Lecture Notes for Math 696
Coding Theory

Michael E. O'Sullivan
mosulliv@math.sdsu.edu
www-rohan.sdsu.edu/~mosulliv

March 4, 2002

1 A few more things about finite fields

Definition 1.1. The characteristic of a field $F$ is 0 if no finite sum of $1 \in F$ is 0. Otherwise, the characteristic is the smallest integer $p$ such that

$$1 + 1 + 1 + \cdots + 1 + 1 = 0$$

$p$ terms

Definition 1.2. A subfield of a field $K$ is a subset $F$ which contains $0_K$ and $1_K$ and is a field under the operations of $K$, $+$ and $\ast_K$.

If $F$ is a subfield of $K$, and $\alpha \in K$ we define $F[\alpha]$ to be the smallest subfield of $K$ containing $F$ and $\alpha$.

Theorem 1.3. Let $F$ be a subfield of $K$. Suppose that $\alpha \in K$ is the root of an irreducible monic polynomial $P(x) \in F[x]$. Then $F[x]/P(x)$ is isomorphic to $F[\alpha]$ under the map taking the conjugate class of $x$ to $\alpha$.

Proof: Suppose that $P(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0$. The field $F[x]/P(x)$ has $1, x, x^2, \ldots, x^{n-1}$ as a basis (here I really mean the conjugate class of these elements). And the field $F[\alpha]$ has basis $1, \alpha, \ldots, \alpha^{n-1}$. The map $\phi$ taking $x^i$ to $\alpha^i$ is clearly an isomorphism of vector spaces. The multiplicative structure on $F[\alpha]$ is completely determined by $P(\alpha) = 0$, that is, $\alpha^n = -b_{n-1}\alpha^{n-1} + b_{n-2}\alpha^{n-2} + \cdots + b_1\alpha + b_0$. Likewise, the multiplicative structure on $F[x]/P(x)$ is determined by a similar formula with the conjugate class of $x$ replacing $\alpha$. Consequently, $\phi(f(x) + g(x)) = \phi(f(x)) + \phi(g(x))$ (again, conjugate classes of $f(x), g(x)$).

This theorem is of great use in showing isomorphisms between two different representations of $\mathbb{F}_q$ over $\mathbb{F}_p$. It is sufficient to find an element in each representation which satisfies a particular irreducible polynomial, $P(x) \in \mathbb{F}_p[x]$. Then map these two elements to each other. This comment holds when $p$ itself is a power of a prime.

Useful formulas

We assume $q = p^n$ with $p$ prime. Recall that we showed that $\mathbb{F}_q$ with is the splitting field of $x^{q-1} - 1$ over $\mathbb{F}_p$. Here are some simple consequences:
For any $\alpha \in \mathbb{F}_q$, 

$$\alpha^q = \alpha$$ \hspace{1cm} (1) 

$$1 + \alpha + \alpha^2 + \alpha^3 + \cdots + \alpha^{q-2} = \begin{cases} 1 & \text{if } \alpha = 0 \\ -1 & \text{if } \alpha = 1 \\ 0 & \text{otherwise} \end{cases}$$ \hspace{1cm} (2) 

The final formula follows from the fact that $x^{q-1} - 1 = (x+1)(x^{q-2}+x^{q-3}+\cdots+x+1)$. All elements of $\mathbb{F}_q$ except 0 and 1 are therefore roots of $(x^{q-2} + x^{q-3} + \cdots + x + 1)$.

**Conjugates**

**The Fourier transform**

See Blahut's book [1, p. 169]

**Vandermonde determinant**

See Blahut's book [1, p. 169]

## 2 The Euclidean Algorithm

Let $a, b$ be integers with $b > 0$. The following algorithm computes the greatest common divisor of $a$ and $b$.

**Input:** Nonzero integers $a, b$.

**Objective:** To compute the (positive) greatest common divisor of $a$ and $b$.

**Algorithm:** Define inductively $r_i$ for $i \geq 0$ and $q_i$ for $i \geq 1$:

While $r_i \neq 0$,

$$r_0 = a$$

$$r_1 = b$$

and $r_{i+1}, q_i$ are the remainder and quotient when $r_{i-1}$ is divided by $r_i$,

$$r_{i-1} = q_ir_i + r_{i+1}$$

$$0 \leq r_{i+1} < r_i$$

**Theorem 2.1.** The algorithm above terminates after a finite number of steps. If $n$ is the smallest integer such that $r_{n+1} = 0$ then $r_n$ is the greatest common divisor of $a$ and $b$.

The number of steps $n$ is at most $1 + \log b/(\log(1 + \sqrt{5}) - 1)$, where $\log$ is base 2.

**Proof:** See Rosen [2]. \hfill $\Box$

We now consider a matrix version of the Euclidean algorithm that produces the linear combination of $a$ and $b$ that gives the gcd.
Input: Nonzero integers \( a, b \).
Objective: To compute the a linear combination of \( a \) and \( b \) which gives the greatest common divisor of \( a \) and \( b \).
Algorithm: Define inductively the remainders \( r_i \) and quotients \( q_i \) of the previous algorithm. We also define matrices \( R^{(i)} \), and \( 2 \times 2 \) matrix \( T^{(i)} \) for \( i \geq 0 \):

\[
R^{(0)} = \begin{bmatrix} b \\ a \end{bmatrix}
\]
\[
T^{(0)} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}
\]

While \( r_i \neq 0 \), define \( q_i \) as usual

\[
Q^{(i)} = \begin{bmatrix} -q_i & 0 \\ 1 & 0 \end{bmatrix}
\]
\[
R^{(i)} = Q^{(i)} R^{(i-1)}
\]
\[
T^{(0)} = Q^{(i)} T^{(i-1)}
\]

**Theorem 2.2.** The matrix \( R^{(i)} \) keeps track of the usual remainders.

\[
R^{(i)} = \begin{bmatrix} r_{i+1} \\ r_i \end{bmatrix}
\]

The matrix \( T^{(k)} \) is the product of the \( Q^{(i)} \),

\[
T^{(k)} = \prod_{i=1}^{k} Q^{(i)}
\]

If the algorithm terminates after \( n \) steps then

\[
\begin{bmatrix} r_{n+1} \\ r_n \end{bmatrix} = T^{(n)} \begin{bmatrix} b \\ a \end{bmatrix}
\]

so the bottom row of \( T^{(n)} \) gives a linear combination of \( a \) and \( b \) that produces the gcd, \( r_n \).

**Exercises 2.3.**

1) Write a procedure implementing the matrix version of the Euclidean algorithm. Do it first for integers, then for polynomials over \( \mathbb{Q} \), then generalize to polynomials over finite fields.

2) Write a Maple procedure to find all irreducible polynomials of degree less than \( n \) over \( \mathbb{F}_2 \). Extend to other finite fields.

3) Factor \( x^{80} - 1 \) over \( \mathbb{F}_3 \) and explain the relationship between the factors and the elements of \( \mathbb{F}_{81} \).

Factor \( x^{80} - 1 \) over \( \mathbb{F}_9 \) and explain the relationship between the factors and the elements of \( \mathbb{F}_{81} \).
4) Make a table showing the possible orders and the number of elements of each order for \( F_{64}, F_{128}, \) and \( F_{256} \).

5) Let \( n = 6 \). Find all irreducible polynomials over \( F_2 \) of \( \text{deg} \, d \) where \( d | n \). Find the product of these polynomials.

For a given prime \( p \), let \( I(d) \) be the set of irreducible polynomials of degree \( d \) over \( F_p \). Shop that for \( n > 0 \),

\[
\prod_{d | n} \prod_{f \in I(d)} f = x^n - 1
\]

Write Maple code to verify this result.

6) Prove that for any polynomial \( f(x) \) of degree less than \( q - 1 \),

\[
\sum_{\alpha \in F_q} f(\alpha) = 0
\]

. Hint: reduce to the case of a monomial, \( x^i \). For \( i \) coprime to \( q - 1 \) use (2). For \( i \) not coprime to \( q - 1 \) you will need to think about the previous exercise and (2).

References
