



Problem 6. «Bob's symbol»

Bob learned the Goldwasser–Micali cryptosystem at the university. Now, he is thinking about functions over finite fields that are similar to Jacobi symbol.

He chose a function $B_n : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$ (Bob's symbol) defined as follows for any $a \in \mathbb{F}_{2^n}$:

$$B_n(a) = \begin{cases} 1, & \text{if } a = x^2 + x \text{ for some } x \in \mathbb{F}_{2^n}, \\ 0, & \text{otherwise.} \end{cases}$$

Bob knows that finite fields may have some subfields. Indeed, it is well known that \mathbb{F}_{2^k} is a subfield of \mathbb{F}_{2^n} if and only if $k|n$. Bob wants to exclude the elements of subfields. In other words, he considers the restriction of B_n to the set

$$\widehat{\mathbb{F}}_{2^n} = \mathbb{F}_{2^n} \setminus \bigcup_{k|n, k \neq n} \mathbb{F}_{2^k}.$$

Here, by $\mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$ we mean the removal from \mathbb{F}_{2^n} the elements forming the field of order 2^k .

Finally, Bob is interested in the sets

$$B_n^0 = \{y \in \widehat{\mathbb{F}}_{2^n} : B_n(y) = 0\} \quad \text{and} \quad B_n^1 = \{y \in \widehat{\mathbb{F}}_{2^n} : B_n(y) = 1\}.$$

Q1 Help Bob to find $|B_n^0|/|B_n^1|$ if n is odd.

Q2 Help Bob to find $|B_n^0|$ and $|B_n^1|$ for an arbitrary n .