MODELLING FINITE FIELDS

Hendrik Lenstra

Mathematisch Instituut

Universiteit Leiden

Finite fields

A *finite field* is a finite set E equipped with elements $0,\, 1 \in E$ and maps $+,\, \cdot : E \times E \to E$ such that for all $a,\, b,\, c \in E$ one has

$$\begin{aligned} (a \cdot b) \cdot c = a \cdot (b \cdot c), &\quad (a + b) + c = a + (b + c), \\ \exists d : d + a = 0, &\quad (\exists e : e \cdot a = 1) \Leftrightarrow a \neq 0, \\ 1 \cdot a = a, &\quad (a + b) \cdot c = (a \cdot c) + (b \cdot c), \\ 0 + a = a, &\quad a \cdot (b + c) = (a \cdot b) + (a \cdot c). \end{aligned}$$

Classifying finite fields

Theorem (E. Galois, 1830; E. H. Moore, 1893)**.**
There is a bijective map

$$\{\text{finite fields}\}/\cong \;\longrightarrow\; \{\text{primes}\} \times \mathbf{Z}_{>0}$$

sending $[E]$ *to* $(\operatorname{char} E, \deg E)$.

A field of size p^n is denoted by $\mathbf{F}_{p^n}$ or $\mathrm{GF}(p^n)$.

Explicit models

An *explicit model* for a field of size p^n is a field with additive group $\mathbf{F}_p^n = \bigoplus_{i=0}^{n-1} \mathbf{F}_p \cdot e_i$, where $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.

Such a model is numerically specified by the system $(a_{ijk})_{i,j,k=0}^{n-1}$ of elements $a_{ijk} \in \mathbf{F}_p$ satisfying

$$e_i \cdot e_j = \sum_{k=0}^{n-1} a_{ijk} e_k \quad \text{for all } i,\ j.$$

Space: $O(n^3 \log p)$.

Recognizing explicit models

Theorem. *For some* $t \in \mathbf{Z}_{>0}$*, there is an algorithm that, when* $p \in \mathbf{Z}_{>1}$*,* $n \in \mathbf{Z}_{>0}$*, and a system* $(a_{ijk})_{i,j,k=0}^{n-1}$ *of* n^3 *elements* $a_{ijk} \in \mathbf{Z}/p\mathbf{Z}$ *are given, decides in time at most* $(n + \log p)^t$ *whether these define an explicit model for a field of size* p^n*.*

Defining finite fields

A *finite field* is a finite set E equipped with elements 0, $1 \in E$ and maps $+, \cdot : E \times E \to E$ such that for all a, b, $c \in E$ one has

$$\begin{aligned} (a \cdot b) \cdot c = a \cdot (b \cdot c), &\quad (a + b) + c = a + (b + c), \\ \exists d : d + a = 0, &\quad (\exists e : e \cdot a = 1) \Leftrightarrow a \neq 0, \\ 1 \cdot a = a, &\quad (a + b) \cdot c = (a \cdot c) + (b \cdot c), \\ 0 + a = a, &\quad a \cdot (b + c) = (a \cdot b) + (a \cdot c). \end{aligned}$$

Characterizing finite fields

Theorem. *Let $R, +$ be a finite abelian group equipped with a bilinear multiplication $\cdot$. Then R is a field with $+$ and $\cdot$ if and only if*

- *the multiplication is associative;*
- *the exponent p of R is prime;*
- *the map $F\colon R \to R$, $x \mapsto x^p$ is bijective;*
- *the preimage of 0 under the map $F - 1\colon R \to R$, $x \mapsto x^p - x$, has size p.*

An algorithm for recognizing finite fields

Input: p, n, a_{ijk} $(0 \le i,\ j,\ k < n)$.

To be tested: $R = \bigoplus_{i=0}^{n-1} (\mathbf{Z}/p\mathbf{Z}) e_i$ is a field with multiplication $e_i \cdot e_j = \sum_{k=0}^{n-1} a_{ijk} e_k$.

- test commutativity and associativity;
- test primality of p;
- with $e_i^p = \sum_{j=0}^{n-1} f_{ij} e_j$ and $F = (f_{ij})_{i,j=0}^{n-1}$, test $\operatorname{rank} F = n$ and $\operatorname{rank}(F - I) = n - 1$.

Irreducibility testing

Corollary. *There is a polynomial-time algorithm that, given a finite field E and $f \in E[X]$, tests whether f is irreducible.*

Proof: f is irreducible if and only if $E[X]/(f)$ is a finite field.

Factoring polynomials

Open problem. *Is there a polynomial-time algorithm that, given a finite field E and $f \in E[X] \setminus \{0\}$, factors f into irreducible factors?*

Factoring polynomials

Open problem. *Is there a polynomial-time algorithm that, given a finite field E and $f \in E[X]\setminus\{0\}$, factors f into irreducible factors?*

- Yes if a probabilistic algorithm is allowed.
- Yes if $\operatorname{char} E$ is fixed.
- Yes if GRH is true and $\deg f$ is fixed.

Factoring quadratic polynomials

Theorem. *There is, for some* $t \in \mathbf{Z}_{>0}$, *an algorithm that, given a finite field* E *and* $f \in E[X]$, $\deg f = 2$, *finds the set* $Z(f)$ *of all zeroes of* f *in* E, *and that, if GRH is true, runs in time at most* $(1 + \log \#E)^t$.

The case $\operatorname{char} E = 2$

Let $f = uX^2 + vX + w$.

The map $E \to E$, $x \mapsto ux^2 + vx$, is $\mathbf{F}_2$-linear.

Using linear algebra over $\mathbf{F}_2$, one can determine the preimage of w, which equals $Z(f)$.

The case $\operatorname{char} E > 2$

Let $f = uX^2 + vX + w$ and $d = v^2 - 4uw$.

- If $d^{(\#E-1)/2} = -1$, then $Z(f) = \emptyset$.
- If $d = 0$, then $Z(f) = \{-v/(2u)\}$.
- If $d^{(\#E-1)/2} = 1$, then

  $$Z(f) = \{(-v + x)/(2u) : x \in E,\ x^2 = d\}.$$

The case $\operatorname{char} E > 2$

Let $f = uX^2 + vX + w$ and $d = v^2 - 4uw$.

- If $d^{(\#E-1)/2} = -1$, then $Z(f) = \emptyset$.
- If $d = 0$, then $Z(f) = \{-v/(2u)\}$.
- If $d^{(\#E-1)/2} = 1$, then
  $$Z(f) = \{(-v + x)/(2u) : x \in E,\ x^2 = d\}.$$

Conclusion: we may assume $f = X^2 - d$ and $d^{(\#E-1)/2} = 1$.

Taking squareroots in $\mathbf{F}_p$ *with* p *odd*

First, trying $c = 2, 3, \ldots$ in succession, find $c \in \mathbf{F}_p$ with $c^{(p-1)/2} = -1$.

If GRH is true, then the least such c is at most $4(\log p)^2$.

Taking squareroots in $\mathbf{F}_p$ with p odd

First, trying $c = 2,\ 3,\ \ldots$ in succession, find $c \in \mathbf{F}_p$ with $c^{(p-1)/2} = -1$.

If GRH is true, then the least such c is at most $4(\log p)^2$.

Next apply the *Shanks-Tonelli* method to find $\sqrt{d}$.

The Shanks-Tonelli method

Given an odd prime p and c, $d \in \mathbf{F}_p$ with $c^{(p-1)/2} = -1$ and $d^{(p-1)/2} = 1$, it finds $x \in \mathbf{F}_p$ with $x^2 = d$.

The Shanks-Tonelli method (1)

Given an odd prime p and c, $d \in \mathbf{F}_p$ with $c^{(p-1)/2} = -1$ and $d^{(p-1)/2} = 1$, it finds $x \in \mathbf{F}_p$ with $x^2 = d$.

Write $p - 1 = 2^k \cdot (2l + 1)$.
Replacing c and d by c^{2l+1} and d^{2l+1}, one may assume

$$c^{2^{k-1}} = -1, \quad d^{2^{k-1}} = 1.$$

(Note: $\sqrt{d} = \sqrt{d^{2l+1}} \cdot d^{-l}$.)

The Shanks-Tonelli method (2)

The method works with pairs (x, i) $\in \mathbf{F}_p \times \{0, 1, \ldots, k-1\}$ that satisfy

$$(x^2)^{2^i} = d^{2^i},$$

starting with $x = c$ and $i = k - 1$.

The Shanks-Tonelli method (2)

The method works with pairs (x, i) $\in \mathbf{F}_p \times \{0, 1, \ldots, k-1\}$ that satisfy

$$(x^2)^{2^i} = d^{2^i},$$

starting with $x = c$ and $i = k - 1$.

- If $i = 0$: done! Else:
- If $(x^2)^{2^{i-1}} = d^{2^{i-1}}$: replace (x, i) by $(x, i-1)$ and repeat.
- If $(x^2)^{2^{i-1}} = -d^{2^{i-1}}$: replace (x, i) by $(x \cdot c^{2^{k-1-i}}, i-1)$ and repeat.

Factoring quadratic polynomials

Theorem. *There is, for some* $t \in \mathbf{Z}_{>0}$, *an algorithm that, given a finite field* E *and* $f \in E[X]$, $\deg f = 2$, *finds the set* $Z(f)$ *of all zeroes of* f *in* E, *and that, if GRH is true, runs in time at most* $(1 + \log \# E)^t$.

The remaining case

Given a finite field E and $d \in E$ with $\#E = p^n$, $p > 2$, $n > 1$, $d^{(p^n-1)/2} = 1$, find $x \in E$ with $x^2 = d$.

The remaining case

Given a finite field E and $d \in E$ with $\#E = p^n$, $p > 2$, $n > 1$, $d^{(p^n-1)/2} = 1$, find $x \in E$ with $x^2 = d$.

Use linear algebra over $\mathbf{F}_p$ to find $y \in E$, $y \neq 0$, with $y^p = d^{(p-1)/2} \cdot y$.

The remaining case

Given a finite field E and $d \in E$ with $\#E = p^n$, $p > 2$, $n > 1$, $d^{(p^n-1)/2} = 1$, find $x \in E$ with $x^2 = d$.

Use linear algebra over $\mathbf{F}_p$ to find $y \in E$, $y \neq 0$, with $y^p = d^{(p-1)/2} \cdot y$.

Then $(d/y^2)^{(p-1)/2} = 1$, so d/y^2 is a square in $\mathbf{F}_p$, and if $z^2 = d/y^2$ then $(yz)^2 = d$.

Classifying finite fields

Theorem (E. Galois, 1830; E. H. Moore, 1893)**.**
There is a bijective map

$$\{\text{finite fields}\}/\cong \;\longrightarrow\; \{\text{primes}\} \times \mathbf{Z}_{>0}$$

sending $[E]$ *to* $(\operatorname{char} E, \deg E)$.

A field of size p^n is denoted by $\mathbf{F}_{p^n}$ or $\mathrm{GF}(p^n)$.

Constructing finite fields

Conjecture. *For some $t \in \mathbf{Z}_{>0}$, there is an algorithm that for given p, n constructs in time at most $(n + \log p)^t$ an explicit model for a field of size p^n.*

This is correct

- if a probabilistic algorithm is allowed,
- if GRH is true,
- if p is fixed.

Constructing quadratic finite fields

For $p > 2$, knowing an explicit model for $\mathbf{F}_{p^2}$ is equivalent to knowing $c \in \mathbf{F}_p$ with $c^{(p-1)/2} = -1$.

Such a value for c can be efficiently found with a probabilistic algorithm by drawing c at random.

Deterministically, one can try $c = 2, 3, \ldots$ in succession. If GRH is true, this method runs in polynomial time.

Classifying finite fields

Theorem (E. Galois, 1830; E. H. Moore, 1893)**.**
There is a bijective map

$$\{\text{finite fields}\}/\cong \;\longrightarrow\; \{\text{primes}\} \times \mathbf{Z}_{>0}$$

sending $[E]$ *to* $(\operatorname{char} E, \deg E)$.

A field of size p^n is denoted by $\mathbf{F}_{p^n}$ or $\mathrm{GF}(p^n)$.

The number of isomorphisms between
two fields of size p^n equals n.

Field homomorphisms

The number of field homomorphisms from a finite field E to a finite field E' equals $\deg E$ if

$$\operatorname{char} E = \operatorname{char} E' \text{ and } \deg E \,|\, \deg E'$$

and 0 otherwise, and all these field homomorphisms are *injective*.

Field homomorphisms

The number of field homomorphisms $E \to E'$ equals $\deg E$ if

$$\operatorname{char} E = \operatorname{char} E' \text{ and } \deg E \mid \deg E'$$

and 0 otherwise, and all these field homomorphisms are *injective*.

If E and E' are specified as explicit models, then a field homomorphism $E \to E'$ is specified as a matrix over $\mathbf{F}_p$, where $p = \operatorname{char} E = \operatorname{char} E'$.

Finding field homomorphisms

Given two finite fields E, E' with $\operatorname{char} E = \operatorname{char} E' = p$, how to construct all field embeddings $E \to E'$?

Finding field homomorphisms

Given two finite fields E, E' with $\operatorname{char} E = \operatorname{char} E' = p$, how to construct all field embeddings $E \to E'$?

Conventional wisdom: write $E = \mathbf{F}_p(\alpha)$; find the irreducible polynomial f of α over $\mathbf{F}_p$; and find all zeroes β of f in E'. All embeddings $E \to E'$ are given by $\alpha \mapsto \beta$.

Finding a primitive element

If $E = \bigoplus_{i=0}^{n-1} \mathbf{F}_p \cdot e_i$ is a finite field, then some $\alpha \in \{e_0, e_1, \ldots, e_{n-1}\}$ satisfies

$$\#\{\alpha^{p^i} : 0 \leq i < n\} = n.$$

For any such α one has $E = \mathbf{F}_p(\alpha)$, and the irreducible polynomial f of α over $\mathbf{F}_p$ equals $\prod_{i=0}^{n-1}(X - \alpha^{p^i})$.

Modern wisdom

Theorem (HWL, 1991). *There is a polynomial-time algorithm that, given two explicit models E, E' for finite fields, computes all field embeddings $E \to E'$.*

The quadratic case

Suppose $p = \operatorname{char} E = \operatorname{char} E' > 2$,
$\deg E = \deg E' = 2$.

Write $E = \mathbf{F}_p(\sqrt{c})$ and $E' = \mathbf{F}_p(\sqrt{d})$,
where c, $d \in \mathbf{F}_p$, $c^{(p-1)/2} = d^{(p-1)/2} = -1$.

Then $(c/d)^{(p-1)/2} = 1$, so using
Shanks-Tonelli we can find all $e \in \mathbf{F}_p$
with $c/d = e^2$.

The two field isomorphisms are then
given by $\sqrt{c} \mapsto e \cdot \sqrt{d}$.

Consistent embeddings

Theorem (Bart de Smit & HWL). *There is a polynomial-time algorithm that, given two explicit models E, E' for finite fields, computes a field embedding $\varphi_{E,E'}\colon E \to E'$ if there is one, and that has the property $\varphi_{E,E''} = \varphi_{E',E''} \circ \varphi_{E,E'}$ whenever meaningful.*

Consistent embeddings

Theorem (Bart de Smit & HWL). *There is a polynomial-time algorithm that, given two explicit models E, E' for finite fields, computes a field embedding $\varphi_{E,E'}\colon E \to E'$ if there is one, and that has the property $\varphi_{E,E''} = \varphi_{E',E''} \circ \varphi_{E,E'}$ whenever meaningful.*

The algorithm is potentially useful for large distributed computing projects.

Proof modulo the main theorem

Main theorem (Bart de Smit & HWL)**.**
There is a polynomial-time algorithm that on input p, n, and an explicit model E for a field of size p^n, computes the standard model $\mathbf{F}_{p^n}$ as well as a field isomorphism $\psi_E\colon \mathbf{F}_{p^n} \to E$.

To obtain consistent embeddings, it suffices to take $\varphi_{E,E'} = \psi_{E'} \circ \psi_E^{-1}$.

Standard models

Here $\mathbf{F}_{p^n}$ denotes the *standard model* for a field of size p^n.

There are compatible embeddings $\mathbf{F}_{p^n} \subset \mathbf{F}_{p^m}$ for $n|m$.

The quadratic case

For $p > 2$, $n = 2$ one can take

$$\mathbf{F}_{p^2} = \mathbf{F}_p \cdot 1 \oplus \mathbf{F}_p \cdot \sqrt{s(p)},$$

where

$$s(p) = \sqrt{\sqrt{\cdots\sqrt{1}}},$$

each squareroot being chosen in

$$\{(p+1)/2, \ldots, p-2, p-1\},$$

and the number of $\sqrt{\ }$-signs being the number of factors 2 in $p-1$.

The general case

To define the standard model $\mathbf{F}_{p^n}$ for general p and n, in such a way that the main theorem can be proved, we use a structural description of $\bar{\mathbf{F}}_p$, to be presented tomorrow.