

## Network Coding IN2315, SoSe 2024

### Tutorial 1

June 5, 2024

### Problem 1 Finite extension fields

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

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

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

- a)\* Find a generator (primitive element) of  $\mathbb{F}_3$ .
- 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  $a = 1/b$ ).
- 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  $a = -b$ ).
- d)\* Enumerate all  $a \in F_q[x]$ .
- e)\* Determine all reduction polynomials such that  $F_q[x]$  forms a finite extension field.
- 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.

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

- g)\* State the addition and multiplication tables for  $F_q[x]$  subject to  $r(x) = x^2 + 1$ .
- h) For all  $a \in F_q[x]$ , determine the additive 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  $F_q[x]$ .
- j) State the log and antilog tables for  $F_q[x]$  subject to  $r(x) = x^2 + 1$  and  $g(x)$ .
- k) Compute the following multiplications via the log table approach and validate the result with the multiplication table

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

## 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.