Problem 1. «The image set»

Special Prize from the Program Committee!

Let $\mathbb{F}_2$ be the finite field with two elements and n be any positive integer. Let $g(X)$ be an irreducible polynomial of degree n over $\mathbb{F}_2$. It is widely known that the set of equivalence classes of polynomials over $\mathbb{F}_2$ modulo $g(X)$ is a finite field of order 2^n; we denote it by $\mathbb{F}_{2^n}$.

Characterize in a non-straightforward way the image set (depending on n) of the function F over $\mathbb{F}_2^n$ defined as follows:

$$F(x) = x^3 + x.$$

That is, characterize in a way which brings additional information, for instance on its algebraic structure.

An example. For $n = 3$ we can take $g(X) = X^3 + X + 1$, then each element of the field $\mathbb{F}_{2^3}$ can be written as a polynomial of degree at most 2: $a_0 + a_1X + a_2X^2$, with $a_0, a_1, a_2 \in \mathbb{F}_2$. We can calculate the table of multiplication in $\mathbb{F}_{2^3}$ modulo $g(X)$, while the table of addition just corresponds to adding polynomials over $\mathbb{F}_2$. For example,

$$(1 + X + X^2) + (X + X^2) = 1,$$

$$(X + X^2)(1 + X^2) = X + X^2 + X^3 + X^4 = 1 + X \pmod{g(X)}.$$

Now we can calculate all the elements of the image set of $F(x)$. Indeed,

$$\{F(x) \mid x \in \mathbb{F}_{2^3}\} = \{0,\ 1,\ 1 + X,\ 1 + X^2,\ 1 + X + X^2\}.$$

Then we note that it is the union of $\{0\}$ and of the affine plane $1 + \{0, X, X^2, X + X^2\}$. In our case it is a desirable algebraic structure of this set.

You need to study this problem for an arbitrary n (or some partial cases).

Remark. Functions over the finite field of order 2^n are of great interest for using in cryptographic applications, for example, as S-boxes. For instance, AES S-box is based on the inverse function over $\mathbb{F}_{2^8}$. But in fact, there are many open problems in fields of finding new constructions and descriptions of cryptographically significant functions!