_j)} \psi$ for any polynomial φ, ψ

By this, we can see $\overset{*}{\leftrightarrow}_{(E,R)}$ is an equivalence relation over the set of polynomials.

Lemma 3.16
Let ζ and ξ be arbitrary polynomials, and $\Xi_1, \Xi_2, \ldots, \Xi_m$ a minimal evidence of $\zeta \overset{*}{\leftrightarrow} \xi$. Then,

(i) There is no equation in it which uses a Boolean polynomial in some E_i.

(ii) There is no j such that Ξ_{j-1} is a reduction from ξ_j to ξ_{j-1} and Ξ_j is a reduction from ξ_j to ξ_{j+1} (we denote this situation $\xi_{j-1} \leftarrow \xi_j \rightarrow \xi_{j+1}$).

Proof:

By the above lemma, for each $j = 1, \ldots, m$, Ξ_j is neither an equation using a Boolean polynomial eliminated by Rule 1 or 5 nor a reduction using a Boolean polynomial eliminated by Rule 3 or 4. In other words, unless Ξ_j is a reduction by $\rightarrow_\times$, Ξ_j is either an equation using a Boolean polynomial in E^∞ or a reduction using a Boolean polynomial in R^∞. By the condition (i) of the definition of the algorithm, $E^\infty = \emptyset$. Hence (i) follows.

Suppose we have $\xi_{j-1} \leftarrow \xi_j \rightarrow \xi_{j+1}$. There are several possibilities.

Case 1: Both reductions are $\rightarrow_\times$. In this case, $\xi_{j-1}\downarrow = \xi_{j+1}\downarrow$. Therefore, $\xi_{j-1} \leftarrow \xi_j \rightarrow \xi_{j+1}$ can be replaced by

$$\xi_{j-1} \overset{*}{\rightarrow}_\times \xi_{j-1}\downarrow = \xi_{j+1}\downarrow \overset{*}{\leftarrow}_\times \xi_{j+1},$$

which is easily verified to be less than $\xi_{j-1} \leftarrow \xi_j \rightarrow \xi_{j+1}$. This contradicts the minimality.

Case 2: One reduction is $\rightarrow_\times$ and the other $\rightarrow_{R^\infty}$. We can assume $\xi_{j-1} \leftarrow_\times \xi_j \rightarrow_{R^\infty} \xi_{j+1}$ without generality. There are three subcases.

Subcase 1: $\xi_j = \varphi + aXX\alpha$, $\xi_{j-1} = \varphi + aX\alpha$, $\varphi \rightarrow_{R^\infty} \varphi'$, and $\xi_{j+1} = \varphi' + aXX\alpha$

Subcase 2: $\xi_j = \varphi + aXX\alpha$, $\xi_{j-1} = \varphi + aX\alpha$, $a\alpha \rightarrow_{R^\infty} \psi$, and $\xi_{j+1} = \varphi + XX\psi$

Subcase 3: $\xi_j = \varphi + aXX\alpha\beta$, $\xi_{j-1} = \varphi + aX\alpha\beta$, $aX\alpha\beta \rightarrow_{bX\alpha\oplus\phi} \psi$, for $bX\alpha \oplus \phi$ and $\xi_{j+1} = \varphi + X\psi$

We consider only Subcase 3. The others are much simpler. Let $\varphi \rightarrow_{bX\alpha\oplus\phi} \varphi'$ by rewriting a monomial of a form $cX\alpha\beta$ in φ. (If this is not possible, it is just a dummy reduction). Then, $\xi_{j-1} = \varphi + aX\alpha\beta \rightarrow_{bX\alpha\oplus\phi} \varphi' + \psi \leftarrow_{bX\alpha\oplus\phi} \varphi + \psi =_{X\psi+\psi} \varphi + X\psi = \xi_{j+1}$. Note that $X\psi + \psi = ab\beta(X\phi + \phi)$. By the condition (ii) of the definition of the algorithm, $X\phi + \phi \in E_k$ for some k. By replacing $=_{X\psi+\psi}$ by an evidence using $=_{X\phi+\phi}$, we can easily get an evidence of $\xi_{j-1} \overset{*}{\leftrightarrow}_{(E_k,R_k)} \xi_{j+1}$ which is smaller than the original evidence $\xi_{j-1} \leftarrow \xi_j \rightarrow \xi_{j+1}$. This contradicts the minimality.

Case 3: Both reductions are $\rightarrow_{R^\infty}$. There are three subcases.

Subcase 1: $\xi_j = \varphi + a\alpha + b\beta$, $a\alpha \rightarrow_{R^\infty} \psi$, $\xi_{j-1} = \varphi + \psi + b\beta$, $b\beta \rightarrow_{R^\infty} \phi$, and $\xi_{j+1} = \varphi + a\alpha + \phi$

Subcase 2: $\xi_j = \varphi + c\alpha\beta\gamma$, $a\alpha \oplus \psi, b\beta \oplus \phi \in R^\infty$, $\xi_{j-1} = \varphi + c(1+a)\alpha\beta\gamma + ca\beta\gamma\psi$, and $\xi_{j+1} = \varphi + c(1+b)\alpha\beta\gamma + cb\alpha\gamma\phi$, where $ca, cb \neq 0$.

Subcase 3: $\xi_j = \varphi + c\alpha\beta\gamma\delta$, $a\alpha\beta \oplus \psi, b\beta\gamma \oplus \phi \in R^\infty$, $\xi_{j-1} = \varphi + c(1+a)\alpha\beta\gamma\delta + ca\gamma\delta\psi$, and $\xi_{j+1} = \varphi + c(1+b)\alpha\beta\gamma\delta + cb\alpha\delta\phi$, where $ca, cb \neq 0$, and $\alpha \cap \gamma = \emptyset$.

We consider only Subcase 3. The others are much simpler. $\xi_{j-1} = \varphi + c(1+a)\alpha\beta\gamma\delta + ca\gamma\delta\psi$ $\rightarrow_{b\beta\gamma\oplus\phi} \varphi + c(1+a)(1+b)\alpha\beta\gamma\delta + c(1+a)b\alpha\delta\phi + ca\gamma\delta\psi \overset{*}{\rightarrow}_\times (\varphi + c(1+a)(1+b)\alpha\beta\gamma\delta + c(1+a)b\alpha\delta\phi + ca\gamma\delta\psi)\downarrow =_{(b\gamma\psi+a\alpha\phi)\downarrow} (\varphi + c(1+a)(1+b)\alpha\beta\gamma\delta + c(1+b)a\gamma\delta\psi + cb\alpha\delta\phi)\downarrow \overset{*}{\leftarrow}_\times \varphi + c(1+a)(1+b)\alpha\beta\gamma\delta + c(1+b)a\gamma\delta\psi + cb\alpha\delta\phi \leftarrow_{a\alpha\beta\oplus\psi} \varphi + c(1+b)\alpha\beta\gamma\delta + cb\alpha\delta\phi = \xi_{j+1}$. Note that $(b\gamma\psi + a\alpha\phi)\downarrow = cp(a\alpha\beta \oplus \psi, b\beta\gamma \oplus \phi)$. By the condition (ii) of the algorithm, this is in E_k for some k. It is easy to see the above evidence is smaller than the original evidence. (When $ab = 0$, $(\varphi + c(1+a)(1+b)\alpha\beta\gamma\delta + c(1+a)b\alpha\delta\phi + ca\gamma\delta\psi)\downarrow = (\varphi + c(1+a)(1+b)\alpha\beta\gamma\delta + c(1+b)a\gamma\delta\psi + cb\alpha\delta\phi)\downarrow$. Hence critical pair is not needed.)

This contradicts the minimality. ∎

Lemma 3.17
$\{\rightarrow_\varphi | \varphi \in R^\infty\} \cup \{\rightarrow_\times\}$ is a confluent and terminating rewriting system on polynomials for equivalence relation $\overset{*}{\leftrightarrow}_{(E,R)}$.

Proof: Confluence is an easy consequence of the above lemma and its proof. Termination is Corollary 2.3. ∎

Lemma 3.18
Let φ and ψ be arbitrary Boolean polynomials such that $\varphi \overset{*}{\leftrightarrow}_{(E,R)} \psi$, then there is a Boolean polynomial, ϕ, such that $\varphi \overset{*}{\Rightarrow}_{R^\infty} \phi$ and $\psi \overset{*}{\Rightarrow}_{R^\infty} \phi$.

Proof: Let ϕ be the normal form of φ and ψ by $\{\rightarrow_\zeta | \zeta \in R^\infty\} \cup \{\rightarrow_\times\}$. Since the rewriting system is confluent and terminating, whichever order we take for applying rewriting rules, we finally reach ϕ from φ or ψ. Apply $\rightarrow_\times$ as far as possible in the reductions from φ and ψ. Then we get reductions $\varphi \overset{*}{\Rightarrow}_{R^\infty} \phi$ and $\psi \overset{*}{\Rightarrow}_{R^\infty} \phi$. ∎

Lemma 3.19
The same statement as the above lemma holds for some R_i instead of R^∞.

Proof: Since E_0 is finite, only a finite number of Variables appear in the algorithm. Moreover only finite number of elements of B (say S) appear as coefficient of Boolean polynomials in E_0. Note that any coefficient of Boolean polynomials in $\cup_i(E_i \cup R_i)$, is in the subalgebra generated by S which is also finite. Therefore only finite number of Boolean polynomials appear in the algorithm. Especially R^∞ is finite. Therefore, there exists some R_i such that $R^\infty \subseteq R_i$ by definition of R^∞. Clearly the assertion holds for this R_i. ∎

Proof of the last statement of the definition of the algorithm: We first show the termination of the algorithm and that R is a Boolean Gröbner base, i.e. it has the properties (i) and (ii).

Note that for each k, $\psi \in E_k \Longrightarrow \psi \overset{*}{\leftrightarrow}_{(E,R)} 0$. Take i such that the above lemma holds. Since any φ in E_i is reduced to 0 by $\Rightarrow_{R_i}$, by applying Rules 1 and 2 several times, say l-times, E_{i+l} will be empty, i.e. the algorithm terminates, and output R_{i+l} for R. Note that the above lemma also holds for R_{i+l}. Therefore, in order to see R has the "only if" part of (i) of the definition of Boolean Gröbner base, it suffices to show the next lemma.

Lemma 3.20
Let I be an ideal generated by a finite set, E, of Boolean polynomials. Then for each Boolean polynomial, φ and ψ,

$$\varphi \equiv \psi \pmod{I} \quad \text{iff} \quad \varphi \overset{*}{\leftrightarrow}_{(E_0,R_0)} \psi.$$

Proof: Easy to check. ∎

"if" part is straightforward, since $\zeta \in I$ for each $\zeta \in R$. The property (ii) of the definition clearly holds by the definition of algorithm.

To complete the proof, it suffices to show $\Rightarrow_R$ and $\Rightarrow_{Glue(R)}$ have the same normal form. The property (iii) is trivial.

Lemma 3.21
$\Rightarrow_R$ and $\Rightarrow_{Glue(R)}$ have the same normal form, i.e. for each Boolean polynomial φ, the irreducible forms by reductions $\Rightarrow_R$ and $\Rightarrow_{Glue(R)}$ are same.

Proof:

Let $a_1\alpha \oplus \phi_1, \ldots, a_n\alpha \oplus \phi_n$ be all Boolean polynomials in R which has α as the largest Boolean product. Let $a = a_1 + \ldots + a_n$, $\phi = \phi_1 + \ldots + \phi_n$ and $a\alpha \oplus \phi$ in $Glue(R)$. Note that when we do reductions to get a normal form by $\Rightarrow_R$, we can choose whatever order of reductions we like. For a monomial of the form $b\alpha\beta$, apply $\Rightarrow_{a_1\alpha\oplus\phi_1}, \ldots, \Rightarrow_{a_n\alpha\oplus\phi_n}$ in this order as far as possible. Then we get $b\alpha\beta \rightarrow_{a_1\alpha\oplus\phi_1} b(1+a_1)\alpha\beta + ba_1\beta\phi_1 \Rightarrow_{a_2\alpha\oplus\phi_2} b(1+a_1)(1+a_2)\alpha\beta + b(1+a_1)a_2\beta\phi_2 + ba_1\beta\phi_1 \Rightarrow \ldots \Rightarrow_{a_n\alpha\oplus\phi_n} b(1+a_1)(1+a_2)\ldots(1+a_n)\alpha\beta + b(1+a_1)(1+a_2)\ldots(1+a_{n-1})a_n\beta\phi_n + \ldots + b(1+a_1)a_2\beta\phi_2 + ba_1\beta\phi_1 = b(1+a_1+\ldots+a_n)\alpha\beta + ba_n\beta\phi_n + \ldots + ba_1\beta\phi_1$ (since $a_ia_j = 0$ if $i \neq j$) $= b(1+a)\alpha\beta + b\beta(a_1\phi_1 + \ldots + a_n\phi_n)$ $= b(1+a)\alpha\beta + ba\beta\phi$ (since $a\phi = a\phi_1 + \ldots + a\phi_n \Longrightarrow a_i\phi = a_i\phi_i$ for each $i \Longrightarrow a\phi = a_1\phi + \ldots + a_n\phi - a_1\phi_1 + \ldots + a_n\phi_n$) We can nomore reduce this by any $\Rightarrow_{a_i\alpha\oplus\phi_i}$. We also have $b\alpha\beta \Rightarrow_{a\alpha+\phi} b(1+a)\alpha\beta + ba\beta\phi$. By the above, we can see $\Rightarrow_R$ and $\Rightarrow_{Glue(R)}$ have the same normal form. ∎

The next lemma is an important property of normal Boolean Gröbner base.

Lemma 3.22
Under a fixed admissible ordering on Boolean monomials, normal Boolean Gröbner base is determined unique.

Proof:

Easily proved by property (ii) and (iii). ∎

REFERENCES

[Bachmair 86] Bachmair, L., Dershowitz, N., and Hsiang, J.: *Ordering for equational proof*, Proc. Symp. Logic in Computer Science, Cambridge, Massachusetts (June 1986)

[Buchberger 83] Buchberger, B.: *Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory*, Technical Report, CAMP-LINTZ (Nov. 1983)

[Dershowitz 79] Dershowitz, N. and Manna, Z.: *Proving termination with multiset orderings*, Comm. ACM 22, pp. 465-467 (1979)

[Dickson 13] Dickson, L. E.: *Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors*, Am. J. of Math., vol. 35, pp. 413-426 (1913)

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

[Huet 80] Huet, G. and Oppen, D. C.: *Equations and Rewrite Rules: a survey*, Formal Language: Perspectives and Open Problems Academic Press, pp. 349-405 (1980)

[Knuth 70] Knuth, D. E. and Bendix, P. B.: *Simple word problems in universal algebras*, Computational problems in abstract algebra, Pergamon Press, Oxford (1970)

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

[SaSa 90] Sakai, K. and Sato, Y.: *Zero-point theorem for Boolean polynomial ring*, ICOT Technical Memorandum (1990)

[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)