

HONORS ASSIGNMENT I
MATH 571 FALL 2019
DUE OCT 10TH

Let P_n be the set of all n -ary Boolean functions and let $P = \bigcup_{n \in \mathbb{N}} P_n$.

Definition 1. A set $Q \subseteq P$ is complete if every function in P can be obtained from the projection functions I_k^n ($n, k \in \mathbb{N}$) and the functions in Q using composition.

Recall, that $\oplus$ is the logical connective that realizes the binary Boolean function that is true when exactly one of its arguments is true.

Problem 1. Prove that the set $\{B_T^0, B_\oplus^2, B_\wedge^2\}$ is complete and every Boolean function in P_n can be realized by a unique formula of the form:

$$\begin{aligned} & a_0 \oplus a_1 \wedge A_1 \oplus a_2 \wedge A_2 \oplus \cdots \oplus a_n \wedge A_n \oplus \\ & a_{12} \wedge A_1 \wedge A_2 \oplus a_{13} \wedge A_1 \wedge A_3 \oplus \cdots \oplus a_{n-1,n} A_{n-1} \wedge A_n \oplus \\ & \cdots \\ & a_{123\dots n} \wedge A_1 \wedge A_2 \wedge \cdots \wedge A_n. \end{aligned}$$

Here each $a_{i_1 \dots i_k}$ is a Boolean constant (either T or F). If its value is T we include the term that follows it and if its value is F we omit it. The formula above is called a *Zhegalkin polynomial*. For example $A_1 \rightarrow A_2 \models T \oplus A_1 \oplus A_1 \wedge A_2$. Here $a_0 = a_1 = a_{12} = T$ and $a_2 = F$. (It is convenient to think of T as 1, F as 0, $\wedge$ as multiplication and $\oplus$ as addition modulo 2.) *Hint!* To prove the second part, use a size argument: count the number of possible functions of this sort and prove that different Zhegalkin polynomials realize different functions.

Find the Zhegalkin polynomial for each of the 16 Boolean functions of arity 2.

Definition 2. We define the following five classes of Boolean functions:

- T_1 is the set of all Boolean functions that preserve truth, i.e. if $B \in P_n \cap T_1$ then $B(T, T, \dots, T) = T$.
- T_0 is the set of all Boolean functions that preserve falsity, i.e. if $B \in P_n \cap T_0$ then $B(F, F, \dots, F) = F$.
- S is the set of self-dual functions. A Boolean function $B \in P_n$ is self-dual if for every $(X_1 \dots X_n) \in \{T, F\}^n$ we have that $B(X_1, \dots, X_n) = \neg B(\neg X_1, \dots, \neg X_n)$. Here we use $\neg$ as a unary Boolean function.
- L is the set of all Boolean functions with linear Zhegalkin polynomial, i.e. all Boolean constants except for possibly $a_0 \dots a_n$ in the Zhegalkin polynomial have value F. For example $A_1 \leftrightarrow A_2$ realizes a function in L , but $A_1 \vee A_2$ does not. Why?
- We order the Boolean vectors as follows: $F \leq T$ and $(X_1, X_2, \dots, X_n) \leq (Y_1, Y_2, \dots, Y_n)$ if and only if for every i $X_i \leq Y_i$. M is the set of monotone functions with respect to this ordering, i.e. functions $B \in P_n$ satisfying $B(X_1, \dots, X_n) \leq B(Y_1, \dots, Y_n)$ whenever $(X_1, X_2, \dots, X_n) \leq (Y_1, Y_2, \dots, Y_n)$.

Problem 2. Prove that each of the five classes is closed under composition.

Problem 3. Determine the size of each of the following sets:

- | | |
|----------------------|--------------------------------------|
| (1) $T_0 \cap P_n$; | (4) $L \cap S \cap P_n$. |
| (2) $S \cap P_n$; | (5) $T_0 \cap T_1 \cap L \cap P_n$. |
| (3) $L \cap P_n$; | |

Problem 4. Prove that if $B \in P_n$ is a Boolean function and $B \notin M$ then there are vectors $(X_1, \dots, X_n)$ and $(Y_1, \dots, Y_n)$ that differ in precisely one bit and witness that B is not monotone, i.e. $(X_1, \dots, X_n) \leq (Y_1, \dots, Y_n)$ but $B(X_1, \dots, X_n) \not\leq B(Y_1, \dots, Y_n)$.

Theorem 1 (Post). *A set $Q \subseteq P$ is complete if and only if Q is not a subset of any of the classes T_0, T_1, S, L or M .*

Proof. To show that complete sets are not subsets of either of the five classes listed above, for each class give an example of a Boolean function that is not in it. Explain why this is sufficient! Use Problem 2.

Suppose that Q satisfies the statement of the Theorem. Fix functions $B_0 \notin T_0$, $B_1 \notin T_1$, $B_s \notin S$, $B_l \notin L$ and $B_m \notin M$, all members of Q . The proof breaks down into steps:

Step 1: Our goal is to obtain the constant functions T and F . Consider the composition of B_0 with I_1^1 , i.e. the function $G_0(X_1) = B_0(X_1, X_1, \dots, X_1)$. Similarly consider $G_1(X_1) = B_1(X_1, \dots, X_1)$. There are several possibilities for these functions. There is one case that gives us only the function G_- realized by negation. In all other cases we get both constant function. Why?

If we only have negation then combine it with the function B_s to get a constant function: Let $(Y_1, \dots, Y_n)$ be the vector that witnesses that $B_s \notin S$. Consider the function $G(X_1) = G_s(Z_1, \dots, Z_n)$, where $Z_i = X_1$ if $Y_i = T$ and $Z_i = G_-(X_1)$ if $Z_i = F$. Why does this work?

Step 2: We have the two constant function. Our next goal is to get negation. To do this use the function B_m and Problem 4.

Step 3: We have the two constants and negations. Using the function B_l , the two constants and negation we can get conjunction. Consider

$$B_l(X_1, \dots, X_k) = a_0 \oplus a_1 \wedge A_1 \oplus a_2 \wedge A_2 \oplus \dots \oplus a_k \wedge A_k \oplus A_{i_1} \wedge A_{i_2} \dots A_{i_m} \oplus \dots$$

where $A_{i_1} \wedge A_{i_2} \dots A_{i_m}$ is the first nonlinear term with constant T in front. Consider the function $H(X_1, X_2) = B_l(Z_1, \dots, Z_k)$, where $Z_i = X_1$ if $i = i_1$, $Z_i = X_2$ if $i = i_2$, $Z_i = T$ if $i = i_3, \dots, i_m$, and $Z_i = F$ in all other cases. It follows that $H(X_1, X_2) = c_0 \oplus c_1 \wedge X_1 \oplus c_2 \wedge X_2 \oplus X_1 \wedge X_2$. Consider all cases for the constants c_0, c_1 , and c_2 and prove that in each case we can get $B_\wedge^2$ by using compositions of H, G_- and the constants. This completes the proof. Why? $\square$

Problem 5. Fill in the gaps in the proof of Post's theorem.