International Students' Olympiad in Cryptography - 2018Second roundNSUCRYPTOOctober 15-22



A polynomial $f(X_1, \ldots, X_n) \in \mathbb{F}_2[X_1, \ldots, X_n]$ is called *reduced* if the degree of each X_i in f is at most 1. For $0 \leq r \leq n$, the rth order Reed — Muller code of length 2^n , denoted by R(r, n), is the \mathbb{F}_2 -space of all reduced polynomials in X_1, \ldots, X_n of total degree $\leq r$. We also define $R(-1, n) = \{0\}$.

The general linear group $\operatorname{GL}(n, \mathbb{F}_2)$ acts on R(r, n) naturally: Given $A \in \operatorname{GL}(n, \mathbb{F}_2)$ and $f(X_1, \ldots, X_n) \in R(r, n)$, Af is defined to be the reduced polynomial obtained from $f((X_1, \ldots, X_n)A)$ by replacing each power X_i^k $(k \ge 2)$ with X_i . Consequently, $\operatorname{GL}(n, \mathbb{F}_2)$ acts on the quotient space R(r, n)/R(r-1, n).

Let $A \in \operatorname{GL}(n, \mathbb{F}_2)$ be such that its characteristic polynomial is a primitive irreducible polynomial over \mathbb{F}_2 . Prove that the only element in R(r, n)/R(r-1, n), where 0 < r < n, fixed by the action of A is 0.



