PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série tome 42 (56), 1987, pp. 29–34

THE FORMULAS OF THE GENERAL REPRODUCTIVE SOLUTION OF AN EQUATION IN BOOLEAN RING WITH UNIT

Dragić Banković

Abstract. We explicitly give the formulas of the general reproductive solution of an equation in Boolean ring with unit. In accordance with the equivalence between Boolean algebras and Boolean rings with unit (Theorem 1) we use Vaught's theorem 2 and solve the equation in $\{0,1\}$. We allso use Presić's formula of the general reproductive solution of the equation in the finite set.

We use in this paper the operations $+$ and $\times$, where $+$ is the operation of Boolean ring and is the addition in the set of natural numbers.

THEOREM 1. [4] *Let* $(B, \cup, \cdot, ', 0, 1)$ *be a Boolean algebra and* n *a natural number. A mapping* $f : B^n \to B$ *is a Boolean function if and only if it is a polinomial of the ring* $(B, +, \cdot, 0, 1)$.

Definition 1. Let $f : B^n \to B$ be a Boolean function. The system $\psi = (\psi_1, \dots, \psi_n)$ of Boolean functions $\psi_1, \dots, \psi_n : B^n \to B$ defines the general reproductive solution of the consistent equation $f(X) = 0$, $(X = (x_1, \dots, x_n) \in B^n)$ if and only if

$$(1) \qquad (\forall X) f(\psi(X)) = 0 \ \wedge \ (\forall X)(f(X) = 0 \Rightarrow X = \psi(X)).$$

Definition 2. Horn formulas over language L are defined as follows:

— elementary Horn formulas are defined as the atomic formulas of L and the formulas of the form $F_1 \wedge \cdots \wedge F_n \Rightarrow G$, where $F_1, \dots F_n, G$ are atomic;

— every Horn formula is built from elementary Horn formulas using $\wedge$, $\forall$, $\exists$.

THEOREM 2. (Vaught, see e.g. [2]) *Let* H *be a Horn sentence in the language* L_B *of Boolean algebras. If* $B_2 \vDash H$ *then* $B \vDash H$.

COROLLARY. *Let* $T = (t_1, \dots, t_n) \in B^n$. *If* $X = \psi(T)$ *is the general reproductive solution of the Boolean equation* $f(X) = 0$ *in* B_2, *then* $x = \psi(T)$ *is the general reproductive solution of* $f(X) = 0$ *in* B.

AMS Subject Classification (1980): Primary 06E20, 03G05.

Proof. Using Vaught's theorem, because the sentence "$X = \psi(T)$ is the general reproductive solution of $f(X) = 0$" can be written as Horn sentence

$$(\forall X) f(\psi(X)) = 0 \wedge (\forall X)(f(X) = 0 \Rightarrow \psi(X)).$$

THEOREM 3 (Prešić [3]). *Let $0 \in E$ and $J : S \to E$, where $S = \{s_1, \dots, s_k\}$. Let $J(x) = 0$ be the consistent equation and C_q be a cycle of $q \in S$, i.e. $\{q, C_q(q), C_q^2(q), \dots, C_q^{k-1}(q)\} = S$. Let $*$ and $\circ$ be binary operations on $S \cup E$ satisfying*
$0 \circ e = e \circ 0 = 0 \circ 0 = 0$, $e \circ e = e$, $0 \circ q = 0$, $e \circ q = q$, $q * 0 = 0 * q = q$, $0 * 0 = 0$ *($q \in S$, $e \in E$) and let $^{-}$ and $^{=}$ be functions from E into E defined by*

$$\begin{aligned} &\overline{\overline{y}} = e \quad \textit{for} \quad y = 0, \quad \overline{y} = 0 \quad \textit{for} \quad y = 0, \\ &\overline{\overline{y}} = 0 \quad \textit{for} \quad y \neq 0, \quad \overline{y} = e \quad \textit{for} \quad y \neq 0. \end{aligned}$$

Then the general reproductive solution of $J(x) = 0$ is defined by the following formula

$$\begin{aligned} x = {} & \overline{\overline{J}}(q) \circ q * \overline{J}(q) \circ \overline{\overline{J}}(C_q(q)) \circ C_q(q) * \dots \\ & * \overline{J}(q) \circ \overline{J}(C_q(q)) \circ \dots \circ \overline{J}(C_q^{k-3}(q)) \circ \overline{\overline{J}}(C_q^{k-2}(q)) \circ C_q^{k-2}(q) * \\ & * \overline{J}(q) \circ \overline{J}(C_q(q)) \circ \dots \circ \overline{J}(C_q^{k-2}(q)) \circ C_q^{k-1}(q). \end{aligned}$$

Definition 3. Let $k_1, \dots, k_n$ be the binary digits of the number

$$k \in \{0, 1, 2, \dots, 2^n - 1\}$$

in the binary numeration, i.e.

$$(k_1 \dots k_n)_2 = (k)_{10} \in \{0, 1, 2, \dots, 2^n - 1\}.$$

If $T = (t_1, \dots, t_n) \in B^n$ then

$$T \oplus k \stackrel{\text{def}}{=} (t_1 + k_1, \dots, t_n + k_n).$$

Example 1. For $n = 4$ we have

$$T \oplus 3 = (t_1 + 0, t_2 + 0, t_3 + 1, t_4 + 1) = (t_1, t_2, t_3 + 1, t_4 + 1),$$

since $(3)_{10} = (0011)_2$.

Definition 4. Let $(k_1 \dots k_n)_2 = (k)_{10} \in \{0, 1, 2, \dots, 2^n - 1\}$ and $N = \{1, \dots, n\}$.

$$\begin{aligned} & k_Q \stackrel{\text{def}}{=} k_{q_1} \dots k_{q_s}, \quad \text{where} \quad Q = \{q_1, \dots, q_s\} \subset N \\ & D(k) \stackrel{\text{def}}{=} \{i \mid k_i = 1 \wedge i \in N\}. \end{aligned}$$

Note that $k_\Phi = 1$, because $\prod_{x \in \Phi} x = 1$.

PROPOSITION. *Let $f : B^n \to B$ be a Boolean function and $\sum_{S\subset N} a_S \prod_{i\in S} t_i$ be the canonical polinomial form of the function f, where $N = \{1, \ldots, n\}$.*
Then

$$f(T \oplus k) = \sum_{R\subset N} \left(\sum_{S\subset R} a_S \prod_{h\in S/R} k_h \right) \prod_{j\in R} t_j$$

where $(k_1 \ldots k_n)_2 = (k)_{10} \in \{0, 1, 2, \ldots, 2^n - 1\}$.

Proof.

$$\begin{aligned} f(T \oplus k) &= \sum_{S\subset N} a_S \prod_{i\in S} (t_i + k_i) = \\ &= \sum_{S\subset N} a_S \left(\sum_{R\subset S} \prod_{j\in R} t_j \prod_{h\in S/R} k_h \right) = \\ &= \sum_{R\subset N} \left(\sum_{S\subset R} a_S \prod_{h\in S/R} k_h \right) \prod_{j\in R} t_j. \quad \square \end{aligned}$$

LEMMA. *Let $f(T) = \sum_{S\subset N} a_S \prod_{i\in S} t_i$ be the canonical polinomial form of Boolean function $f : B^n \to B$. Then*

$$\begin{aligned} & f(T)f(T \oplus 1)f(T \oplus 2) \ldots f(T \oplus p) = \\ (2) \qquad & = \sum_{V\subset N} \left(\sum_{V\subset \cup_{i=0}^{p} S_i} a_{S_0} a_{S_1} \ldots a_{S_p} \sum_{p} 1 \right) \prod_{j\in V} t_j \end{aligned}$$

for $p \in \{0, 1, 2, \ldots, 2^n - 2\}$, where $\sum_p$ means the sum over all $(L_0, L_1, \ldots, L_p) \in N^{p\times 1}$ satisfying the conditions

(a) $L_j \subset S_j \cap D(j), \qquad j = 0, 1, \ldots, p$

(b) $\cup_{i=0}^{p} (S_i \backslash L_i) = V$.

Proof.

$$\begin{aligned} & f(T)f(T \oplus 1)f(T \oplus 2) \ldots f(T \oplus p) = \\ & = \left(\sum_{S\subset N} a_S \prod_{i\in S} t_i \right) \left(\sum_{S\subset N} a_S \prod_{i\in S} (t_1 + 1_i) \right) \ldots \left(\sum_{S\subset N} a_S \prod_{i\in S} (t_i + p_i) \right) \\ & = \sum_{S_0, S_1, \ldots, S_p \subset N} a_{S_0} \prod_{i\in S_0} t_i a_{S_1} \prod_{i\in S_1} (t_i + 1_i) \ldots a_{S_p} \prod_{i\in S_p} (t_i + p_i) \\ & = \sum_{S_0, S_1, \ldots, S_p \subset N} a_{S_0} a_{S_1} \ldots a_{S_p} \sum_{V\subset \cup_{i=0}^{p} S_i} \left(\sum_{pp} 0_{L_0} 1_{L_1} \ldots p_{L_p} \right) \prod_{j\in V} t_j \end{aligned}$$

($\sum_{pp}$ means the sum over all $(L_0, L_1, \ldots, L_p) \in N^{p\times 1}$ satisfying the conditions

(c) $L_j \subset S_j, \qquad j = 0, 1, \ldots, p$

(d) $\cup_{i=0}^{p}(S_i \backslash L_i) = V$)
$= \sum_{V\subset N} \sum_{V\subset \cup_{i=0}^{p} S_i} a_{S_0} \ldots a_{S_p} (\sum_{pp} 0_{L_0} 1_{L_1} \ldots p_{L_p}) \prod_{j\in V} t_j.$
$0_{L_0} 1_{L_1} \ldots p_{L_p} = 1$ if and only if
(e) $L_j \subset D(j), \qquad j = 0, 1, \ldots, p$

so we get (2), because the conditions (c) and (e) are equivalent to (a). □

THEOREM 4. *Let* $f(X) = \sum_{S\subset N} a_S \prod_{i\in S} x_i$ *be the canonical polynomial form of Boolean function* $f : B^n \to B$. *Let*

$$\sum_{S\subset N} a_S \prod_{i\in S} x_i = 0 \tag{3}$$

be the consistent equation. The formulas

$$x_i = t_i + \sum_{V\subset N} \left(\sum_{k=0}^{2^n-2} C(V,k)(k_i + (k \times 1)_i) \right) \prod_{j\in V} t_j \quad (i = 1, \ldots, n) \tag{4}$$

are the general reproductive solution of the equation (3) *where*

$$C(V,k) = \sum_{\cup_{q=0}^{k} Sq \supset V} a_{S_0} a_{S_1} \ldots a_{S_k} \sum_k 1 \tag{5}$$

and $\sum_k$ *is the sum over all* $(L_0, L_1, \ldots L_k) \in N^{k\times 1}$ *satisfing the conditions*
(i) $L_j \subset S_j \cup D(j) \qquad (j = 0, 1, \ldots, k)$
(ii) $\cup_{i=0}^{k}(S_i \backslash L_i) = V$.

Proof. In accordance with Theorem 1 and Corollary it is sufficient to prove the theorem in B_2. We form the cycle for all $T = (t_1, \ldots, t_n) \in \{0,1\}^n$ in the following way

$$T,\ T \oplus 1,\ T \oplus 2,\ \ldots\ ,\ T \oplus (2^n - 1).$$

It is obvious that

$$\{T, T\oplus 1, T\oplus 2, \ldots, T \oplus (2^n - 1)\} = \{0,1\}^n$$

for arbitrary $T \in \{0,1\}^n$.

Introducing

$$\overline{y} = y \quad \text{and} \quad \overline{\overline{y}} = y + 1$$

we get, by Theorem 2, the general reproductive solutions of the equation (3) in the form

$$\begin{aligned} X = {} & (f(T)+1)T + f(T)(f(T\oplus 1)+1)(T\oplus 1) + \\ & + f(T)f(T\oplus 1)(f(T\oplus 2)+1)(T\oplus 2) + \cdots + \\ & + f(T)f(T\oplus 1)\ldots f(T\oplus(2^n-3))(f(T\oplus(2^n-2))+1)(T\oplus(2^n-2)) \\ & + f(T)f(T\oplus 1)\ldots f(T\oplus(2^n-3))f(T\oplus(2^n-2))(T\oplus(2^n-1)) \end{aligned}$$

or in the scalar form

$$\begin{aligned}x_i=&(f(T)+1)t_i+f(T)(f(T\oplus 1)+1)(t_i+l_i)+\\&+f(T)f(T\oplus 1)(f(T\oplus 2)+1)(t_i+2_i)+\dots+\\&+f(T)f(T\oplus 1)\dots f(T\oplus(2^n-3))(f(T\oplus(2^n-2))+1)(t_i+(2^n-2)_i)+\\&+f(T)f(T\oplus 1)\dots f(T\oplus(2^n-2))f(T\oplus(2^n-2))(t_i+(2^n-1)_i)\\&(i=1,\dots,n)\end{aligned}$$

i.e.

$$\begin{aligned}x_i&=t_i(f(T)+1+f(T)(f(T\oplus 1)+1)+f(T)f(T\oplus 1)(f(T\oplus 2)+1)+\dots\\&+f(T)f(T\oplus 1)\dots f(T\oplus(2^n-3))(f(T\oplus(2^n-2))+1)+\\&+f(T)f(T\oplus 1)\dots f(T\oplus(2^n-3))f(T\oplus(2^n-3))f(T\oplus(2^n-2)))=\\&=f(T)(f(T\oplus 1)+1)1_i+f(T)f(T\oplus 1)(f(T\oplus 2)+1)2_i+\dots+\\&+f(T)f(T\oplus 1)\dots f(T\oplus(2^n-3))(f(T\oplus(2^n-2))+1)(2^n-2)_i+\\&+f(T)f(T\oplus 1)\dots f(T\oplus(2^n-3))f(T\oplus(2^n-2))(2^n-2)_i,\\&\qquad(i=1,\dots,n).\end{aligned}$$

Multiplying and using the equality $a+a=0$ we get

$$\begin{aligned}x_i&=t_i+f(T)1_i+f(T)f(T)f(T\oplus 1)(1_i+2_i)+\dots+\\&+f(T)f(T\oplus 1)\dots f(T\oplus(2^n-3))((2^n-3)_i+(2^n-2)_i)+\\&+f(T)f(T\oplus 1)\dots f(T\oplus(2^n-2))((2^n-2)_i+(2^n-1)_i),\\&\qquad(i=1,\dots,n).\end{aligned}$$

The last equalities can be written as

$$x_i=t_i+\sum_{k=0}^{2^n-2}\left(\prod_{m=0}^{k}f(T\oplus m)\right)(k_i+(k\times 1)_i),$$
$$(i=1,\dots,n).$$

Using Lemma we can write

$$\prod_{m=0}^{k}f(T\oplus m)=\sum_{V\subset N}C(V,k)\prod_{j\in V}t_j$$

where $C(V,k)$ is given by (5). Hence

$$x_i=t_i+\sum_{k=0}^{2^n-2}\left(\sum_{V\subset N}C(V,k)\prod_{j\in V}t_j\right)(k_i+(k\times 1)_i),$$

i.e.

$$x_i=t_i+\sum_{V\subset N}\left(\sum_{V\subset N}\left(\sum_{k=0}^{2^n-2}C(V,k)(k_i+(k\times 1)_i\right)\right)\prod_{j\in V}t_j.\quad\square$$

Example 2. Solve the equation $a_{12}x_1x_2 + a_1x_1 + a_2x_2 + a_0 = 0$.

Performing the necessery procedure on a digital computer we get

$$C(\Phi,0) = a_0, C(\Phi,1) = a_0 + a_0a_2, C(\Phi,2) = a_0 + a_0a_1 + a_0a_2 + a_0a_1a_2,$$
$$C(\{1\},0) = a_1, C(\{1\},1) = a_1 + a_1a_2 + a_0a_{12} + a_1a_{12},$$
$$C(\{1\},2) = a_0a_{12} + a_0a_1a_{12},$$
$$C(\{2\},0) = a_2, C(\{2\},1) = 0, C(\{2\},2) = a_0a_{12} + a_0a_2a_{12}$$
$$C(\{1,2\},0) = a_{12}, C(\{1,2\},1) = 0, C(\{1,2\},2) = a_0a_{12} + a_1a_2a_{12}.$$

Using the formulas (3) we have

$$\begin{aligned} x_i = t_i &+ (C(\Phi,0)(0_i + 1_i) + C(\Phi,1)(1_i + 2_i) + C(\Phi,2)(2_i + 3_i)) \\ &+ (C(\{1\},0)(0_i + 1_i) + C(\{1\},1)(1_i + 2_i) + C(\{1\},2)(2_i + 3_i))t_1 \\ &+ (C(\{2\},0)(0_i + 1_i) + C(\{2\},1)(1_i + 2_i) + C(\{2\},0)(2_i + 3_i))t_2 \\ &+ (C(\{1,2\},0)(0_i + 1_i) + C(\{1,2\},1)(1_i + 2_i) + C(\{1,2\},2)(2_i + 3_i))t_1t_2 \\ &\qquad (i = 1,2) \end{aligned}$$

i.e.

$$\begin{aligned} x_1 &= t_1 + C(\Phi,1) + C(\{1\},1)t_1 + C(\{2\},1)t_2 + C(\{1,2\},1)t_1t_2 = \\ &= t_1 + a_0 + a_0a_2 + (a_1 + a_1a_2 + a_1a_{12} + a_0a_{12})t_1 = \\ &= a_0 + a_0a_2 + (1 + a_1 + a_2 + a_1a_{12} + a_0a_{12})t_1 \\ x_2 &= t_2 + C(\Phi,0) + C(\Phi,1) + C(\Phi,2) + (C(\{1\},0) + C(\{1\},1) + C(\{1\},2))t_1 + \\ &+ (C(\{2\},0) + C(\{2\},1) + C(\{2\},2))t_2 + \\ &+ (C(\{1,2\},0) + C(\{1,2\},1) + C(\{1,2\},2))t_1t_2 = \\ &= t_2 + a_0 + a_0 + a_0a_2 + a_0a_1 + a_0a_2 + a_0a_1a_2 + \\ &+ (a_1 + a_1 + a_1a_2 + a_0a_{12} + a_1a_{12} + a_0a_{12} + a_0a_1a_{12})t_1 + \\ &+ (a_2 + a_0a_{12} + a_0a_2a_{12})t_2 + (a_{12} + a_0a_{12} + a_1a_2a_{12})t_1t_2 = \\ &= a_0 + a_0a_1 + a_0a_1a_2 + (a_1a_2 + a_1a_{12} + a_0a_1a_{12})t_1 + \\ &+ (1 + a_2 + a_0a_{12} + a_0a_2a_{12})t_2 + (a_{12} + a_0a_{12} + a_1a_2a_{12})t_1t_2. \end{aligned}$$

REFERENCES

[1] D. Banković, *The general reproductive solution of Boolean equation*, Publ. Inst. Math. (Beograd) **34** (**48**) (1984), 7–11.

[2] Ž. Mijajlović, *Some remarks on Boolean terms-model theoretic approach*, Publ. Inst. Math. (Beograd) **21** (**35**) (1977), 135–140.

[3] S. Prešić, *Une methode de resolution des equations dont toutes les solutions appartiennet a une ensemble fini donne*, C. R. Acad. Sci. Paris **272** (1971) 654–657.

[4] S. Rudeanu, *Boolean Functions and Equations*, North Holland, Amsterdam, London and Elsevier, New York, 1974.

Prirodno-matematički fakultet
34000 Kragujevac
Jugoslavija

(Received 10 02 1986)