PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 34 (48), 1983, pp. 7-11

THE GENERAL REPRODUCTIVE SOLUTION OF BOOLEAN EQUATION

Dragić Banković

Abstract. We give the formula of the general reproductive solution of Boolean equation using Prešić theorem related to the formula of the general reproductive solution of the equation of the finite set and Vaught theorem. We also give a very simple proof of the theorem which gives the consistency condition of Boolean equation.

Definition. 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 $F_1, \ldots, F_n, G$ are atomic

—Every Horn formula is built from elementary Horn formulas by use $\wedge$, $\forall, \exists$.

Theorem 1. (Vaught) *Let H be a Horn sentence in the language L_B of Boolena algebras. If $B_2 \models H$ then $B \models H$.*

Corollary 1. *Let $X = (x_1, \ldots, x_n) \in B^n$, $T = (t_1, \ldots, t_n) \in B^n$, $f : B^n \to B$ and $P = (p_1, \ldots, p_n)$, where $p_i : B^n \to B$ for $i = 1, \ldots, n$. If $X = P(T)$ is the general solution of Boolean equation $f(X) = 0$ in B_2, then $X = P(T)$ is the general solution of $f(X) = 0$ in B.*

Proof. The sentence "$X = P(T)$ is general solution of $f(X) = 0$" can be written in the form

$$(\forall X)(f(X) = 0 \Leftrightarrow (\exists T)(X = P(T)))$$

i.e. in the form

$$(\forall X)(\exists T)(f(X) = 0 \Rightarrow X = P(T)) \wedge (\forall T)(X = P(T) \Rightarrow f(X) = 0)).$$

Since this formula is Horn's, it holds in B if it holds in B_2.

Corollary 2. *If $X = P(T)$ is the general reproductive solution of Boolean equation $f(X) = 0$ in B_2, then $X = P(T)$ is the general reproductive solution of $f(X) = 0$ in B.*

AMS Subject Classification (1980): Primary 02.

Proof. The sentence "$X = P(T)$ is the general reproductive solution of $f(X) = 0$" can be written as Horn sentence

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

THEOREM 2. (Boole, Schöder) *Boolean equation $f(X) = 0$ is consistent if and only if $\Pi_A f(A) = 0$, where Π_A means the conjuction over all $A = (a_1, \dots, a_n) \in \{0,1\}^n$.*

Proof. Theorem 2 can be written in the form

$$(\exists X) f(X) = 0 \Leftrightarrow \Pi_A f(A) = 0$$

or, equivalently,

$$(\forall X)(f(X) = 0 \Rightarrow \Pi_A f(A) = 0) \wedge (\exists X)(\Pi_A f(A) = 0 \Rightarrow f(X) = 0).$$

This is a Horn sentence and it obviously holds in B_2. This means that it holds in B.

THEOREM 3. (Prešić) *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 $\cdot$ be binary operations on $S \cup E$ satisfying

$$\begin{aligned} &0 \cdot e = e \cdot 0 = 0 \cdot 0 = 0,\ e \cdot e = e,\ 0 \cdot q = 0,\ e \cdot q = q \\ &q + 0 = 0 + q = q, \qquad 0 + 0 = 0 \qquad\qquad (q \in S, e \in E) \end{aligned}$$

and let * and $^-$ be functions from E into E defined by

$$\begin{aligned} &y^* = 0 \text{ for } y = 0 \qquad \bar{y} = e \text{ for } y = 0 \\ &y^* = e \text{ for } y \neq 0 \qquad \bar{y} = 0 \text{ for } y \neq 0. \end{aligned}$$

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

$$\begin{aligned} x = {} &\bar{J}(q)q + J^*(q)J(C_q(q))C_q(Q) + \cdots \\ &+ J^*(q)J^*(C_q(q)) \dots J^*(C_q^{k-3}(q))J(C_q^{k-2}(q))C_q^{k-2}(q) + \\ &+ J^*(q)J^*(C^q(q)) \dots J^*(C_q^{k-2}(q))C_q^{k-1}. \end{aligned} \tag{1}$$

Definition 2. Let $T = (t_1, \dots, t_n) \in B^n$. Then

$$T \oplus i \stackrel{def}{=} (t_1^{b_1}, \dots, t_n^{b_n} \qquad (i = 1, \dots, 2^n - 1)$$

where $b_1, \dots, b_n$ are the binary digits of the number $i - 1$.

For example, $(t_1, t_2, t_3) \oplus 3 = (t_1^0, t_2^1, t_3^0) = (t_1', t_2, t_3')$ because $3 - 1$ i.e. 2 can be written as 010.

We also use the following notation: $m(1),\ m(2),\dots,m(n)$ are the binary digits of the number $m\in\{0,1,2,\dots,2^n-1\}$. For example, since we write number 5 as 0101 for $n=4$, then 5(3)=0.

Lemma. *Let $f: B^b\to B$. Then* $f(T\oplus i)=\cup_A f(A\oplus i)T^A$ $(i=1,\dots,2^n-1)$

Proof. Since $T\oplus i=(t_1^{b_1},\dots,t_n^{b_n})$, where $b_j=(i-1)(j)$, we have

$$\begin{aligned} f(T\oplus i)&=\cup_A f(a_1,\dots,a_n)(t_1^{b_1},\dots,t_n^{b_n})^{(a_1,\dots,a_n)}\\ &=\cup_A f(a_1,\dots,a_n)(t_1,\dots,t_n)^{(a_1^{b_1},\dots,a_n^{b_n})}\end{aligned}$$

Denoting $a_1^{b_1}=c_1,\dots,a_n^{b_n}=c_n$ we have $a_1=c_1^{b_1},\dots,a_n=c_n^{b_n}$ i.e.

$$\begin{aligned} f(T\oplus i)&=\cup_C f(c_1^{b_1},\dots,c_n^{b_n})(t_1,\dots,t_n)^{(c_1,\dots,c_n)}\\ &=\cup_C f(C\oplus i)T^C.\end{aligned}$$

Theorem 4. *The general reproductive solution of consistent Boolean equation $f(X)=0$ is defined by the following formulas:*

$$\begin{aligned} x_j=\cup_A(&a_jf'(A)\cup a_j^{0(j)}f(A)f'(A\oplus 1)\cup a_j^{1(j)}f(A)f(A\oplus 1)f'(A\oplus 2)\cup\dots\\ &\cup a^{(2^n-3)(j)}f(A)f(A\oplus 1)\dots f'(A\oplus(2^n-2))\\ &\cup a^{(2^n-2)(j)}f(A)f(A\oplus 1)\dots f(A\oplus(2^n-2)))T^A,\quad (j=1,\dots,n).\end{aligned}\tag{2}$$

Proof. By Corollary 2 it is sufficient to prove in B_2 that (2) is the general reproductive solution of $f(X)=0$. It is obvious that

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

for every $T\in\{0,1\}^n$. Using the formula (1) with $\bar z=z'$ and $z^*=z$ we get

$$\begin{aligned} X=&f'(T)T\cup f(T)f'(T\oplus 1)(T\oplus 1)\cup\dots\\ &\cup f(T)f(T\oplus 1)\dots f'(T\oplus(2^n-2))(T\oplus(2^n-2))\\ &\cup f(T)f(T\oplus 1)\dots f(T\oplus(2^n-2))(T\oplus(2^n-1)).\end{aligned}$$

Using Lemma we get

$$\begin{aligned} X=&\Big(\bigcup_A f'(A)T^A\Big)T\cup\Big(\bigcup_A f(A)T^A\Big)\Big(\bigcup_A f'(A+1)T^A\Big)(T\oplus 1)\cup\dots\\ &\cup\Big(\bigcup_A f(A)T^A\Big)\dots\Big(\bigcup_A f'(A\oplus(2^n-2))T^A\big(T\oplus(2^n-2)\big)\\ &\cup\Big(\bigcup_A f(A)T^A\Big)\dots\Big(\bigcup_A f(A\oplus(2^n-2))T^A\big(T\oplus(2^n-1)\big)\end{aligned}$$

i.e.

$$\begin{aligned} x_j=&\Big(\bigcup_A f'(A)T^A\Big)T_j\cup\Big(\bigcup_A f(A)f'\big((A\oplus 1)T^A\Big)(T\oplus 1)_j\cup\dots\\ &\cup\Big(\bigcup_A f(A)\dots f'(A\oplus(2^n-2))T^A\Big)\big(T\oplus(2^n-2)\big)_j\\ &\cup\Big(\bigcup_A f(A)\dots f(A\oplus(2^n-2))T^A\big(T\oplus(2^n-1)\big)_j,\quad (j=1,\dots,n)\end{aligned}$$

Since $T^A(T\oplus i)_j = t_1^{a_1}\dots t_n^{a_n} t_j^{(i-1)(j)} = a_j^{(i-1)(j)} T^A$ and

$T^A T_j = t_1^{a_1}\dots t_n^{a_n} t_j = a_j T^A$, then

$$\begin{aligned} x_j = &\bigcup_A a_j f'(A) T^A \cup \bigcup_A a_j^{0(j)} f(A) f'(A\oplus 1) T^A \cup \dots \\ &\cup \bigcup_A a_j^{(2n-3)(j)} f(A) f(A\oplus 1)\dots f'(A\oplus(2^n-2)) T^A \\ &\cup \bigcup_A a^{(2n-2)(j)} f(A) f(A\oplus 1)\dots f\big(A\oplus(2^n-2)\big) T^A, \quad (j=1,\dots,n) \end{aligned}$$

From this we get (2).

I, we define the scalar product of two vectors $P=(p_1,\dots,p_s)$ and $Q=(q_1,\dots,q_s)$ as $p\circ Q=(p_1q_1\cup\dots\cup p_nq_n)$, we can write (2) in the form

$$x_j = \bigcup_A \big(a_j, a_j^{0(j)}, a_j^{1(j)},\dots, a_j^{(2^n-2)(j)}\big)\circ F(A)$$

where $F(A) = (f'(A), f(A)f'(A\oplus 1),\dots, f(A)\dots f(A\oplus(2^n-2)))$.

Example. Solve the Boolean equation $axy\cup bx'y'\cup cx'y\cup dxy' = 0$.

The consistency condition is $abcd = 0$

$$\begin{aligned} F(1,1) =&(f'(1,1), f(1,1)f'(1^0,1^0), f(1,1)f(1^0,1^0)f'(1^0,1^1), \\ &f(1,1)f(1^0,1^0)f(1^0,1^1)) = (a', ab', abc', abc) \\ F(0,0) =&(f'(0,0), f(0,0)f'(0^0,0^0), f(0,0)f(0^0,0^0)f'(0^0,0^1), \\ &f(0,0)f(0^0,0^0)f(0^0,0^1)) = (b', ba', bad', bad) \\ F(0,1) =&(f'(0,1), f(0,1)f'(0^0,1^0), f(0,1)f(0^0,1^0)f'(0^0,1^1), \\ &f(0,1)f(0^0,1^0)f(0^0,1^1)) = (c', cd', cda', cda) \\ f(1,0) =&(f'(1,0), f(1,0)f'(1^0,0^0), f(1,0)f(1^0,0^0)f'(1^0,0^1), \\ &f(1,0)f(1^0,0^0)f(1^0,0^1)) = (d', dc', dcb', dcb) \end{aligned}$$

$$\begin{aligned} x =& (1,1^0,1^0,1^1)(a',ab',abc',abc)tu \cup (0,0^0,0^0,0^1)(b',ba',bad',bad)t'u' \\ &\cup (0,0^0,0^0,0^1)(c',cd',cda',cda)t'u \cup (1,1^0,1^0,1^1)(d',dc',dcb',dcb)tu' \\ &= (a'\cup abc)tu \cup (ba'\cup bad')t'u' \cup (cd'\cup cda')t'u \cup (d'\cup dcb)tu' = \\ &= (a'\cup bc)tu \cup b(a'\cup d')t'u' \cup c(d'\cup a')t'u \cup (d'\cup cb)tu' \\ y =& (1,1^0,1^1,1^0)(a',ab',abc',abc)tu \cup (0,0^0,0^1,0^0)(b',ba',bad',t'u' \\ &\cup (1,1^0,1^1,1^0)(c',cd',cda',cda)t'u \cup (0,0^0,0^1,0^0)(d',dc',cdcb',dcb)tu' \\ &= (a'\cup abc')tu \cup (ba'\cup bad)t'u' \cup (c'cda')t'u \cup (dc'\cup dcb)tu' = \\ &= (a'\cup bc')tu \cup b(a'\cup d)t'u' \cup (c'\cup da')t'u \cup d(c'\cup b)tu'. \end{aligned}$$

REFERENCES

[1] C. C. Chang, H. J. Keisler, *Model Theory*, North Holland, Amsterdam, 1973.

[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 apparatiennent a une ensemble fini donne*, C. R. Acad. Sci. Paris, **272** (1917) 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 13 12 1982)