Introduction to Coding Theory (CMU: Spring 2010)
Basics of Finite Fields

Venkatesan Guruswami

February 2010

In the next segment of the course, we will study explicitly constructed codes, and develop error-correction algorithms for them. Prominent among these will be certain algebraic constructions of codes based on polynomials over finite fields.

It is possible to get quite far treating finite fields as "black-boxes" that allow the field operations to be performed efficiently as atomic steps, along with just one important mantra:

> A non-zero polynomial of degree d with coefficients from a field $\mathbb{F}$ has at most d roots in $\mathbb{F}$.

But it is nevertheless desirable to have a good working knowledge of the basics of the theory of finite fields, and we will appeal to some of these results later on for list decoding some powerful algebraic codes. You are likely already familiar with this material from your undergraduate algebra. You can refer to your favorite algebra text for the basic theorems and their proofs, but I wanted to point to some notes that you can turn to if you need a refresher and a convenient reference.

So here are some excellently done notes on finite fields, written by G. David Forney and available on MIT's OpenCourseWare for the course 6.451 Principles of Digital Communication II. These notes rigorously prove everything that we would need (and more!) from first principles, in a nice sequence.

Collected below are some basic results about finite fields, for quick reference. (I do not recall the definition of fields and the field axioms here.) All these facts are proved in the above linked notes.

1. For every prime p, there is a unique finite field of size p that is isomorphic to $\mathbb{F}_p$ which is the set $\{0, 1, \ldots, p-1\}$ under mod-p addition and multiplication.
2. For each prime p, positive integer $m \geq 1$, and polynomial $g(X)$ with coefficients in $\mathbb{F}_p$ of degree m that is *irreducible* (in $\mathbb{F}_p[X]$), the set of polynomials in $\mathbb{F}_p[X]$ of degree at most $m-1$ with addition and multiplication of the polynomials defined modulo $g(X)$ is a finite field (denoted $\mathbb{F}_{g(X)}$) with p^m elements.
3. Every finite field is isomorphic to such a field, and therefore must have p^m elements for some prime p and positive integer m.

4. For every prime p and integer $m \geq 1$, there exists an irreducible polynomial $g(X) \in \mathbb{F}_p[X]$ of degree m. Therefore, there is a finite field with p^m elements for every prime p and positive integer m.

5. Additively, a finite field with p^m elements has the structure of a vector space of dimension m over $\mathbb{F}_p$.

6. The multiplicative group of a finite field (consisting of its non-zero elements) is cyclic. In other words, the non-zero elements of a field $\mathbb{F}$ can be written as $\{1, \gamma, \gamma^2, \ldots, \gamma^{|\mathbb{F}|-2}\}$ for some $\gamma \in \mathbb{F}$.

   - A γ with such a property is called a *primitive element* of the field $\mathbb{F}$.
   - A field $\mathbb{F}$ has $\varphi(|\mathbb{F}| - 1)$ primitive elements, where $\phi(\cdot)$ is the Euler's totient function.

7. All fields of size p^m are isomorphic to $\mathbb{F}_{g(X)}$ for an arbitrary choice of degree m irreducible polynomial $g(X) \in \mathbb{F}_p[X]$.

   The finite field with p^m elements is therefore unique up to isomorphism field and will be denoted by $\mathbb{F}_{p^m}$.

   Remark: While one can pick any irreducible $g(X)$ to represent the field $\mathbb{F}_{p^m}$ as $\mathbb{F}_{g(X)}$, sometimes a special choice can be judicious. For example, the complexity of multiplication is better if $g(X)$ is sparse (i.e., has very few non-zero coefficients).

8. The elements of $\mathbb{F}_{p^m}$ are the p^m distinct roots of the polynomial $X^{p^m} - X \in \mathbb{F}_p[X]$.

9. For each k dividing m, the field $\mathbb{F}_{p^m}$ has a unique subfield of size p^k, which consists of the roots of the polynomial $X^{p^k} - X$.

10. The polynomial $X^{p^m} - X$ is the product of all monic irreducible polynomials in $\mathbb{F}_p[X]$ whose degree divides m, with no repetitions.