Introduction to Information Theory, Fall 2020

Practice problems for exercise class #11

You do **not** have to hand in these exercises, they are for your practice only.

1. **Finite fields $\mathbb{F}_q$:** The set $\mathbb{F}_q = \{0, 1, \ldots, q-1\}$, where q is a prime number, has natural addition and multiplication operations, by performing these modulo q.

   $\mathbb{F}_2$ is just a bit with addition modulo 2 (XOR) and the usual multiplication: $1 \oplus 1 = 0$, $1 \times 1 = 1$ etc. In mathematics, $\mathbb{F}_q$ is called a finite 'field' with q elements.

   In $\mathbb{F}_q$, any nonzero number has a multiplicative inverse, i.e., if $x \neq 0$ is in $\mathbb{F}_q$ then there exists a unique element y in $\mathbb{F}_q$ such that $xy = yx = 1$ (all arithmetic is done modulo q). We usually write x^{-1} for this element y and call it the *inverse of* x. For example, $2^{-1} = 2$ in $\mathbb{F}_3$, since $2 \times 2 = 4 \pmod 3 = 1$.

   (a) Write down all nonzero elements of $\mathbb{F}_5$ and $\mathbb{F}_7$, and find their inverses.

   In class, we said that an element $\alpha \in \mathbb{F}_q$ is called a *generator* (or 'primitive element') if $\{\alpha, \alpha^2, \ldots, \alpha^{q-1}\}$ runs over all nonzero numbers in $\mathbb{F}_q$. Generators exist for any prime q.

   (b) Find all generators of $\mathbb{F}_5$ and $\mathbb{F}_7$.

   Remark: The restriction to prime numbers is important. Otherwise, inverses and generators do not necessarily exist.

2. **Multiplying polynomials:** One can also consider polynomials with coefficients in a finite field $\mathbb{F}_q$, which we will write as

   $$P = p_0 + p_1 Z + \cdots + p_d Z^d$$

   with $p_i \in \mathbb{F}_q$, $d \in \mathbb{N}$ and Z a formal variable. The number d is called the degree of the polynomial (assuming that $p_d \neq 0$). The algebraic structure of $\mathbb{F}_q$ allows us to define addition and multiplication of polynomials over $\mathbb{F}_q$ as well.

   (a) Compute the product of the following polynomials with coefficients in $\mathbb{F}_5$: $P = Z^2 + 2Z + 3$ and $Q = Z^3 + Z^2 + 1$.
   (b) Compute the product of the following polynomials with coefficients in $\mathbb{F}_7$: $P = Z^3 + Z + 4$ and $Q = 2Z^2 + 5Z + 1$.

   Just like for polynomials with coefficients in $\mathbb{C}$ we can study roots of polynomials. If $\alpha \in \mathbb{F}_q$ and P is a polynomials with coefficients in $\mathbb{F}_q$, we say that α is a root of $P = p_0 + p_1 Z + \cdots + p_d Z^d$ if

   $$P(\alpha) = p_0 + p_1 \alpha + \cdots + p_d \alpha^d = 0.$$

   (c) Find the roots $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_5$ of the polynomial $P = Z^3 + Z^2 + Z + 1$ with coefficients in $\mathbb{F}_5$. Verify that you can write P in the form $P = (Z - \alpha_1)(Z - \alpha_2)(Z - \alpha_3)$. *Remark: Not all polynomials over $\mathbb{F}_q$ have roots in $\mathbb{F}_q$. Can you find an example?*

3. **Dividing polynomials:** Just like we can divide integers by each other when we are happy with leaving a remainder, we can divide any two polynomials with remainder. That is, given two polynomials A and B, where $B \neq 0$, there are unique polynomials Q and R such that

$$A = QB + R,$$

and the degree of R is less than the degree of B. We will call Q the *quotient* and R the *remainder*, and write $R = A \bmod B$. You can compute Q and R in completely the same way how you do 'long division' between integers to figure out their quotient and remainder:

```
Q <- 0
R <- A
while R and degree(R) >= degree(B):
  d <- degree(R) - degree(B)
  L <- leading_coeff(R) leading_coeff(B)^{-1} * Z^d
  Q <- Q + L
  R <- R - L B
```

Here, the leading coefficient of a polynomial $P = p_0 + p_1 Z + \cdots + p_d Z^d$ of degree d is p_d. That is, we start with A and repeatedly subtract a suitable multiple of B such that the degree decreases. This algorithm works not only for polynomials whose coefficients are real numbers, but also when the coefficients are in $\mathbb{F}_q$.

(a) Compute the quotient Q and remainder R for the following polynomials with coefficients in $\mathbb{F}_3$: $A = Z^3 + 1$ and $B = 2Z$. Verify that your procedure gave the correct answer by computing $QB + R$.
(b) Compute the quotient Q and remainder R for the following polynomials with coefficients in $\mathbb{F}_5$: $A = Z^3 + 2Z$ and $B = Z + 4$. Verify that your procedure gave the correct answer by computing $QB + R$.
(c) Consider two polynomials A and B with coefficients in a finite field $\mathbb{F}_q$, and let $R = A \bmod B$. Suppose that $\alpha \in \mathbb{F}_q$ is a root of B, meaning that $B(\alpha) = 0$. Show that α is also a root of $C = A - R$.