Ho Chi Minh University of Science HCMUS

Update: 16/09/2013

Finite fields: some applications

Michel Waldschmidt [1]

Exercises

We fix an algebraic closure $\overline{\mathbf{F}}_p$ of the prime field $\mathbf{F}_p$ of characteristic p. When q is a power of p, we denote by $\mathbf{F}_q$ the unique subfield of $\overline{\mathbf{F}}_p$ having q elements. Hence $\overline{\mathbf{F}}_p$ is also an algebraic closure of $\mathbf{F}_q$.

Exercise 1. Let $\mathbf{F}_q$ be a finite field and n a positive integer prime to q.
a) Check that the polynomial $X^{q^n} - X$ has no multiple factors in the factorial ring $\mathbf{F}_q[X]$.
b) Let $f \in \mathbf{F}_q[X]$ be an irreducible factor of $X^{q^n} - X$. Check that the degree d of f divides n.
c) Let f be an irreducible polynomial in $\mathbf{F}_q[X]$ of degree d where d divides n. Show that f divides $X^{q^n} - X$.
d) For $d \geq 1$ denote by E_d the set of monic irreducible polynomials in $\mathbf{F}_q[X]$ of degree d. Check

$$X^{q^n} - X = \prod_{d|n} \prod_{f \in E_d} f.$$

Exercise 2. Let $\mathbf{F}_q$ be a finite field and $f \in \mathbf{F}_q[X]$ be a monic irreducible polynomial with $f(X) \neq X$.
a) Show that the roots α of f in $\overline{\mathbf{F}}_p$ all have the same order in the multiplicative group $\overline{\mathbf{F}}_p^\times$. We denote this order by $p(f)$ and call it the *period* of f.
b) For ℓ a positive integer, check that $p(f)$ divides ℓ if and only if $f(X)$ divides $X^\ell - 1$.
c) Check that if f has degree n, then $p(f)$ divides $q^n - 1$. Deduce that q and $p(f)$ are relatively prime.
d) A monic irreducible polynomial f is *primitive* if its degree n and its period $p(f)$ are related by $p(f) = q^n - 1$. Explain the definition.
e) Recall that $X^2 + X + 1$ is the unique irreducible polynomials of degree 2 over $\mathbf{F}_2$, that there are two irreducible polynomials of degree 3 over $\mathbf{F}_2$:

$$X^3 + X + 1, \quad X^3 + X^2 + 1,$$

[1] This text is accessible on the author's web site
http://www.math.jussieu.fr/∼miw/coursVietnam2009.html

three irreducible polynomials of degree 4 over $\mathbf{F}_2$:

$$X^4 + X^3 + 1, \quad X^4 + X + 1, \quad X^4 + X^3 + X^2 + X + 1$$

and three monic irreducible polynomials of degree 2 over $\mathbf{F}_3$:

$$X^2 + 1, \quad X^2 + X - 1, \quad X^2 - X - 1.$$

For each of these 9 polynomials compute the period. Which ones are primitive?
f) Which are the irreducible polynomials over $\mathbf{F}_2$ of period 15? Of period 5?

Exercise 3. Let $f : \mathbf{F}_3^2 \to \mathbf{F}_3^4$ be the linear map

$$F(a,b) = (a, b, a+b, a-b)$$

and $\mathcal{C}$ be the image of f.
a) What are the length and the dimension of the code $\mathcal{C}$? How many elements are there in $\mathcal{C}$? List them.
b) What is the minimum distance $d(\mathcal{C})$ of $\mathcal{C}$? How many errors can the code $\mathcal{C}$ detect? How many errors can the code $\mathcal{C}$ correct? Is it a MDS code?
c) How many elements are there in a Hamming ball of $\mathbf{F}_3^4$ of radius 1? Write the list of elements in the Hamming ball of $\mathbf{F}_3^4$ of radius 1 centered at $(0,0,0,0)$.
d) Check that for any element $\underline{x}$ in $\mathbf{F}_3^4$, there is a unique $\underline{c} \in \mathcal{C}$ such that $d(\underline{c}, \underline{x}) \leq 1$.
What is $\underline{c}$ when $\underline{x} = (1, 0, -1, 1)$?

Exercise 4. Let $\mathbf{F}_q$ be a finite field with q elements. Assume $q \equiv 3 \pmod 7$. How many cyclic codes of length 7 are there on $\mathbf{F}_q$? For each of them describe the code: give its dimension, the number of elements, a basis, a basis of the space of linear forms vanishing on it, its minimum distance, the number of errors it can detect or correct and whether it is MDS or not.

Solutions to the exercises

Solution to Exercice 1.
a) The derivative of $X^{q^n} - X$ is -1, which has no root, hence $X^{q^n} - X$ has no multiple factor in characteristic p.
b) Let f be an irreducible divisor of $X^{q^n} - X$ of degree d and α be a root of f in $\overline{\mathbf{F}}_p$. The polynomial $X^{q^n} - X$ is a multiple of f, therefore it vanishes at α, hence $\alpha^{q^n} = \alpha$ which means $\alpha \in \mathbf{F}_{q^n}$. From the field extensions

$$\mathbf{F}_q \subset \mathbf{F}_q(\alpha) \subset \mathbf{F}_{q^n}$$

we deduce that the degree of α over $\mathbf{F}_q$ divides the degree of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$, that is d divides n.
c) Let $f \in \mathbf{F}_q[X]$ be an irreducible polynomial of degree d where d divides n. Let α be a root of f in $\overline{\mathbf{F}}_p$. Since d divides n, the field $\mathbf{F}_q(\alpha)$ is a subfield of $\mathbf{F}_{q^n}$, hence $\alpha \in \mathbf{F}_{q^n}$ satisfies $\alpha^{q^n} = \alpha$, and therefore f divides $X^{q^n} - X$.
d) In the factorial ring $\mathbf{F}_q[X]$, the polynomial $X^{q^n} - X$ having no multiple factor is the product of the monic irreducible polynomials which divide it.
□

Solution to Exercice 2.
a) Two conjugate elements α and $\sigma(\alpha)$ have the same order, since $\alpha^m = 1$ if and only if $\sigma(\alpha)^m = 1$.
b) Let α be a root of f. Since α has order $p(f)$ in the multiplicative group $\mathbf{F}_q(\alpha)^\times$ we have

$$p(f) | \ell \iff \alpha^\ell = 1 \iff f(X) | X^\ell - 1.$$

c) The n conjugates of a root α of f over $\mathbf{F}_q$ are its images under the iterated Frobenius $x \mapsto x^q$, which is the generator of the cyclic Galois group of $\mathbf{F}_q(\alpha)/\mathbf{F}_q$. From $\alpha^{q^n} = \alpha$ we deduce that f divides the polynomial $X^{q^n} - X$ (see also Exercise 1). Since $f(X) \neq X$ we deduce $\alpha \neq 0$, hence f divides the polynomial $X^{q^n - 1} - 1$. As we have seen in question b), it implies that $p(f)$ divides $q^n - 1$. The fact that the characteristic p does not divide $p(f)$ is then obvious.
d) An irreducible monic polynomial $f \in \mathbf{F}_q[X]$ is primitive if and only if any root α of f in $\overline{\mathbf{F}}_p$ is a generator of the cyclic group $\mathbf{F}_q(\alpha)^\times$.
e) Here is the answer:

q	d	$f(X)$	$p(f)$	primitive
2	2	X^2+X+1	3	yes
2	3	X^3+X+1	7	yes
2	3	X^3+X^2+1	7	yes
2	4	X^4+X^3+1	15	yes
2	4	X^4+X+1	15	yes
2	4	$X^4+X^3+X^2+X+1$	5	no
3	2	X^2+1	4	no
3	2	X^2+X-1	8	yes
3	2	X^2-X-1	8	yes

f) The two irreducible polynomials of period 15 over $\mathbf{F}_2$ are the two factors X^4+X^3+1 and X^4+X+1 of Φ_{15}. The only irreducible polynomial of period 5 over $\mathbf{F}_2$ is $\Phi_5(X)=X^4+X^3+X^2+X+1$.

□

Solution to Exercice 3.
a) This ternary code has length 4, dimension 2, the number of elements is $3^2=9$, the elements are

$$\begin{array}{ccc} (0,0,0,0) & (0,1,1,-1) & (0,-1,-1,1) \\ (1,0,1,1) & (1,1,-1,0) & (1,-1,0,-1) \\ (-1,0,-1,-1) & (-1,1,0,1) & (-1,-1,1,0) \end{array}$$

b) Any non–zero element in $\mathcal{C}$ has three non–zero coordinates, which means that the minimum weight of a non–zero element in $\mathcal{C}$ is 3. Since the code is linear, its minimum distance is 3. Hence it can detect two errors and correct one error. The Hamming balls of radius 1 centered at the elements in $\mathcal{C}$ are pairwise disjoint.

Recall that a MDS code is a linear code $\mathcal{C}$ of length n and dimension d for which $d(\mathcal{C})=n+1-d$. Here $n=4$, $d=2$ and $d(\mathcal{C})=3$, hence this code $\mathcal{C}$ is MDS.
c) The elements at Hamming distance ≤ 1 from $(0,0,0,0)$ are the elements of weight ≤ 1. There are 9 such elements, namely the center $(0,0,0,0)$ plus $2\times 4=8$ elements having three coordinates 0 and the other one 1 or -1:

$$\begin{array}{cccc} (1,0,0,0), & (-1,0,0,0), & (0,1,0,0), & (0,-1,0,0), \\ (0,0,1,0), & (0,0,-1,0), & (0,0,0,1), & (0,0,0,-1). \end{array}$$

A Hamming ball $B(\underline{x},1)$ of center $\underline{x}\in\mathbf{F}_3^4$ and radius 1 is nothing but the translate $\underline{x}+B(0,1)$ of the Hamming ball $B(0,1)$ by $\underline{x}$, hence the number

of elements in $B(\underline{x}, 1)$ is also 9.
d) The 9 Hamming balls of radius 1 centered at the elements of $\mathcal{C}$ are pairwise disjoint, each of them has 9 elements, and the total number of elements in the space $\mathbf{F}_3^4$ is 81. Hence these balls give a perfect packing: each element in $\mathbf{F}_3^4$ belongs to one and only one Hamming ball centered at $\mathcal{C}$ and radius 1.
For instance the unique element in the code at distance ≤ 1 from $\underline{x} = (1, 0, -1, 1)$ is $(1, 0, 1, 1)$. □

Solution to Exercice 4. The class of 3 in $(\mathbf{Z}/7\mathbf{Z})^\times$ is a generator of this cyclic group of order $6 = \phi(7)$:

$$(\mathbf{Z}/7\mathbf{Z})^\times = \{3^0 = 1,\ 3^1 = 3,\ 3^2 = 2,\ 3^3 = 6,\ 3^4 = 4,\ 3^5 = 5\}.$$

The condition $q \equiv 3 \pmod 7$ implies that q has order 6 in $(\mathbf{Z}/7\mathbf{Z})^\times$, hence Φ_7 is irreducible in $\mathbf{F}_q[X]$. The polynomial $X^7 - 1 = (X - 1)\Phi_7$ has exactly 4 monic divisors in $\mathbf{F}_3[X]$, namely

$$Q_0(X) = 1, \quad Q_1(X) = X - 1,$$

$$Q_2(X) = \Phi_7(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1, \quad Q_3(X) = X^7 - 1.$$

Hence there are exactly 4 cyclic codes of length 7 over $\mathbf{F}_q$.

The code $\mathcal{C}_0$ associated to the factor $Q_0 = 1$ has dimension 7, it is the full code $\mathbf{F}_q^7$ with q^7 elements. A basis of $\mathcal{C}_0$ is any basis of $\mathbf{F}_q^7$, for instance the canonical basis. The space of linear forms vanishing on $\mathcal{C}$ has dimension 0 (a basis is the empty set). The minimum distance is 1. It cannot detect any error. Since $d(\mathcal{C}) = 1 = n + 1 - d$, the code $\mathcal{C}_0$ is MDS.

The code $\mathcal{C}_1$ associated to the factor $Q_1 = X - 1$ has dimension 6, it is the hyperplane of equation $x_0 + \cdots + x_6 = 0$ in $\mathbf{F}_q$, it has q^6 elements. Let $T : \mathbf{F}_q^7 \to \mathbf{F}_q^7$ denote the right shift

$$T(a_0, a_1, a_2, a_3, a_4, a_5, a_6) = (a_6, a_0, a_1, a_2, a_3, a_4, a_5).$$

A basis (with 6 elements, as it should) of $\mathcal{C}_1$ is

$$\begin{array}{rrrrrrrrr}
e_0 = & & (1, & -1, & 0, & 0, & 0, & 0, & 0), \\
e_1 = & Te_0 = & (0, & 1, & -1, & 0, & 0, & 0, & 0), \\
e_2 = & T^2e_0 = & (0, & 0, & 1, & -1, & 0, & 0, & 0), \\
e_3 = & T^3e_0 = & (0, & 0, & 0, & 1, & -1, & 0, & 0), \\
e_4 = & T^4e_0 = & (0, & 0, & 0, & 0, & 1, & -1, & 0), \\
e_5 = & T^5e_0 = & (0, & 0, & 0, & 0, & 0, & 1, & -1).
\end{array}$$

Notice that $T^6e_0 = (-1, 0, 0, 0, 0, 0, 1)$ and

$$e_0 + Te_0 + T^2e_0 + T^3e_0 + T^4e_0 + T^5e_0 + T^6e_0 = 0.$$

This is related to

$$1 + X + X^2 + X^3 + X^4 + X^5 + X^6 = \Phi_7(X) = \frac{X^7 - 1}{X - 1}\cdot$$

The minimum distance of $\mathcal{C}_1$ is 2, it is a MDS code. It can detect one error (it is a parity bit check) but cannot correct any error.

The code $\mathcal{C}_2$ associated to the factor Q_2 has dimension 1 and q elements:

$$\mathcal{C}_2 = \{(a, a, a, a, a, a, a)\ ;\ a \in \mathbf{F}_q\} \subset \mathbf{F}_q^7.$$

It is the repetition code of length 7, which is the line of equation spanned by $(1, 1, 1, 1, 1, 1, 1)$ in $\mathbf{F}_q$, there are q elements in the code. It has dimension 1, its minimum distance is 7, hence is MDS. It can detect 6 errors and correct 3 errors.

The code $\mathcal{C}_3$ associated to the factor Q_3 is the trivial code of dimension 0, it contains only one element, a basis is the empty set, a basis of the space of linear forms vanishing on $\mathcal{C}_3$ is $x_0, x_1, x_2, x_3, x_4, x_5, x_6$. Its minimum distance is not defined, it is not considered as a MDS code.

□

This text is accessible on the internet

http://www.math.jussieu.fr/∼miw/coursVietnam2009.html