**Algebraic Methods** November 30, 2016

# Finite Fields

Lecturer: Amir Shpilka Hand in date: **Not for submission**

The point of the following questions is to construct a finite field of order $p^d$, for every prime $p$ and positive integer $d$, as well as some facts about finite fields.

**Definition 0.1.** *A polynomial $f \in \mathbb{F}[x]$ is monic if its leading coefficient equals 1. That is, if $\deg(f) = d$ then $f = x^d + \sum_{i=0}^{d-1} a_i x^i$, where for every $i$ $a_i \in \mathbb{F}$.* ◊

1. Polynomial division with reminder: Let $\mathbb{F}$ be a field. Prove that for any two polynomials $f, g \in \mathbb{F}[x]$ there exist unique polynomials $s, r \in \mathbb{F}[x]$ such that $f = sg + r$ and $\deg(r) < \deg(g)$.

2. Given two polynomials $f, g \in \mathbb{F}[x]$ such that $\deg(f) \geq \deg(g)$ consider Euclid's algorithm for them: If $g = 0$ then stop and output $f$. Otherwise, let $f = sg + r$ as in Question 1. Run the algorithm again on $g$ and $r$. Prove that the algorithm returns the greatest common divisor of $f$ and $g$.

3. Let $f \in \mathbb{F}[x]$ be an irreducible[1] monic polynomial of degree $d$. Consider the set of all polynomials of degree at most $d-1$ over $\mathbb{F}$:

$$\mathbb{K} = \{g \mid g \in \mathbb{F}[x] \text{ and } \deg(g) < \deg(f)\}.$$

   Define addition of two polynomials in $\mathbb{K}$ in the natural way. Define multiplication in $\mathbb{K}$, denoted $\cdot_{\mathbb{K}}$, in the following way. Let $g_1, g_2 \in \mathbb{K}$. Consider division with reminder in $\mathbb{F}$: $g_1 \cdot g_2 = s \cdot f + r$. Then, in $\mathbb{K}$, we define $g_1 \cdot_{\mathbb{K}} g_2 \triangleq r$. In other words, multiplication in $\mathbb{K}$ is simply multiplication modulo $f$. Prove that $\mathbb{K}$ is a field.

4. Prove that if in Question 3 we would take a *reducible* polynomial $f$ then $\mathbb{K}$ would not be a field.

5. Prove that the field that you constructed in Question 3 has dimension $d$ as a vector space over $\mathbb{F}$.

6. Conclude that for every prime number $p$ and integer $d$ there exists a field of size $p^d$. You can use the fact that for every $d$ there exists an irreducible polynomial of degree $d$ over $\mathbb{F}$. This field is called Galois Field and is denoted $\mathrm{GF}(p^d)$ (or sometimes just $\mathbb{F}_{p^d}$).

7. Let $\mathbb{F}$ be e finite field. For an integer $n$, let $n_{\mathbb{F}}$ be the element of $\mathbb{F}$ obtained by adding 1 to itself $n$ times in $\mathbb{F}$. I.e. $4_{\mathbb{F}} = 1 + 1 + 1 + 1$ where addition is done in $\mathbb{F}$. Let $m$ be the minimal nonzero integer such that $m_{\mathbb{F}} = 0_{\mathbb{F}}$ (why does such $m$ exist?). Prove that $m$ is a prime number. $m$ is called the characteristic of $\mathbb{F}$.

[1] If $g \in \mathbb{F}[x]$ is monic and $g$ divides $f$ then $g = f$ or $g = 1$.

8. Prove that if $\mathbb{F}$ is a finite field of order $q$ and characteristic $p$ (recall the definition in Question 7), then $q = p^d$ for some integer $d$.

9. Prove that if $\mathbb{F} \subseteq \mathbb{K}$ are two finite fields then there exists an integer $c$ such that $|\mathbb{F}|^c = |\mathbb{K}|$.

10. The order of an element $0 \neq x \in \mathbb{F}_q$, $\text{ord}(x)$, is the minimal integer $0 < r$ such that $x^r = 1$. Prove that for every $x \neq 0$, $\text{ord}(x)$ divides $q - 1$.
**Hint:** Define an equivalence relation on $\mathbb{F}_q \setminus \{0\}$: $y \sim z$ if and only if $y/z$ is a power of $x$. I.e., iff there exists some $s$ such that $y/z = x^s$ (make sure you understand that this is an equivalence relation). Then show that all equivalence classes have the same order.

11. Prove that if $\text{ord}(x) = a$ and $\text{ord}(y) = b$ and $a$ and $b$ are co-prime (i.e. they do not have non-trivial common factors) then $\text{ord}(x \cdot y) = a \cdot b$.

12. Prove that for every integer $0 < t < q$ there are at most $t$ elements in $\mathbb{F}_q$ for which $\text{ord}(x)$ divides $t$.
**Hint:** a nonzero polynomial of degree $t$ has at most $t$ roots.

13. Prove that there exists an integer $x \in \mathbb{F}_q$ such that $\{1, x, x^2, \ldots, x^{q-2}\} = \mathbb{F}_q \setminus \{0\}$. In other words, the powers of $x$ give all the nonzero elements in $\mathbb{F}_q$.