Chair of Network Architectures and Services
School of Computation, Information and Technology
Technical University of Munich

Network Coding
IN2315, WiSe 2021/22

Tutorial 1

October 25, 2021

Problem 1 Finite extension fields

Given the finite field $\mathbb{F}_p$, we consider the finite extension field

$$F_q[x] = \left\{ \sum_{i=0}^{n-1} a_i x^i \mid a_i \in \mathbb{F}_p \right\} \tag{1}$$

with $q = p^n$ elements. Specifically, let $p = 3$ and $n = 2$.

a)* Find a generator (primitive element) of $\mathbb{F}_3$.

As we know that there is a primitive element and that $0, 1 \in \mathbb{F}_3$ cannot be generators since those elements are idempotent, the generator must be 2, which is unique in this case.

b) Determine the inverse elements of the multiplicative group of $\mathbb{F}_3$, i. e., given $a \in \mathbb{F}_3 \setminus \{0\}$ determine $b \in \mathbb{F}_3 \setminus \{0\}$ such that $a \cdot b = 1$ (and thus $a = 1/b$).

- 1 is the neutral element and therefore self-inverse
- $(2 \cdot 2) \bmod 3 = 1$, i. e., 2 is also self-inverse

c) Determine the inverse elements of the additive group of $\mathbb{F}_3$, i. e., given $a \in \mathbb{F}_3$ determine $b \in \mathbb{F}_3$ such that $a + b = 0$ (and thus $a = -b$).

$$\begin{aligned}
(0+0) \bmod 3 &= 0 \quad &\Rightarrow -0 = 0 \\
(1+2) \bmod 3 &= 0 \quad &\Rightarrow -1 = 2 \\
(2+1) \bmod 3 &= 0 \quad &\Rightarrow -2 = 1
\end{aligned}$$

d)* Enumerate all $a \in F_q[x]$.

There are $q = 3^2 = 9$ elements:

$$\begin{aligned}
F_q[x] = \{ \ & 0, & 1, & \quad 2, \\
& x, & x+1, & \quad x+2, \\
& 2x, & 2x+1, & \quad 2x+2 \}
\end{aligned}$$

e)* Determine all reduction polynomials such that $F_q[x]$ forms a finite extension field.

The reduction polynomials must be of degree 2, i. e., candidates

$$\begin{aligned} a \in A = \{\ & x^2, & x^2+1, && x^2+2,\\ & x^2+x, & x^2+x+1, && x^2+x+2,\\ & x^2+2x, & x^2+2x+1, && x^2+2x+2,\\ & 2x^2, & 2x^2+1, && 2x^2+2,\\ & 2x^2+x, & 2x^2+x+1, && 2x^2+x+2,\\ & 2x^2+2x, & 2x^2+2x+1, && 2x^2+2x+2\} \end{aligned}$$

In order to obtain the set B of reducible polynomials of degree 2, it is sufficient to consider all polynomials of degree 1 in $F_q[x]$:

$\cdot$	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
x	x^2	–	–	–	–	–
$x+1$	x^2+x	x^2+2x+1	–	–	–	–
$x+2$	x^2+2x	x^2+2	x^2+x+1	–	–	–
$2x$	$2x^2$	$2x^2+2x$	$2x^2+x$	x^2	–	–
$2x+1$	$2x^2+x$	$2x^2+1$	$2x^2+2x+2$	x^2+2x	x^2+x+1	–
$2x+2$	$2x^2+2x$	$2x^2+x+2$	$2x^2+1$	x^2+x	x^2+2	x^2+2x+1

Suitable reduction polynomials are therefore $r \in A \backslash B$, i. e.,

$$r \in \{x^2+1, x^2+x+2, x^2+2x+2, 2x^2+2, 2x^2+x+1, 2x^2+2x+1\}.$$

f) Take two reduction polynomials $r_1 \neq r_2$ and show that $(a \cdot b) \bmod r_1 \neq (a \cdot b) \bmod r_2$ for $a, b \in F_q[x]$ in general.

We choose $a = x+2$, $b = 2x+2$, $r_1 = x^2+1$, and $r_2 = 2x^2+2x+1$. Then we obtain

$$\begin{aligned} a \cdot b &= 2x^2+1,\\ (2x^2+1) \bmod (x^2+1) &= 2, \text{ and}\\ (2x^2+1) \bmod (2x^2+2x+1) &= x. \end{aligned}$$

From now on we assume $r(x) = x^2+1$.

g)* State the addition and multiplication tables for $F_q[x]$ subject to $r(x) = x^2+1$.

$+$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
1	1	2	0	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$
2	2	0	1	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$
x	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$	0	1	2
$x+1$	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$	1	2	0
$x+2$	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$	2	0	1
$2x$	$2x$	$2x+1$	$2x+2$	0	1	2	x	$x+1$	$x+2$
$2x+1$	$2x+1$	$2x+2$	$2x$	1	2	0	$x+1$	$x+2$	x
$2x+2$	$2x+2$	$2x$	$2x+1$	2	0	1	$x+2$	x	$x+1$

$\cdot$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$x+1$	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
$x+2$	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
$2x$	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$2x+1$	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
$2x+2$	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

h) For all $a \in F_q[x]$, determine the addtive inverse element, i. e., $b \in F_q[x] : a + b = 0$. Note that we can write $b = -a$.

i) Determine a generator g for $F_q[x]$.

We have to check all elements $a \in F_q[x]$ wether they are a generator. We try $a = (x + 2)$ and prove that it can generate all elements of $F_q[x]$:

$$\begin{aligned}
(x+2)^0 &= 1\\
(x+2)^1 &= x+2\\
(x+2)^2 &= x\\
(x+2)^3 &= 2x+2\\
(x+2)^4 &= 2\\
(x+2)^5 &= 2x+1\\
(x+2)^6 &= 2x\\
(x+2)^7 &= x+1
\end{aligned}$$

j) State the log and antilog tables for $F_q[x]$ subject to $r(x) = x^2 + 1$ and $g(x)$.

With the solution of the previous subproblem we can simply fill the tables:

	A
0	1
1	$x+2$
2	x
3	$2x+2$
4	2
5	$2x+1$
6	$2x$
7	$x+1$

	L
1	0
2	4
x	2
$x+1$	7
$x+2$	1
$2x$	6
$2x+1$	5
$2x+2$	3

k) Compute the following multiplications via the log table approach and validate the result with the multiplication table

$$(2x+2)(x+1) =$$
$$(x+1)(2x) =$$

$$(2x+2)(x+1) = \mathrm{A}(\mathrm{L}(2x+2)+\mathrm{L}(x+1)) = \mathrm{A}(3+7) = \mathrm{A}(2) = x$$
$$(x+1)(2x) = \mathrm{A}(\mathrm{L}(x+1)+\mathrm{L}(2x)) = \mathrm{A}(7+6) = \mathrm{A}(5) = 2x+1$$

Problem 2 Implementation (homework)

For this problem, use the finite extension field from the previous problem, i. e. $p = 3$, $n = 2$, $r(x) = x^2 + 1$, and the generator $g(x)$ you have previously determined.

a) Implement both the log table algorithm and the full table approach (creating a two-dimensional array with all possible multiplication results) in a programming language of your choice.

b) Benchmark your algorithms, i. e., determine the average execution time per multiplication, and explain the results.