CS 810: Complexity Theory	2/20/2007
Handout: Finite Fields	
Instructor: Dieter van Melkebeek	TA: Jeff Kinne

This handout covers some basic properties of finite fields that will be needed in the course and may not be familiar to all students. We first show the existence of finite fields and then consider the efficiency of arithmetic within finite fields. We conclude with a few remarks regarding uses of finite fields.

1 Preliminaries

We first recap the terminology we use. A *group* is a structure consisting of a universe G and a binary operation $+$ that is associative, has a neutral element (a.k.a. a unit), and such that every element has an inverse. If $+$ is commutative, the group is called commutative. A *ring* is a structure consisting of a universe R and two binary operations $+$ and $\cdot$ where: $(R, +)$ forms a commutative group, $\cdot$ is associative on R, and $\cdot$ distributes over $+$. If $\cdot$ is commutative, the ring is called commutative. A *field* is a commutative ring with a multiplicative unit such that each element other than the additive unit 0 has an inverse for $\cdot$. We often refer to $(F, +)$ as the additive group of the field and to $(F \setminus \{0\}, \cdot)$ as the multplicative group of the field.

The following proposition gives a useful sufficient condition for a finite ring to be a field.

Proposition 1. *Consider a finite commutative ring R with a multiplicative unit that is different from 0. Then R is a field iff for all $a, b \in R$, $ab = 0$ implies that $a = 0$ or $b = 0$.*

Proof. Let the multiplicative unit of R be denoted by 1. We must only show that each element a of R has a multiplicative inverse. We show this by showing that the mapping $x \to a \cdot x$ is a bijection. If this is a bijection, then there is some element a' such that $a \cdot a' = 1$. This a' is the multiplicative inverse of a.

Now suppose for the purpose of contradiction that $x \to a \cdot x$ is not a bijection. Then we have $a \cdot x_1 = a \cdot x_2$ for distinct $x_1, x_2 \in R$. Rearranging terms, we have $a \cdot (x_1 - x_2) = 0$ which contradicts the hypothesis. □

Given a field F, we consider polynomials over a single variable with coefficients from F.

Exercise 1. *The set of polynomials $F[x]$ over F forms a commutative ring with a multiplicative unit.*

We will be interested in polynomials over F that do not factor over F, as defined presently.

Definition 1. *Let F be a field. A polynomial $g(x)$ with coefficients from F is called* irreducible over F *if there are no two polynomials $g_1(x)$ and $g_2(x)$ with coefficients over F and of degree less than $g(x)$ such that $g(x) = g_1(x) \cdot g_2(x)$.*

Example: Consider the polynomial $g(x) = x^3 + x + 1$ over $\mathbb{Z}_2$. We claim that $g(x)$ is irreducible over $\mathbb{Z}_2$. In principle, we must verify that each pair of polynomials of degree less than three over $\mathbb{Z}_2$ multiplies to yield something other than $g(x)$. The set of polynomials that must be checked is:

$\{1, x, 1+x, x^2, 1+x^2, x+x^2, 1+x+x^2\}$. In this case we can also argue as follows. Since $g(x)$ has degree 3, at least one of the factors of any factorization as $g(x) = g_1(x)g_2(x)$ with $g_1(x)$ and $g_2(x)$ of degree less than three, has to have degree exactly one. This implies that $g(x)$ would have a zero over $\mathbb{Z}_2$. However, $g(0) = 1 = g(1)$. ⊠

An irreducible polynomial plays the role in the polynomial ring that prime numbers play in the integers. The following is a property of irreducible polynomials that also holds for prime numbers in the integers.

Proposition 2. *Let $g(x)$, $g_1(x)$, and $g_2(x)$ be polynomials over a field F. If $g(x)$ is irreducible over F, then $g(x)$ divides $g_1(x) \cdot g_2(x)$ iff $g(x)$ divides $g_1(x)$ or $g(x)$ divides $g_2(x)$.*

Proof idea: Just as an integer can be factored uniquely into its prime factors, a polynomial over a field can be factored uniquely into irreducible polynomials. If $g(x)$ divides $g_1(x) \cdot g_2(x)$, then $g(x) \cdot h(x) = g_1(x) \cdot g_2(x)$ for some polynomial $h(x)$. If we view this equation in terms of the unique factorization of each polynomial into irreducible polynomials, it becomes evident that $g(x)$ must divide either $g_1(x)$ or $g_2(x)$. □

The final building block we need is that of modular arithmetic. We assume the reader is familiar with $\mathbb{Z}_n$, the integers modulo n. We can also use modular arithmetic over the ring of polynomials over a field F.

Definition 2. *Let $F[x]$ be the ring of polynomials over a field F, and let $g(x)$ be a polynomial with coefficients from F. Then $F[x]/g(x)$ is the ring of polynomials over F modulo $g(x)$. Formally, $F[x]/g(x)$ contains an equivalence class for each polynomial that can result as a remainder upon dividing by $g(x)$, and arithmetic among the equivalence classes is performed modulo $g(x)$.*

Exercise 2. *If F is a field and $g(x)$ is a polynomial with coefficients from F, then $F[x]/g(x)$ is a finite commutative ring with a multiplicative unit. Further, if $g(x)$ has degree d, the elements of $F[x]/g(x)$ are in one-to-one and onto correspondence with the polynomial of degree less than d over F.*

2 Existence

We have now set up the appropriate background to prove the existence of finite fields. We first mention the finite fields that we are most familiar with.

Theorem 1. *For all $n \geq 2$, $\mathbb{Z}_n$ is a commutative ring with a multiplicative unit. $\mathbb{Z}_n$ is a field if and only if n is prime.*

The second part of Theorem 1 follows from Proposition 1 and demonstrates finite fields that are suitable for many of our purposes. However, there are other finite fields we will need to make use of. The following theorem is the main purpose of this handout, demonstrating a finite field for all prime powers.

Theorem 2. *For prime p, and $k \geq 1$ there is a field with p^k elements.*

Proof. Let $\mathbb{Z}_p[x]$ be the ring of polynomials with coefficients from $\mathbb{Z}_p$, and $\mathbb{Z}_p[x]/g(x)$ be the quotient ring of polynomials modulo the polynomial $g(x)$. By Exercise 2, $\mathbb{Z}_p[x]/g(x)$ is a finite commutative ring with a multiplicative unit. The theorem follows from the following two lemmas.

Lemma 1. *Let $k \geq 1$ be an integer and p a prime. There exists an irreducible polynomial of degree k over $\mathbb{Z}_p$.*

Proof idea: This can be proved by a careful counting argument showing that the number of irreducible polynomials is positive. We do not present further details here. □

Lemma 2. *$\mathbb{Z}_p[x]/g(x)$ is a field if and only if $g(x)$ is irreducible over $\mathbb{Z}_p$.*

Proof. The elements of $\mathbb{Z}_p[x]/g(x)$ are in one-to-one and onto correspondence with the polynomials over $\mathbb{Z}_p$ of degree less than the degree of $g(x)$. A product of two elements is zero iff the product of the corresponding polynomials is a multiple of $g(x)$.

If $g(x)$ is not irreducible, then $g(x) = g_1(x) \cdot g_2(x)$ for some polynomials $g_1(x)$ and $g_2(x)$ of degree less than the degree of $g(x)$, meaning that for non-zero ring elements $g_1(x)$ and $g_2(x)$ their product is zero. Then $\mathbb{Z}_p[x]/g(x)$ is not a field by Proposition 1.

Let $g(x)$ be irreducible. Suppose there are $g_1(x)$ and $g_2(x)$ whose product is a multiple of $g(x)$ (i.e., whose product is zero in the ring). Then Proposition 2 tells us that $g(x)$ must divide at least one of $g_1(x)$ or $g_2(x)$, meaning at least one of $g_1(x)$ or $g_2(x)$ is zero in the ring. By Proposition 1, $\mathbb{Z}_p[x]/g(x)$ is a field. □

□

In fact, the construction given in Theorem 2 is enough to generate all possible finite fields, stated formally in the following theorem whose proof we omit.

Theorem 3. *Let F be a finite field. Then F has p^k elements for some prime p and integer $k \geq 1$. Further, each finite field with p^k elements is isomorphic.*

We use $\mathrm{GF}(p^k)$ to denote a generic finite field with p^k elements. [1]

Example: Let us construct $\mathrm{GF}(2^3)$ using the irreducible polynomial of degree 3 from the example in the first section. Therefore, $\mathrm{GF}(2^3)$ can be constructed as $\mathbb{Z}_2[x]/(x^3 + x + 1)$. Each element of the field is viewed as a degree at most two polynomial, and can thus be specified with three bits. As an example of multiplication in the field, $(x^2+1)\cdot(x+1) = (x^3+x+x^2+1) = (x^3+x+1)+x^2 = 0 + x^2 = x^2$. As an example of addition in the field, $(x^2 + 1) + (x + 1) = (x^2 + x + 1 + 1) = x^2 + x$. ⊠

3 Complexity

Theorem 2 only shows that finite fields of order p^k exist. For a finite field to be of practical use, it should be efficiently constructible, and arithmetic in the field should be efficient. We leave it as an exercise to verify that arithmetic can be performed in $\mathrm{GF}(p^k)$ in polynomial time once an irreducible polynomial of degree k over $\mathbb{Z}_p$ is found.

To efficiently construct $\mathrm{GF}(p^k)$, all that needs to be done is to find an irreducible polynomial of degree k over $\mathbb{Z}_p$. We would like to be able to find such a polynomial in polynomial time, where the input length is the number of bits needed to specify a degree k polynomial with coefficients in

[1] "GF" stands for "Galois Field," after Evariste Galois.

$\mathbb{Z}_p$, i.e. $O(k \cdot \log p)$. It is unknown if there is an algorithm running in time $\text{poly}(k, \log p)$ to do this. The following is essentially the best known algorithm.

Theorem 4 ([Shoup]). *There is a deterministic algorithm running in time poly(k, p) to find an irreducible polynomial of degree k over $\mathbb{Z}_p$.*

Notice that for small values of p this is in fact a polynomial time algorithm. In particular, this shows that we can in polynomial time construct a suitable irreducible polynomial to construct $\text{GF}(2^n)$. For most purposes, this is sufficient. If our requirements are even more lenient, we can do even better. The following gives an explicit formula for irreducible polynomials for certain values of n.

Theorem 5 ([van Lint] Thm 1.1.28). *Let $n = 2 \cdot 3^{\ell-1}$. Then $x^n + x^{n/2} + 1$ is irreducible over $\mathbb{Z}_2$.*

4 Remarks

One common use of finite fields is to view data as elements of the finite field and take advantage of the nice properties of polynomials over fields. In particular, a degree d polynomial can have at most d roots. We will see in the lectures how this property is used.

Finally, we remark on the distinction between formal polynomials and polynomials as functions. A formal polynomial refers to the particular coefficients that specify it. Two formal polynomials over a finite field F induce the same function iff they are equal modulo $\prod_{a \in F}(x - a)$. In particular, all polynomials of degree less than q over $\text{GF}(q)$ induce different functions.

References

[van Lint] J.J. van Lint, *Introduction to Coding Theory, 3rd Edition*, Springer-Verlag New York Inc., 1998.

[Shoup] V. Shoup, "New algorithms for finding irreducible polynomials over finite fields", Mathematics of Computation 54:435-447, 1990.