Certain Boolean equations

D. Banković

Department of Mathematics, University of Kragujevac, P.O. Box 60, 34000 Kragujevac, Yugoslavia

Received 24 March 1989
Revised 2 February 1990

Abstract


In [1] are given two theorems related to the number of parameters of the solution of the equation $f(X_n) = 0$, where $f : B^n \rightarrow B$ is a simple Boolean function. In this paper we prove these theorems for arbitrary Boolean function $f : B^n \rightarrow B$ and we also give the general solution of the equation $f(X_n) = 0$.

Keywords. Boolean equation, Horn formula.

Let $X_n = (x_1, \ldots, x_n) \in B^n$ and $T_n = (t_1, \ldots, t_n)$, where $(B, \cup, \cdot, ' , 0, 1)$ is a Boolean algebra.

Definition 1. Let $f : B^n \rightarrow B$ be a Boolean function. The system $\Phi = (\phi_1, \ldots, \phi_n)$ of Boolean functions $\phi_1, \ldots, \phi_n : B^n \rightarrow B$ is a general solution of the consistent Boolean equation $f(X_n) = 0$ if and only if

$$(\forall T_n) f(\Phi(T_n)) = 0 \land (\forall X_n) (f(X_n) = 0 \Rightarrow (\exists T_n) X_n = \Phi(T_n)).$$

(1)

In this case we also say: the formulas $x_k = \phi_k(t_1, \ldots, t_n) \ (k = 1, \ldots, n)$ define a general solution of $f(X_n) = 0$.

Definition 2. Let $f : B^n \rightarrow B$ be a Boolean function. The system $\delta = (\delta_1, \ldots, \delta_n)$ of Boolean functions $\delta_1, \ldots, \delta_n : B^n \rightarrow B$ is a general reproductive solution of the consistent Boolean equation $f(X_n) = 0$ if and only if

$$(\forall T_n) f(\delta(T_n)) = 0 \land (\forall T_n) (f(T_n) = 0 = T_n = \delta(T_n)).$$

(2)

In this case we also say: the formulas $x_k = \delta_k(t_1, \ldots, t_n) \ (k = 1, \ldots, n)$ define a general reproductive solution of $f(X_n) = 0$. 

0166-218X/92/$05.00 \copyright \ 1992$ — Elsevier Science Publishers B.V. All rights reserved
Theorem 3 (Deschamps). Let \( f(X_n) = 0 \) be a consistent Boolean equation. The formulas \( X_n = \lambda(T_n) \), where \( \lambda = (\lambda_1, \ldots, \lambda_n) \) and \( \lambda_i : B^n \to B \) \( (i = 1, \ldots, n) \) are Boolean functions, define a general solution of \( f(X_n) = 0 \) if and only if

\[
(\forall X_n) \left( f(X_n) = \prod_{A_n} \bigcup_{i=1}^n (\lambda_i(A_n) + x_i) \right)
\]

where \( \prod_{A_n} \) means the product over all \( A_n = (a_1, \ldots, a_n) \in \{0, 1\}^n \) and the operation + is defined as \( a + b = a'b \cup ab' \).

Definition 4. The Horn formulas over the language \( L \) are defined as follows:
- the elementary Horn formulas are defined as atomic formulas of \( L \) and the formulas of the form \( F_1 \land \cdots \land F_k = F \), where \( F_1, \ldots, F_k, F \) are atomic;
- every Horn formula is built from elementary Horn formulas by the use of \( \land \), \( \lor \), \( \exists \).

Theorem 5 (Vaught). Let \( \mathcal{H} \) be a Horn sentence in the language \( L_H \) of Boolean algebras. If \( B \models \mathcal{H} \), then \( B \models \mathcal{H} \).

See, for instance, [5].

Definition 6. Let \( i \in \{0, 1, \ldots, p - 1\} \), where \( p = 2^n \). Then \( i(1), \ldots, i(n) \) are the binary digits of the number \( i \) in binary expansion and \( \overline{i} = (i(1), \ldots, i(n)) \).

Theorem 7. For every Boolean function \( f : B^n \to B \) and every \( m < n \) the following equivalence holds:
There exist the functions \( h_1, \ldots, h_m \) such that the formulas
\[
\begin{align*}
x_1 &= h_1(t_1, \ldots, t_m) \\
&\vdots \\
x_n &= h_n(t_1, \ldots, t_m)
\end{align*}
\]
(3)
define a general solution of the equation \( f(X_n) = 0 \) if and only if the following condition holds:

\[
\prod_{A_n} f(A_n) = 0 \land \bigcup_{S \subseteq \{0, 1\}^n} \prod_{A_n \in S} f(A_n) = 1 \quad (\text{card } S = 2^m).
\]

(4)

Proof. Let us write (3) in the form \( X_n = H(T_n) \), where \( H = (h_1, \ldots, h_n) \). Let

\[
f(X_n) = \bigcup_{A_n} y_{A_n} X_n^{A_n} \quad \text{and} \quad h_k(T_n) = \bigcup_{A_n} h_k(T_n)^{A_n} \quad (k = 1, \ldots, n).
\]

(5)

We introduce the following notation:

\[
Y = (y_0^\overline{0}, y_1^\overline{1}, \ldots, y_{p-1}^\overline{p-1})
\]
and
\[ H_{n \times p} = \begin{bmatrix} h_{1,0} & h_{1,1} \cdots h_{1,p-1} \\ \vdots \\ h_{n,0} & h_{n,1} \cdots h_{n,p-1} \end{bmatrix} \]

where we write \( h_{k,i} \) instead of \( h_{k,i} \).

The condition (4) can be written as
\[ \prod_{A_n} f(A_n) \cup \bigcup_{S \subseteq \{0,1\}^n, A_n \in S} f'(A_n) = 0. \]

Denote the latter equality by \( U_m(Y) = 0 \).

Theorem 7 can be written in the following way:
\[ (\forall Y)(\forall m < n)((\exists h_1, \ldots, h_n)((\forall T_n) f(H(T_n)) = 0 \land (\forall X_n)(\exists T_n)(f(X_n) = 0 \Rightarrow X_n = H(T_n))) \Rightarrow U_m). \]

In accordance with (5) we can write the latter formula as
\[ (\forall Y)(\forall m < n)((\exists H_{n \times p}((\forall T_n) f(H(T_n)) = 0 \land (\forall X_n)(\exists T_n)(f(X_n) = 0 \Rightarrow X_n = H(T_n))) \Rightarrow U_m). \]

Bearing in mind Theorem 3 we write the latter formula as
\[ (\forall Y)(\forall m < n) \left( (\exists H_{n \times p})(\forall X_n) \left( f(X_n) = \prod_{A_n} (h_{k,A_n} + x_k) \Rightarrow U_m \right) \right), \]

i.e.,
\[ (\forall Y) \bigwedge_{m=0}^{n-1} \left( (\exists H_{n \times p})(\forall X_n) \left( U_m(Y) = 0 \Rightarrow \bigcup_{A_n} y_{A_n}X_{A_n} = \prod_{A_n} (h_{k,A_n} + x_k) \land (\forall H_{n \times p})(\exists X_n) \left( \bigcup_{A_n} y_{A_n}X_{A_n} = \prod_{A_n} (h_{k,A_n} + x_k) \Rightarrow U_m(Y) = 0 \right) \right) \right). \]

Since the latter formula is a Horn sentence, it is sufficient to prove Theorem 7 in \( B_2 \) because of Theorem 5. The proof of Theorem 7 in \( B_2 \) is given in [1].

**Corollary 8.** For every Boolean function \( f : B^n \rightarrow B \) it holds:

The equation \( f(X_n) = 0 \) has a unique solution if and only if
\[ \prod_{A_n} f(A_n) = 0 \land \bigcup_{A_n \subseteq c \subseteq \{0,1\}^n} f(C_n) = 1. \]  \( \quad (6) \)

**Proof.** If we put \( m = 0 \) the conjunction (4) in Theorem 5 becomes (6) and \( h_k \) \( (k = i, \ldots, n) \) are constants. \( \square \)

**Problem.** Let the condition
\[ \prod_{A_n} f(A_n) = 0 \land \bigcup_{S \subseteq \{0,1\}^n, A_n \in S} f(A_n) = 1, \]

...
where $\text{card } S = 2^n$, be satisfied. Determine Boolean functions $h_1, \ldots, h_n : B^m \rightarrow B$ such that the formulas

$$x_i = h_i(t_1, \ldots, t_m)$$

$$\vdots$$

$$x_n = h_n(t_1, \ldots, t_m)$$

define a general solution of the equation $f(X_n) = 0$ (by Theorem 5 there exist such functions $h_1, \ldots, h_n$).

**Theorem 9.** For every Boolean function $f : B^n \rightarrow B$ it holds:

There exist the functions $g_{i_1}, \ldots, g_{i_q}$ such that the formulas

$$x_{i_r} = t_{i_r} \quad (r = 1, \ldots, m)$$

$$x_{i_s} = g_{i_s}(t_{i_{j_1}}, \ldots, t_{i_{j_m}}, t_{i_{m+1}}, \ldots, t_i) \quad (s = 1, \ldots, q)$$

$$\begin{array}{c}
(m, q \in \{1, \ldots, n-1\}, m + q = n
\end{array}$$

define a general solution of the Boolean equation $f(X_n) = 0$ if and only if

$$\bigcup_{(a_1, \ldots, a_n) \in \{0, 1\}^n} \prod_{a_{i_1}, \ldots, a_{i_q}} f(a_{i_1}, \ldots, a_n) = 0$$

(8)

where $\{i_1, \ldots, i_m, i_{m+1}, \ldots, i_q\} = \{1, \ldots, n\}$.

**Proof.** Let us write (7) in the form $X = G(T_n)$, where $G = (g_1, \ldots, g_n)$ and $g_{i_r} = t_{i_r}$, $(r = 1, \ldots, m)$.

Let equality (8) be denoted by $V(Y) = 0$. Bearing in mind Theorem 3 we write Theorem 9 as

$$\forall Y \left( V(Y) = 0 \iff \exists G_{n\times p}(\forall X_n) \left( f(X_n) = \prod_{A_k} \bigcup_A (g_k(A) + x_k) \right) \right),$$

i.e.,

$$\forall Y (\exists G_{n\times p})(\forall X_n) \left( V(Y) = 0 \Rightarrow \bigcup_{A_k} y_{A_k} X^{A_k} = \prod_{A_k} \bigcup_{A_k} (g_k(A) + x_k) \quad \land \right.$$

$$\left. (\forall Y)(\forall G_{n\times p})(\exists X_n) \left( \bigcup_{A_k} y_{A_k} X^{A_k} = \prod_{A_k} \bigcup_{A_k} (g_k(A) + x_k) \right) \right)$$

$$= V(Y) = 0).$$

Since the latter formula is a Horn sentence it is sufficient to prove Theorem 9 in $B_2$ because of Theorem 5. The proof of Theorem 9 in $B_2$ is given in [1]. □

Let $f : R^n \rightarrow R$ be a Boolean function. We introduce the following notation:

$$f((t_{i_1}, \ldots, t_{i_m}), (t_{i_{m+1}}, \ldots, t_{i_q})) = f(t_{i_1}, \ldots, t_{i_q})$$

(9)

where $\{i_1, \ldots, i_m, i_{m+1}, \ldots, i_q\} = \{1, \ldots, n\}$ and $m + q = n$. 
Theorem 10. For every Boolean function $f : B^n \to B$ it holds:

If

\[ \bigcup_{(a_1, \ldots, a_n) \in \{0,1\}^n} \prod_{(a_1, \ldots, a_n) \in \{0,1\}^n} f(a_1, \ldots, a_n) = 0, \]  

then the formulas

\[ x_i = \left( \prod_{(a_1, \ldots, a_n) \in \{0,1\}^n} f((t_{j_1}, \ldots, t_{j_m}), (x_{i_1}, \ldots, x_{i_s}, t_{j_1}, a_{i_1}, \ldots, a_{i_s})) \right)^{t_{j_i}}, \]

\[ x_i = \left( \prod_{(a_1, \ldots, a_n) \in \{0,1\}^n} f((t_{j_1}, \ldots, t_{j_m}), (x_{i_1}, \ldots, x_{i_s}, t_{j_1}, a_{i_1}, \ldots, a_{i_s})) \right)^{t_{j_i}} \]  

or, equivalently,

\[ x_i = \left( \prod_{(a_1, \ldots, a_n) \in \{0,1\}^n} f((t_{j_1}, \ldots, t_{j_m}), (x_{i_1}, \ldots, x_{i_s}, 1, a_{i_1}, \ldots, a_{i_s})) \right)^{t_{j_i}}, \]

\[ x_i = \left( \prod_{(a_1, \ldots, a_n) \in \{0,1\}^n} f((t_{j_1}, \ldots, t_{j_m}), (x_{i_1}, \ldots, x_{i_s}, 0, a_{i_1}, \ldots, a_{i_s})) \right)^{t_{j_i}}. \]  

define a general reproductive solution of the Boolean equation $f(X_n) = 0$.

Proof. Let us write formulas (11) and (12) as $x_k = g_k(t_1, \ldots, t_n)$ ($k = 1, \ldots, n$). Bearing in mind Theorem 3 we can write Theorem 10 as

\[ (\forall Y) \left( (V(Y) = 0 \Rightarrow \bigcup_{A_1, \ldots, A_n} X^{A_1} = \prod_{A_1, \ldots, A_n} (g_k(A_n) + x_k) \right) = \bigcup_{A_1, \ldots, A_n} X^{A_1} = \prod_{A_1, \ldots, A_n} (g_k(A_n) + x_k). \]

The latter Horn formula has no free variables because $g_k(A_n) \in \{0,1\}$ or $g_k(A_n)$ depends only on $f$, i.e., $Y$. It means the last formula is a Horn sentence. Thus it is sufficient to prove Theorem 10 in $B_2$ because of Theorem 5.

Let $(t_1, \ldots, t_n) \in \{0,1\}^n$. If we put

\[ t_{j_r} = t_j \quad (r = 1, \ldots, m) \]

formulas (10) give

\[ x_j = t_{j_r} \quad (r = 1, \ldots, m). \]

For $s = 1$ formula (12) gives

\[ x_i = \left( \prod_{(a_1, \ldots, a_n) \in \{0,1\}^n} f((t_{j_1}^s, \ldots, t_{j_m}^s), (t_i, a_{i_1}, \ldots, a_{i_s})) \right)^{t_{j_i}}. \]
\[ t^*_n = \begin{cases} 
    t_{i_n} & \text{if } \prod_{(a_{i_1}, \ldots, a_{i_q}) \in \{0, 1\}^{q-1}} f((t^*_j, \ldots, t^*_m), (t_{i_1}, a_{i_2}, \ldots, a_{i_q})) = 0, \\
    t'_{i_n} & \text{if } \prod_{(a_{i_1}, \ldots, a_{i_q}) \in \{0, 1\}^{q-1}} f((t^*_j, \ldots, t^*_m), (t_{i_1}, a_{i_2}, \ldots, a_{i_q})) = 1. 
\end{cases} \tag{13} \]

Note that
\[ \prod_{(a_{i_1}, \ldots, a_{i_q}) \in \{0, 1\}^{q-1}} f((t^*_j, \ldots, t^*_m), (t_{i_1}, a_{i_2}, \ldots, a_{i_q})) = 0 \tag{14} \]
because of (13) and (10).

Similarly we get from (12)
\[ x_{i_q} = t^*_q = \begin{cases} 
    t_{i_q} & \text{if } \prod_{(a_{i_1}, \ldots, a_{i_q}) \in \{0, 1\}^{q-2}} f((t^*_j, \ldots, t^*_m), (t_{i_1}, t_{i_2}, a_{i_3}, \ldots, a_{i_q})) = 0, \\
    t'_{i_q} & \text{if } \prod_{(a_{i_1}, \ldots, a_{i_q}) \in \{0, 1\}^{q-2}} f((t^*_j, \ldots, t^*_m), (t_{i_1}, t_{i_2}, a_{i_3}, \ldots, a_{i_q})) = 1, \tag{15} \end{cases} \]
and
\[ \prod_{(a_{i_1}, \ldots, a_{i_q}) \in \{0, 1\}^{q-1}} f((t^*_j, \ldots, t^*_m), (t_{i_1}, t_{i_2}, a_{i_3}, \ldots, a_{i_q})) = 0 \]
because of (14) and (15).

Continuing in this way, we finally get
\[ x_{i_q} = t^*_q = \begin{cases} 
    t_{i_q} & \text{if } f((t^*_j, \ldots, t^*_m), (t_{i_1}, \ldots, t_{i_q-1}, t_{i_q})) = 0, \\
    t'_{i_q} & \text{if } f((t^*_j, \ldots, t^*_m), (t_{i_1}, \ldots, t_{i_q-1}, t_{i_q})) = 1, \tag{16} \end{cases} \]
and
\[ f((t^*_j, \ldots, t^*_m), (t_{i_1}, \ldots, t_{i_q})) = 0 \tag{17} \]
because of (16) and \( \prod_{a_{i_q} \in \{0, 1\}} f((t^*_j, \ldots, t^*_m), (t_{i_1}, \ldots, t_{i_q}, a_{i_q})) = 0 \). Equality (17) means that \( x_1, \ldots, x_n \) given by formulas (11) and (12) satisfy the equation \( f(X_n) = 0 \).

Reproductivity will be proved by induction on \( s \). Let \( f(z_1, \ldots, z_n) = 0 \) and \( t_k = z_k \) \((k = 1, \ldots, n)\). Formulas (11) give \( x_{j_r} = z_{j_r} \) \((r = 1, \ldots, m)\). For \( s = 1 \) formula (12) gives
\[ x_{i_q} = \left( \prod_{(a_{i_1}, \ldots, a_{i_q}) \in \{0, 1\}^{q-1}} f((z_j, \ldots, z_m), (a_{i_1}, a_{i_2}, \ldots, a_{i_q})) \right)^{z_i} \]
and
\[ \prod_{(a_{i_1}, \ldots, a_{i_q}) \in \{0, 1\}^{q-1}} f((z_j, \ldots, z_m), (a_{i_1}, a_{i_2}, \ldots, a_{i_q})) = 0 \]
because of \( f(z_1, \ldots, z_n) = 0 \).

Supposing \( x_{i_q} = z_{i_q}, \ldots, x_{i_1} = z_{i_1} \), we get from (12)
\[ x_{i_{q+1}} = \left( \prod_{(a_{i_1}, \ldots, a_{i_q}) \in \{0, 1\}^{q-1}} f((z_j, \ldots, z_m), (z_{i_1}, \ldots, z_{i_q}, a_{i_2}, \ldots, a_{i_q})) \right)^{z_{i_{q+1}}} \]
Certain Boolean equations

because of $f(z_1, \ldots, z_n) = 0$. Reproductivity is proved.

The equalities (12) and (12') are equivalent because of the identity $g(t) \cup g(t) t' = g(1) t \cup g(0) t'$, where $g : B \to B$ is an arbitrary Boolean function. □

Remark 11. In accordance with Theorem 10 it obviously holds:

If $m = 0$, then condition (10) is

$$\prod_{(a_1, \ldots, a_n) \in \{0, 1\}^n} f(a_1, \ldots, a_n) = 0. \quad (18)$$

In this case the formulas

$$X_i = \left(\prod_{(a_1, \ldots, a_n) \in \{0, 1\}^n} f(x_1, \ldots, x_n, 1, a_i, \ldots, a_n)\right)' t_i$$

$$\cup \left(\prod_{(a_1, \ldots, a_n) \in \{0, 1\}^n} f(x_1, \ldots, x_n, 0, a_i, \ldots, a_n)\right)' t_i'$$

$(s = 1, \ldots, n)$

(19)

define a general reproductive solution of $f(X_n) = 0$.

It is known that condition (18) and formulas (19) can be obtained by the method of successive eliminations (see [7]). One can prove that the formulas (12') can be obtained by the method of successive eliminations provided that condition (10) is satisfied.

References


