PhD course: Finite Fields
Some slides for 2nd Lecture

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

12-12-2012

Let F be a field. A subset K of F that is itself a field under the operations of F is called a subfield of F.

A field that containing no proper subfields is called a prime field.

$\mathbb{F}_p$ is a prime field.

Let K be a subfield of F and $\theta \in F$. If θ satisfies a nontrivial polynomial equation with coefficients in k, i.e. if $a_n\theta^n + \cdots + a_1\theta + a_0 = 0$, with $a_i \in K$ not all being 0, then θ is said to be algebraic over K.

An ideal I in a ring R is a subgroup of $(R, +)$ such that $\lambda x \in I$, for every $\lambda \in R$ and $x \in I$.

$F[X]$ is a principal ideal domain, that is every ideal is generated by only one element.
How do we find such an element?, using the Euclidean algorithm.

$$J = \{f \in K[X] : f(\theta) = 0\}$$

is an ideal of $K[X]$.

IF θ is algebraic over K, then the uniquely determined monic polynomial $g \in K[X]$ is called the minimal polynomial of θ over K.

Theorem

If $\theta \in F$ is algebraic over K, then its minimal polynomial g over K has the following properties:

- g is irreducible in $K[X]$.
- For $f \in K[X]$ we have $f(\theta) = 0$ if and only if g divides f.
- g is the monic polynomial in $K[X]$ of least degree having θ as a root.

If L is and extension field of K then L may be viewed as a vector space over K.

Theorem

Let $\theta \in F$ be algebraic over K and g its minimal polynomial over K (of degree n). Then:

- $K(\theta)$ is isomorphic to $K[X]/(g)$
- The dimension of $K(\theta)$ over K (as vector space) is n and a basis is $\{1, \theta, \ldots, \theta^{n-1}\}$

Theorem

Let $\mathbb{F}_q$ be the finite field with $q = p^n$ elements. Then every subfield of $\mathbb{F}_q$ has order p^m, where m is a positive divisor of n. Conversely, if m is a positive divisor of n, then there is exactly one subfield of $\mathbb{F}_q$ with p^m elements.

Why do we need to perform extensions in practice?

Let $f \in \mathbb{F}_q$ be a polynomial of degree $m \geq 1$ with $f(0) \neq 0$. Then there exists a positive integer $e \leq q^m - 1$ such that $f(x)$ divides $x^e - 1$.
e is called the order of f.

Theorem

Let $f \in \mathbb{F}_q[X]$ be an irreducible polynomial over $\mathbb{F}_q$ of degree m with $f(0) \neq 0$. Then the order of f is equal to the order of any root of f in the multiplicative group $\mathbb{F}_q^*$.

Let $f \in \mathbb{F}_q[X]$ of degree $m \geq 1$, f is called primitive over $\mathbb{F}_q$ if it is the minimal polynomial over $\mathbb{F}_q$ of a primitive element of $\mathbb{F}_{q^m}$.

Theorem

A polynomial $f \in \mathbb{F}_q[X]$ of degree m, f is a primitive polynomial over $\mathbb{F}_q$ if and only if is monic, $f(0) \neq 0$ and the order of f is $q^m - 1$.

A third representation of the elements of $\mathbb{F}_q q$

Let $f = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + X^n \in \mathbb{F}_p[X]$ an irreducible polynomial. We consider its companion matrix:

$$A = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

$f(A) = 0$, that is $a_0 I + a_1 A + \cdots + a_{n-1} A^{n-1} + A^n$, where I is the $n \times n$ identity matrix. Hence, A is like a root of f:

The polynomials in A over $\mathbb{F}_p$ of degree less than n yield a representation of the elements of $\mathbb{F}_q$.

Example: $f = X^2 + 1 \in \mathbb{F}_3[X]$. The companion matrix is....? Construct $\mathbb{F}_9$!

Finite fields

- $GF(p^n)$ finite field with p^n elements.
- $GF(p^n) \simeq GF(p)/q(x)$, with $q(x)$ any irreducible polynomial of deg n
- $q(x)$ is primitive if for any root a, $GF(p^n)^* = \{a^0, \ldots, a^{p^n-2}\}$.
- q primitive, a root $\Rightarrow$ elements can be represented as
  - a^k, $0 \leq k \leq p^n - 1$ easy multiplication
  - $f(a)$, $\deg(f) \leq n-1$ easy addition

Example

- $GF(5)$ finite field
- $q = x^2 - 2$ irreducible
- $GF(5^2) = GF(5)(a)$, a root of q.
- $a^3 = 2a$, $a^{11} = 2a$

- $q = x^2 + 4x + 2$ primitive
- $GF(5^2) = GF(5)(a)$, a root of q.
- $a^3 = 4a + 3$, $a^{11} = 3a + 2$

Singular

Singular is free a computer algebra system that is part of SAGE.

```
                     SINGULAR                                 /
 A Computer Algebra System for Polynomial Computations       /   version 3-0-3
                                                           0<
     by: G.-M. Greuel, G. Pfister, H. Schoenemann            \   May 2007
FB Mathematik der Universitaet, D-67653 Kaiserslautern        \
>
```

One can work with polynomial rings over a finite field: $GF(p^n)$

```
> ring R=(2^3,a),(x,y),lp;
> minpoly;
1*a^3+1*a^1+1*a^0
```

$R = \mathbb{F}_8[x, y]$ with the lexicographical order, a is a root of the primitive polynomial $x^3 + x + 1$. Singular has a table with primitive polynomials for $GF(p^n)$, with $p < 256$ and $p^n < 2^{16}$.

Representation of $GF(p^n)$ in Singular

$GF(p^n) = \{a^0, a^1, \ldots, a^{p^n-2}\} \cup \{0\}$

- Multiplication is easy: $a^i a^j = a^{i+j \mod (p^n-1)}$
- $a^i + a^j = a^i(1 + a^{j-i \mod (p^n-1)})$

```
> 1+a;
a3
```

There is a table with the values $1 + a^i$, with $i = 0, \ldots p^n - 2$.

One can define a finite field using his favourite irreducible polynomial. In this case, elements are represented as polynomials of degree lower than or equal to n in $GF(p)[x]$. One can define in this way finite fields with more elements, but computations are not as fast as before.

Extending from a finite field

- $GF(p) = \mathbb{Z}/(p) = \mathbb{F}_p$
- $GF(p^l) = \mathbb{F}_p(a)$
- $GF(p^m) = \mathbb{F}_p(b)$
- $l \mid m \Rightarrow GF(p^l) \hookrightarrow GF(p^m)$
- But $a \hookrightarrow ???$

One possibility:
exhaustive search

Example

- $GF(2) = \mathbb{F}_2$
- $GF(2^3) = \mathbb{F}_2(a)$, minpoly = $a^3 + a + 1$
- $GF(2^6) = \mathbb{F}_2(b)$, minpoly = $b^6 + b + 1$

By exhaustive search:

$$(b^k)^3 + (b^k) + 1 = 0$$

for $k = 27, 54, 45$.

Easy extension

- $GF(p^l) = \mathbb{F}_p(a)$, $GF(p^m) = \mathbb{F}_p(b)$
- $M_{p,n} = p^n - 1$
- The smallest power of b that generates $GF(p^l)$ is $\gamma = b^{M_{p,m}/M_{p,l}}$
- We have an easy extension if $a = \gamma$
- Equivalently, if $q_{GF(p^m)}(x) \mid q_{GF(p^l)}(x^{M_{p,m}/M_{p,l}})$

Example

- $GF(2^3) = \mathbb{F}_2(a)$, $GF(2^6) = \mathbb{F}_2(b)$
- $M_{2,3} = 7$, $M_{2,6} = 63$, $M_{2,6}/M_{2,3} = 9$
- We require $a = b^9$.

Compatibility condition

$$\phi_{S\hookrightarrow F} = \phi_{E\hookrightarrow F} \circ \phi_{S\hookrightarrow E}$$

This condition is satisfied with the previous requirement.

$$GF(p^s) = \mathbb{F}_p(a) \hookrightarrow GF(p^e) = \mathbb{F}_p(b) \hookrightarrow GF(p^f) = \mathbb{F}_p(c)$$

$$a \hookrightarrow b^{M_{p,e}/M_{p,s}}, \quad b \hookrightarrow c^{M_{p,f}/M_{p,e}}$$

$$\Downarrow$$

$$a \hookrightarrow c^{M_{p,f}/M_{p,s}}$$

Conway polynomials-Definition

$C_{p,n}$ Conway polynomial:

- primitive of deg n
- (compatible) $C_{p,n} \mid C_{p,n'}(x^{M_{p,n}/M_{p,n'}}) \forall n' \mid n$
- (unique) $C_{p,n}$ minimal wrt $<_{lex}$:

$$a_d x^d + \cdots + a_0 <_{lex} b_d x^d + \ldots + b_0$$

iff for some i, $a_j = b_j$ for all $j < i$ and
$(-1)^{d-i} a_i < (-1)^{d-i} b_i$
where $0 < 1 < \ldots < p-1$ in $\mathbb{Z}_p$.

Example: Computation of $C_{2,6}$

$C_{2,1} = x+1$, $C_{2,2} = x^2+x+1$ and $C_{2,3} = x^3+x+1$

```
> factorize(gcd(x^63+1, x21^2+x21+1, x9^3+x9+1));
  x6+x5+x2+x+1; x6+x5+1; x6+x4+x3+x+1
```

The Conway polynomial $C_{2,6}$ is $x^6+x^4+x^3+x+1$.

- Conway polynomials were introduced by R. Parker in 1990, they were used in data bases like the Modular Atlas character tables [Jansen, Lux, Parker, Wilson].
- The existence of Conway polynomials is shown using the Chinese Remainder theorem.
- There is no algebraic reason for the requirement that the Conway polynomial is minimal wrt $<_{lex}$.

Applications

- To have an standard notation for elements in $GF(P^n)$.
- To perform an extension from $GF(P^{n'})$ to $GF(P^n)$, with $n' \mid n$.
- Data can be easily ported between different computer algebra systems like Sage, Macaulay2 and Magma.

First algorithm: (improved) exhaustive search

1. $G = gcd(\{C_{p,n'}(x^{M_{p,f}/M_{p,e}})\})$, n' maximal divisor of n.
2. Iterate through all polynomials C of deg n, and check:
   - C is irreducible
   - $C \mid G$
   - C is primitive

Example

Computation of $C_{2,5}$:

1. $G = C_{2,1}(x^{31}) = x^{31} + 1$
2. $x^5 + 1$, not irreducible
   $x^5 + x + 1$, not irreducible
   $x^5 + x^2 + 1$, Conway

Frank Lübeck

- For a project concerning the Lyons simple group it was needed the Conway Polynomial for $GF(67^{18})$.
- Lübeck estimated that it was needed 10^{10} years to compute it using the exhaustive search in GAP
- Using many computers in parallel he was able to compute $C_{67,18}$. He wrote a parallelized program based on the second algorithm (i.e. list the compatible polynomials).
- One can download from his webpage a huge list of Conway Polynomials. For instance, 2^{409} and 109987^4.

`http://www.math.rwth-aachen.de:8001/~Frank.Luebeck/data/ConwayPol/`

Further Algorithms?

For large finite fields, exhaustive search may take a lot of time. Especially when there are few compatible polynomials.

- $GF(p^n)$, with $n = q_1^{e_1} \cdots q_s^{e_s}$.
- For $1 \leq i \leq s$, $d_i = n/q_i$ and $m_i = M_{p,n}/M_{p,d_i}$.
- $g = gcd(m_1, \ldots, m_s)$.

The number of monic polynomials of degree n compatible with the lower order Conway polynomials is g (and some of them are not primitive).

Then, assuming that these polynomials are distributed randomly (uniformly) in the lexicographical listing of all degree n polynomials we expect to text p^n/g polynomials before finding the first acceptable one. For composite n (and even n moderately large) this is impractical.

Second algorithm: based on polynomials [Heath, Loehr, 04]

1. $D = \{d_1, ..., d_s\}$, maximal divisors of n
2. $m_i = M_{p,n}/M_{p,d_i}$
3. $g = gcd_{1 \leq i \leq s}(\{m_i\})$
4. $z = x^g$, $G = gcd(\{C_{p,d_i}(z^{m_i/g})\})$
5. z_0 root of G in $GF(p^n)$.
6. For all α, primitive g-th root of z_0, compute the minimal polynomials.
7. Return the lexicographically smaller one.

Example: Computation of $C_{2,6}$:

1. $D = \{2, 3\}$
2. $m_1 = 21$, $m_2 = 9$
3. $g = 3$
4. $G = gcd(z^{14} + z^7 + 1, z^9 + z^3 + 1) = z^6 + z^5 + z^4 + z^2 + 1$
5. $z_0 = a^{15}$ $GF(2^6) = \mathbb{F}_2(a)$, $a^6 + a + 1 = 0$
6. $\alpha \in \{a^5, a^{26}, a^{47}\}$. The minimal polynomials are $x^6 + x^5 + x^2 + x + 1$, $x^6 + x^4 + x^3 + x + 1$, $x^6 + x^5 + 1$.
7. $C_{2,6} = x^6 + x^4 + x^3 + x + 1$

Third algorithm: based on elements [Heath, Loehr 04]

1. $D = \{d_1, \ldots, d_s\}$, maximal divisors of n
2. x_i a root of C_{p,d_i} in $G^F(p^n)$.
3. x such that $x^{m_i} = x_i$.
4. For all α, primitive g-th root of x, compute the minimal polynomials.
5. Return the lexicographically smaller.

Warning: not any root of C_{p,d_i} works.

- $x^{m_i m_j} = x_i^{m_j} = x_j^{m_i}$
- Therefore, $\{x_i\}$ must satisfy

$$x_i^{m_j} = x_j^{m_i} \ \forall (i,j).$$

- If not, choose another root. (The roots of C_{p,d_i} are $\{x_i, x_i^p, \ldots, x_i^{p^{d_i-1}}\}$.)