MPRI 2.13.2 - Error-correcting codes and applications to cryptography

Exercises on finite fields
20/09/2023

Exercise 1. *Construction of* $\mathbf{F}_{16}$

1. Let α be a root of $X^4 + X + 1$. Compute all successive powers of α. Is α a primitive element in $\mathbf{F}_{16}$?
2. Compute $\alpha^7 \times \alpha^{11}$ and $\alpha^7 + \alpha^{11}$ in $\mathbf{F}_{16}$.
3. Determine all non-trivial multiplicative subgroups of $\mathbf{F}_{16}^*$.
4. Determine the order of each element in $\mathbf{F}_{16}$.
5. Compute the minimal polynomials of α, of α^5, of α^3 and of α^7.
6. Let β be a root of $X^4+X^3+X^2+X+1$. Is the set $\{1, \beta, \beta^2, \beta^3\}$ a basis of $\mathbf{F}_{16}$ over $\mathbf{F}_2$?

Exercise 2. *Power mappings over* $\mathbf{F}_{2^m}$

1. Let $s > 0$ be an integer. When does $F_s : x \mapsto x^s$ permute the field $\mathbf{F}_{2^m}$?
2. When F_s is a permutation, determine its inverse.
3. When does $F_3 : x \mapsto x^3$ permute $\mathbf{F}_{2^m}$?
4. Determine the inverse of $x \mapsto x^{2^{m-1}-1}$ on $\mathbf{F}_{2^m}$.

Exercise 3. *Trace function*
Let q be a power of a prime number, and let $m > 0$ be an integer. The Trace mapping from $\mathbf{F}_{q^m}$ into $\mathbf{F}_q$ is defined by

$$\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x) = \sum_{i=0}^{m-1} x^{q^i}, \; x \in \mathbf{F}_{q^m} \; .$$

1. Prove that $\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x^q) = \mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x)$ for all $x \in \mathbf{F}_{q^m}$.
2. Prove that $\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}$ takes its values in $\mathbf{F}_q$.
3. Prove that $\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}$ is a linear function when $\mathbf{F}_{q^m}$ is seen as a vector space over $\mathbf{F}_q$.
4. Compute $\mathrm{Tr}_{\mathbf{F}_{q^m}/\mathbf{F}_q}(x)$ when $x \in \mathbf{F}_q$. Deduce the value of $\mathrm{Tr}_{\mathbf{F}_{2^m}/\mathbf{F}_2}(1)$.

Exercise 4. *Equations of degree* 2 *in* $\mathbf{F}_{2^m}$

1. Determine the number of solutions in $\mathbf{F}_{2^m}$ of
$$aX^2 + bX + c = 0 \; ,$$
where a, b and c are three elements in $\mathbf{F}_{2^m}$, $a \neq 0$.
[*Hint :* When $b \neq 0$, the problem boils down to solving $X^2 + X + d$.]
2. Let $\alpha \in \mathbf{F}_{2^m}$ and
$$\theta = c\alpha^2 + (c + c^2)\alpha^4 + \ldots + (c + c^2 + c^4 + \ldots + c^{2^{m-2}})\alpha^{2^{m-1}} \; .$$
Prove that, if $\mathrm{Tr}_{\mathbf{F}_{2^m}/\mathbf{F}_2}(\alpha) = 1$, then θ is a root of $X^2 + X + c$.
Deduce a simple expression of the solutions of $X^2 + X + c$ in $\mathbf{F}_{2^m}$, when m is odd.

Exercise 5. *Polynomials with coefficients in a subfield*
Let K be finite field with characteristic p and P be a polynomial in $K[X]$. Prove that $P(X^p) = (P(X))^p$ if and only if the coefficients of P lie in $\mathbf{F}_p$.