ソフトウェア基礎論　３２－５
(1989.11.13)

ブール方程式の可解性について

坂井公、佐藤洋祐

新世代コンピュータ技術開発機構
〒108 東京都港区三田 1-4-28

あらまし　ブール方程式が解を持つための必要十分条件を与える。この条件はブール制約を記述することを許すような制約論理プログラミング言語の処理系を考える上で重要な指針となる。

A note on solvability of Boolean equations

Kô Sakai and Yosuke Sato

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

Abstract　This note gives a necessary and sufficient condition for a set of Boolean equations to have solutions. This condition is an important guide to consider implementation of a constraint logic programming language with Boolean constraints.

1. Introduction

In constraint logic programming (see [Sakai 89], example) there are applications, in which we often want to write constraints about membership and inclusion of sets such as $a \in X$ and $X \subset Y$. These constraints can be written in the form of Boolean equations, such as $\{a\} \wedge X = \{a\}$ and $X \wedge Y = X$, on a Boolean algebra of sets. Therefore, if we have a general method to handle Boolean equations, it can be used as a constraint solver in the constrain logic programming system where constraints like the above are freely written.

The most primitive feature required of such a method is decision of solvability of a given set of equations. To address the decision problem, this note gives a necessary and sufficient condition for a set of Boolean equations to have solutions.

2. Boolean ring

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

For a Boolean algebra $< B, \vee, \wedge, \neg >$, define $a + b = (a \vee \neg b) \wedge (\neg a \vee b)$ and $a \times b = a \wedge b$ for each a, b in B, then $< B, \times, + >$ is known to be a commutative ring with a unit with the following properties.

$$\forall a \in B \quad a \times a = a \qquad \text{(idempotence)}$$

A ring with these properties is called a Boolean ring. As usual, we often abbreviate $\times$ symbols ($a \times b$ is denoted ab, for example) if there is no danger of confusion.

A Boolean ring becomes a lattice if the order $a \leq b$ is defined as $ab = a$. Given a subset F of a Boolean ring B, let IF denote the ideal generated by F. IF is characterized in two different but equivalent ways, namely

$$IF = \{b_1 a_1 + \cdots + b_n a_n \mid b_1, \ldots, b_n \in B, a_1, \ldots, a_n \in F\}$$

and

$$IF = \{b \mid \exists a_1, \ldots, a_n \in F \quad b \leq a_1 \vee \cdots \vee a_n\}$$

The following lemma is immediate from the second characterization.

Lemma 2.1

Let $F = \{a_1, \ldots, a_n\}$ be a finite subset of a Boolean ring. Then,

(1) $\sup F \in IF$,

(2) $a \leq \sup F$ for all $a \in IF$,

where $\sup F$ is the least upper bound of F, $a_1 \vee \cdots \vee a_n$. Therefore, for a finite subset F, IF is a principal ideal generated by $\sup F$, namely $IF = I\{\sup F\}$.

3. Boolean equation

In what follows, let B be a fixed Boolean ring. Elements of B are denoted by symbols $a, b, c, \ldots$ (possibly with suffix).

Definition 3.1

Let us have a set V of *Boolean variables*. We do not put any constraint on the cardinality of V for generality of the theory. Boolean variables are denoted by symbols $x, y, z, \ldots$ (possibly with suffix). A *Boolean power product* is an expression of the form

$$x_1 \ldots x_n \ (0 \leq n),$$

where $x_1, \ldots, x_n$ are distinct Boolean variables. In the case $n = 0$, the power product is denoted by 1. We use symbols $\alpha, \beta, \gamma, \ldots$ (possibly with suffix) for Boolean power products. A *Boolean polynomial* is an expression of the form

$$a_1 \alpha_1 + \cdots + a_n \alpha_n \ (0 \leq n),$$

where $a_1, \ldots, a_n$ are non-zero elements of B, and $\alpha_1, \ldots, \alpha_n$ are distinct Boolean power products. In the case $n = 0$, the polynomial is denoted by 0. We use symbols $\phi, \psi, \ldots$ (possibly with suffix) for Boolean polynomials. The set of all Boolean polynomials is denoted $B[V]$.

It is well-known that $B[V]$ forms a Boolean ring by computation using the basic properties of a ring (that

is, distributivity of $\times$ w.r.t. $+$, commutativity and associativity of $+$ and $\times$) and the idempotence law. For example,

$$(ax + by)(cx + d) = (ac + ad)x + (bc)xy + (bd)y.$$

A Boolean equation is a formula of the form $\phi \simeq \psi$ where ϕ and ψ are Boolean polynomials. (We do not use the symbol $=$ in a Boolean equation, to avoid confusion.)

A function σ from V to B is called a *substitution*. A substitution is obviously extended to a homomorphism from $B[V]$ to B. That is, $(\phi\psi)\sigma = (\phi\sigma)(\psi\sigma)$ and $(\phi + \psi)\sigma = (\phi\sigma) + (\psi\sigma)$ for all ϕ and ψ in $B[V]$. (According to tradition, we will use postfix notation for substitution.)

Let E be a set of Boolean equations. A substitution σ is called a solution of E if $\phi\sigma = \psi\sigma$ for all $\phi \simeq \psi \in E$. E is called *solvable* if it has solutions. Since $\phi \simeq \psi$ and $\phi + \psi \simeq 0$ have the same solution, we can assume every Boolean equation has the form $\phi \simeq 0$ without loss of generality. For a set of Boolean polynomials F, we denote the set of Boolean equations $\{\phi \simeq 0 \mid \phi \in F\}$ by $F \simeq 0$.

The following lemma is clear from either of the characterizations of ideals in Section 1.

Lemma 3.2

Let F be a set of Boolean polynomial and σ is a solution of $F \simeq 0$. Then σ is a solution $I(F) \simeq 0$

4. Unsolvability of Boolean equations

Lemma 4.1

Let ϕ be a Boolean polynomial and let $x_1, \ldots, x_n$ be all the variables occurring in ϕ. If $\{\phi \simeq 0\}$ is unsolvable, then there exists a polynomial $\psi \in I\{\phi\}$ with variables $x_1, \ldots, x_{n-1}$ only such that $\{\psi \simeq 0\}$ is unsolvable. Namely, variable x_n can be eliminated.

Proof: We can put $\phi = \phi_1 x_n + \phi_0$ where ϕ_0 and ϕ_1 are polynomials with variables $x_1, \ldots, x_{n-1}$ only. Then ψ is defined as $\phi_1\phi_0 + \phi_0$. It is easy to verify that $\psi = (\phi_1 x_n + \phi_1 + \phi_0)\phi$. Therefore, $\psi \in I\{\phi\}$. It remains to be shown that ψ is unsolvable. Assume that there is a solution σ of $\{\psi \simeq 0\}$. Then,

$$\psi\sigma = (\phi_1\sigma)(\phi_0\sigma) + \phi_0\sigma = 0.$$

Let us consider the substitution σ', which differs from σ only in that its value at x_n is $\phi_0\sigma$. Namely, $x_n\sigma' = \phi_0\sigma$ and $x\sigma' = x\sigma$ for any other variable x. Clearly, $\phi\sigma' = 0$, which contradicts that $\{\phi \simeq 0\}$ is unsolvable. ∎

Lemma 4.2

Let ϕ be a Boolean polynomial. Then $\{\phi \simeq 0\}$ is unsolvable if and only if there is a non-zero polynomial $\psi \in I\{\phi\}$ without variables. In other words, there is a non-zero intersection between B and $I\{\phi\}$, since a polynomial without variables can be regarded as an element of B.

Proof: The if part is obvious. In order to prove the only-if part, let us use Lemma 4.1 to eliminate variables in ϕ one by one. The proof is easily completed by induction on the number of variables in ϕ. ∎

Theorem 4.3

Let F be a finite set of Boolean polynomials. Then $F \simeq 0$ is unsolvable if and only if there is a non-zero polynomial $\psi \in IF$ without variables.

Proof: It is clear that E is solvable if and only if $\{\sup F \simeq 0\}$ is solvable. Therefore, the proof is easily completed by Lemma 4.2 and Lemma 2.1. ∎

The above theorem does not hold in the case that F is not finite. In order to see this, let $\mathbf{N}$ be the set of all natural numbers and B the class of all finite subsets and cofinite subsets (that is, the subsets whose complements are finite) of $\mathbf{N}$. It is clear that B forms a Boolean algebra with respect to usual set operations. Consider the following infinite set of Boolean polynomials:

$$F = \{\{2n\}x + \{2n\}, \{2n + 1\}x \mid n \in \mathbf{N}\}$$

Intuitively, the equation set $F \simeq 0$ means that x is the subset consisting of all and only the even numbers, which is neither finite nor cofinite. Therefore, $F \simeq 0$ is unsolvable in the above B. It is solvable, however, if B is the class of all subsets of $\mathbf{N}$, which is also a Boolean algebra. Therefore, from Lemma 3.2, there cannot be any non-zero polynomial without variables in $I(F)$.

References

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

[Sakai 89] Sakai, K. and Aiba, A.: *CAL: A theoretical background of constraint logic programming and its applications*, to appear in J. Symbolic Computation (1989)

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

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