Mathematica Balkanica

Mathematical Society of South-Eastern Europe
A quarterly published by
the Bulgarian Academy of Sciences – National Committee for Mathematics

---

New Series Vol.11, 1997, Fasc. 1-2

Boolean Ring Equations [1]

Dragić Banković

Presented by Ž. Mijajlović

If a particular solution of an equation over a Boolean ring is known, Löwenheim's theorem determines a general solution of this equation (see for instance, [7]). In this paper we reduce the finding of a particular solution to solving simple equations in two-element Boolean ring, i.e. on $\{0,1\}$. In the similar way we also determine general solutions of any equations over a Boolean ring, where we do not suppose that a particular solution is known.

1. Introduction

Solving of equations is a basic inference mechanism in algebraic manipulation of formulas, automated reasoning and some programming languages. Since this paper is concerning with general solution we firstly state the definition of a general solutions.

Definition 1. Let E be a given non-empty set and Q be a given unary relation of E. A formula $x = \varphi(t)$, where $\varphi E - E$ is a given function, represents a general solution of the x-equation $Q(x)$ if and only if

$$(\forall t)Q(\varphi(t)) \wedge (\forall x)(Q(x) \Rightarrow (\exists t)x = \varphi(t).$$

We say that the equation $Q(x)$ is consistent if there is $y \in E$ such that $Q(y)$ is true.

2. Boolean functions and Boolean polynomials

Let $N = \{1, ..., n\}$, where n is a natural number.

[1]This research was supported by Science Found of Serbia, Grant number 0401A, through Matematički institut

Theorem 1 [9]. *A mapping f $B^n \to B$ is Boolean function if and only if it can be written in the canonical disjunctive form*

$$f(X) = \bigcup_A f(A)X^A,$$

where $\bigcup_A$ means the union over all $A \in \{0,1\}^n$. f is a simple Boolean function if $(\forall A \in \{0,1\}^n) f(A) \in \{0,1\}$.

Theorem 2 [9]. *A mapping f $B^n \to B$ is a Boolean polynomial if and only if it can be written in the canonical polynomial form*

$$f(X) = \sum_{S \subset N} b_s \prod_{i \in S} x_i.$$

f is a simple Boolean polynomial if an only if $(\forall S \in N) b_s \in \{0,1\}$.

Theorem 3 [9]. *Let $\mathcal{B} = (B, \cup, \cdot, ', 0, 1)$ be a Boolean algebra and n natural number. A mapping f $B^n \to B$ is a Boolean function if and only if it is polynomial of the Boolean ring $\mathcal{R} = (B, +, \cdot, 0, 1)$.*

3. Boolean equations

In this section we collect some background material about Boolean equations. A detailed account is given in [9]. We shall use the notation: $X = (x_1, ..., x_n)$ and $T = (t_1, ..., t_n)$.

Given an arbitrary Boolean algebra $\mathcal{B}$, a Boolean equation in n unknowns over $\mathcal{B}$ is an equation of the form $g(X) = h(X)$, where g, h $B^n \to B$ are Boolean functions.

Theorem 4 [9]. *Every Boolean equation or system of Boolean equations is equivalent to a single Boolean equation of the form $f(X) = 0$, where f is a Boolean function.*

Theorem 5 [9]. *The Boolean equation $f(X) = 0$ is consistent if and only if*

$$\prod_A f(A) = 0,$$

where $\prod_A$ means the product over all $A \in \{0,1\}^n$.

Theorem 6 [4]. *Let $f, g_1, ..., g_n$ $B^n \to B$ be Boolean functions and $G = (g_1, ..., g_n)$. The formula*

$$X = G(T)$$

(or, in scalar form, $x_j = g_j(t_1, ..., t_n)$ $(j = 1, ..., n)$) represents a general solution of the consistent equation $f(X) = 0$ if and only if

$$(\forall T)(f(T) = \prod_A \bigcup_{j=1}^{n} (g_j(A) + t_j)).$$

Theorem 7 [9]. *Let f, g $B^n \to B$ be Boolean functions and assume that $\prod_A f(A) = 0$. Then the following conditions are equivalent:*

$$(\forall X \in B^n)(f(X) = 0 \Rightarrow g(X) = 0)$$
$$(\forall X \in B^n)(g(X \leq f(X))$$
$$(\forall X \in \{0,1\}^n)(g(X) \leq f(X)).$$

We prove now a lemma that will be used in the proofs of Theorem 9 and Theorem 10.

Lemma. *Let g $B^n \to B$ be a Boolean function and f $B^n \to B$ be a simple Boolean function. If $\prod_A f(A) = 0$, then the conditions*
(a) $(\forall X \in B^n)(f(X) = 0 \Rightarrow g(X) = 0)$
(b) $(\forall A \in \{0,1\}^n)(f(A) = 0 \Rightarrow g(A) = 0)$
are equivalent.

Proof. $(a) \to (b)$ is trivial. Since f is the simple Boolean function, we have $(\forall A \in \{0,1\}^n)(f(A) \in \{0,1\}$. Let (b) hold. If $f(A) = 0$, then $g(A) = 0$, i.e. $g(A) \leq f(A))$. If $f(A) = 1$, then $g(A) \leq f(A) = 1$. Therefore we have $(\forall A \in \{0,1\}^n)(g(A) \leq f(A))$. Since the latter formula is equivalent to (a), by Theorem 3, $(b) \to (a)$ is proved. ∎

4. Boolean ring equations

Given an arbitrary Boolean ring $\mathcal{R}$, a Boolean ring equation in n unknowns over $\mathcal{B}$ is an equation of the form $g(X) = h(X)$, where g, h $B \times B \to B$ are Boolean polynomials. Taking in mind Theorem 3 and Theorem 4, every Boolean ring equation is equivalent to a single Boolean ring equation of the form $f(X) = 0$, where f is a Boolean polynomial.

Theorem 8 [9]. *The Boolean ring equation*

$$\sum_{s \subset N} b_s \prod_{i \in S} x_i = 0$$

is consistent (i.e. $(\exists X)\sum_{s\subset N} b_s \prod_{i\in S} x_i = 0$*) if and only if*

$$b_\emptyset \prod_{\emptyset\neq S\subset N} (b_s + 1) = 0.$$

4.1 Particular solutions

Theorem 9. *Let* Y *is the m-tuple* $(m < 2^n)$ *of all different elements* b_s *from* $\sum_{s\subset N} b_s \prod_{1\in S} x_i = 0$ *and let* $h(X,Y) = \sum_{s\subset N} b_s \prod_{i\in S} x_i$. *If* $b_\emptyset \prod_{\emptyset\neq S\subset N}(b_s + 1) = 0$, *then the formulas*

$$(1)\qquad p_j = \sum_C z_{j,C} Y^C \quad (j = 1,\dots,n)$$

($\sum_C$ *means the sum over all* $C \in \{0,1\}^m$*) represents a particular solution of Boolean ring equation* $h(X,Y) = 0$ *with respect to* X*, if and only if*

$$(2)\qquad (\forall Y \in V) h(z_{1,Y},\dots,z_{m,Y},Y) = 0,$$

where

$$V = \{Y | Y \in \{0,1\}^m \quad \wedge \quad (\exists X) h(X,Y) = 0\}, \text{ i.e.}$$

$$(3)\qquad V = \{Y | Y \in \{0,1\}^m \quad \wedge \quad b_\emptyset \prod_{\emptyset\neq S\subset N} (b_s + 1) = 0\}.$$

P r o o f. It is obvious that a particular solution $(p_1,\dots,p_n)$ of the equation $h(X,Y) = 0$ depends on Y, i.e. it is of the form

$$p_j = \sum_C z_{j,C} Y^C \quad (j = 1,\dots,n),$$

because of Theorem 3 and Lemma.

Therefore we have the following equivalences:

$$(\forall Y \in B^m)(b_\emptyset \prod_{\emptyset\neq S\subset N} (b_s + 1) = 0 \Rightarrow h(\sum_C z_{1,C}Y^C,\dots,\sum_C z_{n,C}Y^C, Y) = 0)$$

$$\Leftrightarrow (\forall Y \in \{0,1\}^m)(b_\emptyset \prod_{\emptyset\neq S\subset N}(b_s + 1) = 0$$
$$\Rightarrow h(\textstyle\sum_C z_{1,C}Y^C,\dots,\sum_C z_{n,C}Y^C, Y) = 0)$$

(because of Theorem 4 and Lemma)

$$\Leftrightarrow (\forall Y \in V) h(\sum_C z_{1,C}Y^C,\dots,\sum_C z_{n,C}Y^C, Y) = 0$$

$$(V = \{Y | Y \in \{0,1\}^m \quad \wedge \quad b_\emptyset \prod_{\emptyset \neq S \subset N} (b_s + 1) = 0\})$$

$$\Leftrightarrow (\forall Y \in V) h(z_{1,Y}, ..., z_{n,Y}, Y) = 0$$

(because $(\forall Y \in V)(\forall j \in N)(\sum_C z_{j,C} Y^C = z_{j,Y})$. ∎

The algorithm for solving the latter system has been given in [7].

If we find $z_{1,Y}, ..., z_{n,Y}$ we get the particular solution (1).

4.2 General solutions

Theorem 10. *Let Y be the m-tuple ($m < 2^n$) of all different elements b_s from $\sum_{S \subset N} b_S \prod_{i \in S} x_i = 0$ and let $h(X,Y) = \sum_{S \subset N} b_S \prod_{i \in S} x_i$. If $b_\emptyset \prod_{\emptyset \neq S \subset N} (b_s + 1) = 0$, then the formulas*

$$x_j = \sum_D (\sum_C u_{j,D,C} Y^C) T^D \quad (j = 1, ..., n) \tag{4}$$

($\sum_D$ means the sum over all $D \in \{0,1\}^n$ and $\sum_C$ means the sum over all $C \in \{0,1\}^m$) represent a general solution of Boolean ring equation $h(X,Y) = 0$, with respect to X, if and only if

$$(\forall X \in \{0,1\}^n)(\forall Y \in V) h(X,Y) = \prod_A \bigcup_{j=1}^{n} (z_{j,A,Y} + x_j), \tag{5}$$

where $V = \{Y | Y \in \{0,1\}^m \quad \wedge \quad b_\emptyset \prod_{\emptyset \neq S \subset N} (b_s + 1) = 0\}$.

Proof. If $h(X,Y) = \sum_{S \subset N} b_S \prod_{i \in S} x_i$ and $b_\emptyset \prod_{\emptyset \neq S \subset N} (b_s + 1) = 0$, it is obvious that a general solution

$$x_j = \sum_D g_{j,D} T^D \quad (j = 1, ..., n)$$

of Boolean ring equation $h(X,Y) = 0$ is of the form

$$x_j = \sum_D (\sum_C q_{j,D,C} Y^C) T^D \quad (j = 1, ..., n),$$

since the coefficients $g_{j,D}$ depend on Y, i.e.

$$g_{j,D} = \sum_C q_{j,D,C} Y^C \quad (j \in \{1, ..., n\}, D \in \{0,1\}^n)$$

by Theorem 3 and Theorem 1.

Taking in mind Theorem 7, we have the following equivalences:

$$(\forall Y \in B^m)\Big(b_\emptyset \prod_{\emptyset\neq S\subset N}(b_s+1)=0 \Rightarrow (\forall X\in B^n)h(X,Y)=\prod_A \bigcup_{j=1}^n(\sum_D(\sum_C z_{j,D,C}Y^C)A^D+x_j)\Big)$$
$$\Leftrightarrow (\forall Y \in B^m)\Big(b_\emptyset \prod_{\emptyset\neq S\subset N}(b_s+1)=0 \Rightarrow (\forall X\in B^n)h(X,Y)+\prod_A \bigcup_{j=1}^n(\sum_D(\sum_C z_{j,D,C}Y^C)A^D+x_j)=0\Big)$$

(because $(\forall a,b\in B)\ (a=b \Leftrightarrow a+b=0)$)

$$\Leftrightarrow (\forall X \in B^m)(\forall Y\in B^n)\Big(b_\emptyset \prod_{\emptyset\neq S\subset N}(b_s+1)=0 \Rightarrow h(X,Y)+\prod_A \bigcup_{j=1}^n(\sum_D(\sum_C z_{j,D,C}Y^C)A^D+x_j)=0\Big)$$
$$\Leftrightarrow (\forall X \in \{0,1\}^n)(\forall Y\in \{0,1\}^m)\Big(b_\emptyset \prod_{\emptyset\neq S\subset N}(b_s+1)=0 \Rightarrow h(X,Y)+\prod_A \bigcup_{j=1}^n(\sum_D(\sum_C z_{j,D,C}Y^C)A^D+x_j)=0\Big)$$

(by Theorem 3 and Lemma)

$$\Leftrightarrow (\forall X\in\{0,1\}^n)(\forall Y\in V)h(X,Y)+\prod_A\bigcup_{j=1}^n(\sum_D(\sum_C z_{j,D,C}(Y)A^D+x_j)=0$$

$$\Leftrightarrow (\forall X\in\{0,1\}^n)(\forall Y\in V)h(X,Y)+\prod_A\bigcup_{j=1}^n(\sum_D(\sum_C z_{j,D,C}Y^C)A^D+x_j)$$

$$\Leftrightarrow (\forall X\in\{0,1\}^n)(\forall Y\in V)h(X,Y)=\prod_A\bigcup_{j=1}^n(\sum_C z_{j,A,C}Y^C)+x_j))$$

$$\Leftrightarrow (\forall X\in\{0,1\}^n)(\forall Y\in V)h(X,Y)=\prod_A\bigcup_{j=1}^n(z_{j,A,Y}+x_j).$$

If we solve the system (5) we get the general solution (4).

If we take $Y^*\in V$, we get the system of 2^n equations:

$$(\forall X\in\{0,1\}^n)\ h(X,Y^*)=\prod_A\bigcup_{j=1}^n(z_{j,A,Y^*}+x_j). \tag{6}$$

Remark 1.

(a) The system (6) does not contain the unknowns occurring in other equations of the system (5).

(b) Let S_h be the solution set of $h(X,Y^*)=0$. If we take

$$\{(z_{1,A,Y^*},\dots,z_{n,A,Y^*})|A\in\{0,1\}^n\}=S_h,$$

then the equation

$$h(X, Y^*) = \prod_A \bigcup_{j=1}^{n} (z_{j,A,Y^*} + x_j)$$

is satisfied. Namely, if $h(X, Y^*) = 0$, then

$$(z_{1,A,Y^*}, ..., z_{n,A,Y^*}) = (x_1, ..., x_n) \text{ for some } A \in \{0,1\}^n,$$

i.e.

$$z_{j,A,Y^*} = x_j \quad (j = 1, ..., n) \quad \text{for some } A \in \{0,1\}^n,$$

i.e.

$$\bigcup_{j=1}^{n} (z_{j,A,Y^*} + x_j^*) = 0 \quad \text{for some } A \in \{0,1\}^n,$$

i.e.

$$\prod_A \bigcup_{j=1}^{n} (z_{j,A,Y^*} + x_j^*) = 0.$$

(c) If $Y_0 \notin V$, then $(z_{1,A,Y_0}, ..., z_{n,A,Y_0})$ $(A \in \{0,1\}^n)$ can be arbitrary element from $\{0,1\}^n$ because the n-tuple $(z_{1,A,Y_0}, ..., z_{n,A,Y_0})$ does not occur in (6).

The previous Remark 1 gives simple algorithm for solving the system (5).

If we use the known methods for solving Boolean ring equations ([9]), we really solve these equations in a Boolean ring $\mathcal{B}$ or in some ring $\mathcal{B}'$ generated by the coefficient appearing in these equations ([7]). Our Theorem 10 reduces the finding of a general solution of Boolean ring equation to solving simple equations in two element Boolean ring, i.e. in $\{0,1\}$.

Example . Determine a general solution of the equation

$$axy + ay + b = 0$$

in arbitrary Boolean ring with unit.

Note that $V = \{(0,0), (1,0), (1,1)\}$ because of Theorem 9. Let

$$\begin{aligned}
g_1(t_1, t_2, a, b) &= (p_{0,0}a'b' + p_{0,1}a'b + p_{0,2}ab' + p_{0,3}ab)t_1't_2' \\
&= (p_{1,0}a'b' + p_{1,1}a'b + p_{1,2}ab' + p_{1,3}ab)t_1't_2 \\
&= (p_{2,0}a'b' + p_{2,1}a'b + p_{2,2}ab' + p_{2,3}ab)t_1t_2' \\
&= (p_{3,0}a'b' + p_{3,1}a'b + p_{3,2}ab' + p_{3,3}ab)t_1t_2 \\
g_2(t_1, t_2, a, b) &= (q_{0,0}a'b' + q_{0,1}a'b + q_{0,2}ab' + q_{0,3}ab)t_1't_2' \\
&= (q_{1,0}a'b' + q_{1,1}a'b + q_{1,2}ab' + q_{1,3}ab)t_1't_2 \\
&= (q_{2,0}a'b' + q_{2,1}a'b + q_{2,2}ab' + q_{2,3}ab)t_1t_2' \\
&= (q_{3,0}a'b' + q_{3,1}a'b + q_{3,2}ab' + q_{3,3}ab)t_1t_2'.
\end{aligned}$$

The system (5) becomes

$$axy + ay + b = \prod_{i=0}^{3}((p_{i,r} + x) \cup (q_{i,r} + y)) \quad (r \in \{0,2,3\},\ (x,y) \in \{0,1\}^2),$$

i.e.

$$\begin{aligned} 0 &= \textstyle\prod_{i=0}^{3}((p_{i,0} + x) \cup (q_{i,0} + y)) \quad (x,y) \in \{0,1\}^2) \\ xy + y &= \textstyle\prod_{i=0}^{3}((p_{i,2} + x) \cup (q_{i,2} + y)) \quad (x,y) \in \{0,1\}^2) \\ xy + y + 1 &= \textstyle\prod_{i=0}^{3}((p_{i,3} + x) \cup (q_{i,3} + y)) \quad (x,y) \in \{0,1\}^2). \end{aligned}$$

Let us introduce the notations

$$\begin{aligned} R_0 &= \{(p_{0,0}, q_{0,0}), (p_{1,0}, q_{1,0}), (p_{2,0}, q_{2,0}), (p_{3,0}, q_{3,0})\} \\ R_1 &= \{(p_{0,1}, q_{0,1}), (p_{1,1}, q_{1,1}), (p_{2,1}, q_{2,1}), (p_{3,1}, q_{3,1})\} \\ R_2 &= \{(p_{0,2}, q_{0,2}), (p_{1,2}, q_{1,2}), (p_{2,2}, q_{2,2}), (p_{3,2}, q_{3,2})\} \\ R_3 &= \{(p_{0,3}, q_{0,3}), (p_{1,3}, q_{1,3}), (p_{2,3}, q_{2,3}), (p_{3,3}, q_{3,3})\} \end{aligned}$$

In accordance with Remark 1 (c), R_1 contains arbitrary elements from the set $\{0,1\}^2$. Further, the solutions sets of the equations $0 = 0$, $xy + y = 0$ and $xy + y + 1 = 0$ are $\{(0,0),(0,1),(1,0),(1,1)\}$ $\{(0,0),(1,0),(1,1)\}$ and $\{0,1),(1,0)\}$, respectively. Having in mind Remark 1 (b) we can take, for instance,

$$\begin{aligned} &\{(p_{0,0}, q_{0,0}), (p_{1,0}, q_{1,0}), (p_{2,0}, q_{2,0}), (p_{3,0}, q_{3,0})\} = \{(0,0),(0,1),(1,0),(1,1)\} \\ &R_1 = \{(p_{0,1}, q_{0,1}), (p_{1,1}, q_{1,1}), (p_{2,1}, q_{2,1}), (p_{3,1}, q_{3,1})\} = \{(0,0),(0,0),(0,0),(0,0)\} \\ &R_2 = \{(p_{0,2}, q_{0,2}), (p_{1,2}, q_{1,2}), (p_{2,2}, q_{2,2}), (p_{3,2}, q_{3,2})\} = \{(0,0),(0,0),(1,0),(1,1)\} \\ &R_3 = \{(p_{0,3}, q_{0,3}), (p_{1,3}, q_{1,3}), (p_{2,3}, q_{2,3}), (p_{3,3}, q_{3,3})\} = \{(0,1),(0,1),(1,0),(0,1)\} \end{aligned}$$

Thus, a general solution is determined by

$$\begin{aligned} x &\quad (a'b' + ab')t_1't_2 + (a'b' + ab')t_1t_2 \\ y &= abt_1't_2 + (a'b' + ab)t_1't_2 + abt_1t_2' + (a'b' + ab' + ab)t_1t_2, \end{aligned}$$

i.e.

$$\begin{aligned} x &= (b+1)t_1(t_2+1) + (b+1)t_1t_2 \\ y &= ab(t_1+1)(t_2+1) + (a+b+1)(t_1+1)t_2 + abt_1(t_2+1) + (ab+b+1)t_1t_2. \end{aligned}$$

References

[1] D. B a n k o v i ć. Some remarks on the number of the parameters of the solutions of Boolean equations. *Discrete Mathematics*, **79**, 1989/90, 229-234.

[2] D. B a n k o v i ć. A note on Boolean equations. *Bulletin de la Societe Math. de Belgique*, **41**, 1989, 1, ser B, 47-53.

[3] D. B a n k o v i ć. Certain Boolean equation. *Discrete Applied Mathematics*, **35**, 1992, 21-27.

[4] J. P. S e s c h a m p s. Parametric solutions of Boolean equations. *Discrete Mathematics*, **3**, 1972, 333-342.

[5] C. G h i l e z a n. Une généralisation du théorème de Löwenheim sur les équations de Boole. *Publ. Inst. Math. Beograd*, **11 (25)**, 1971, 57-59.

[6] L. L ö w e n h e i m. Über die Auflösung von Gleichungen im logischen Gebietkalkul. *Sitzungber. Berl. Math. Gesel.*, **7**, 1910, 89-94.

[7] U. M a r t i n, T. N i p k o w. Unification in Boolean rings. *Journal of Automated Reasoning*, **4**, 1988, 381-396.

[8] S.B. P r e š i c. Ein Satz über reproductive Lösungen. *Publ. Inst. Math. Beograd*, **14(28)**, 1973, 133-136.

[9] S. R u d e a n u. *Boolean Functions and Equations*, North-Holland, 1974.

Faculty of Science
Radoja Domanovića 12
34 000 Kragujevac
YUGOSLAVIA

Received 29.12.1992