STANDARD MODELS FOR FINITE FIELDS

Hendrik Lenstra

Joint work with Bart de Smit

Mathematisch Instituut, Universiteit Leiden

Finite fields

A *finite field* is a field E with $\#E < \infty$.

Finite fields, characteristic, degree

A *finite field* is a field E with $\#E < \infty$.

The *characteristic* $\operatorname{char} E$ of a finite field E is the additive order of 1 in E.

The *degree* $\deg E$ of E is the least number of generators of the additive group of E.

If $\operatorname{char} E = p$ and $\deg E = n$ then $\#E = p^n$.

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 $\mathrm{GF}(p^n)$.

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 $\mathrm{GF}(p^n)$.

Example: $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.

The number of isomorphisms between two fields of size p^n equals n, so for $n \geq 2$ a field of size p^n is not *uniquely unique*.

Explicit models for finite fields

An *explicit model* for a finite field of size p^n is a field with underlying additive group $\mathbf{F}_p^n = \mathbf{F}_p \times \mathbf{F}_p \times \ldots \times \mathbf{F}_p$.

Explicit models for finite fields

An *explicit model* for a finite field of size p^n is a field with underlying additive group $\mathbf{F}_p^n = \mathbf{F}_p \times \mathbf{F}_p \times \ldots \times \mathbf{F}_p$.

If $\mathbf{F}_p^n = \bigoplus_{i=0}^{n-1} \mathbf{F}_p{\cdot}e_i$, then

$$e_i \cdot e_j = \sum_{k=0}^{n-1} a_{ijk} e_k$$

for certain $a_{ijk} \in \mathbf{F}_p$.

Explicit models for finite fields

An *explicit model* for a finite field of size p^n is a field with underlying additive group $\mathbf{F}_p^n = \mathbf{F}_p \times \mathbf{F}_p \times \ldots \times \mathbf{F}_p$.

If $\mathbf{F}_p^n = \bigoplus_{i=0}^{n-1} \mathbf{F}_p \cdot e_i$, then

$$e_i \cdot e_j = \sum_{k=0}^{n-1} a_{ijk} e_k$$

for certain $a_{ijk} \in \mathbf{F}_p$.

Exercise. The number of such explicit models equals $\left(\prod_{i=0}^{n-1}(p^n - p^i)\right)/n$.

Specifying finite fields numerically

For use in algorithms, an explicit model is supposed to be specified by the system of n^3 numbers $a_{ijk} \in \mathbf{F}_p = \{0, 1, \ldots, p-1\}$.

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

Specifying finite fields numerically

For use in algorithms, an explicit model is supposed to be specified by the system of n^3 numbers $a_{ijk} \in \mathbf{F}_p = \{0, 1, \ldots, p-1\}$.

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

A field homomorphism $\mathbf{F}_p^m \to \mathbf{F}_p^n$ between explicit models is supposed to be specified by an $n \times m$-matrix over $\mathbf{F}_p$.

Consistent isomorphisms between finite fields

Theorem. *There is, for some* $c \in \mathbf{R}_{>0}$*, an algorithm that on input* p*,* n*, and two explicit models* A*,* B *for fields of size* p^n*, computes in time at most* $(n + \log p)^c$ *a field isomorphism* $\phi_{A,B}\colon A \to B$*,*

Consistent isomorphisms between finite fields

Theorem. *There is, for some* $c \in \mathbf{R}_{>0}$, *an algorithm that on input* p, n, *and two explicit models* A, B *for fields of size* p^n, *computes in time at most* $(n + \log p)^c$ *a field isomorphism* $\phi_{A,B}\colon A \to B$, *and that has the property* $\phi_{A,C} = \phi_{B,C} \circ \phi_{A,B}$ *whenever* A, B, C *are explicit models for finite fields of the same size.*

Consistent isomorphisms between finite fields

Theorem. *There is, for some $c \in \mathbf{R}_{>0}$, an algorithm that on input p, n, and two explicit models A, B for fields of size p^n, computes in time at most $(n + \log p)^c$ a field isomorphism $\phi_{A,B}\colon A \to B$, and that has the property $\phi_{A,C} = \phi_{B,C} \circ \phi_{A,B}$ whenever A, B, C are explicit models for finite fields of the same size.*

One has $\phi_{A,A} = \mathrm{id}_A$ and $\phi_{B,A} = \phi_{A,B}^{-1}$.

Standard models

Of all $\left(\prod_{i=0}^{n-1}(p^n - p^i)\right)/n$ explicit models for a field of size p^n, one is called the *standard model*.

Standard models

Of all $\left(\prod_{i=0}^{n-1}(p^n - p^i)\right)/n$ explicit models for a field of size p^n, one is called the *standard model*.

The good algorithmic properties of the standard model are easier to explain than its definition.

Computing the standard model

Conjecture. *There is a polynomial-time algorithm that on input p and n computes the standard model for a field of size p^n.*

Computing the standard model

Conjecture. *There is a polynomial-time algorithm that on input p and n computes the standard model for a field of size p^n.*

This is valid if the generalized Riemann hypothesis is true; probabilistically; and for any fixed value of p.

Computing the standard model

Conjecture. *There is a polynomial-time algorithm that on input p and n computes the standard model for a field of size p^n.*

This is valid if the generalized Riemann hypothesis is true; probabilistically; and for any fixed value of p.

One proves these results by *standardizing explicit models.*

Standardizing explicit models

Theorem. *There is a polynomial-time algorithm that on input p, n, and an explicit model A for a field of size p^n, computes the standard model for a field of size p^n as well as an isomorphism ϕ_A of A with the standard model.*

Standardizing explicit models

Theorem. *There is a polynomial-time algorithm that on input p, n, and an explicit model A for a field of size p^n, computes the standard model for a field of size p^n as well as an isomorphism ϕ_A of A with the standard model.*

Thus, standard models do not contain "hidden information".

Consistent isomorphisms between finite fields

Theorem. *There is, for some* $c \in \mathbf{R}_{>0}$*, an algorithm that on input* p*,* n*, and two explicit models* A*,* B *for fields of size* p^n*, computes in time at most* $(n + \log p)^c$ *a field isomorphism* $\phi_{A,B} \colon A \to B$*, and that has the property* $\phi_{A,C} = \phi_{B,C} \circ \phi_{A,B}$ *whenever* A*,* B*,* C *are explicit models for finite fields of the same size.*

Proof. Take $\phi_{A,B} = \phi_B^{-1} \circ \phi_A$.

Compatibility between standard models

Let the basis vectors e_0, e_1, $\ldots$, e_{n-1} of the standard model of size p^n be renumbered as ϵ_0, $\epsilon_{1/n}$, $\ldots$, $\epsilon_{(n-1)/n}$.

Compatibility between standard models

Let the basis vectors e_0, e_1, . . . , e_{n-1} of the standard model of size p^n be renumbered as ϵ_0, $\epsilon_{1/n}$, . . . , $\epsilon_{(n-1)/n}$.

Then for each m dividing n, there is a field embedding of the standard model of size p^m into the standard model of size p^n that maps ϵ_s to ϵ_s for each $s \in \{0, 1/m, \ldots, (m-1)/m\}$.

The standard algebraic closure

Taking the union over n, one obtains the *standard algebraic closure* $\bar{\mathbf{F}}_p$ of $\mathbf{F}_p$, with $\mathbf{F}_p$-basis $(\epsilon_s)_{s\in\mathbf{Q}\cap[0,1)}$.

The standard algebraic closure

Taking the union over n, one obtains the *standard algebraic closure* $\bar{\mathbf{F}}_p$ of $\mathbf{F}_p$, with $\mathbf{F}_p$-basis $(\epsilon_s)_{s\in\mathbf{Q}\cap[0,1)}$.

For each

$$\alpha = \sum_{s\in\mathbf{Q}\cap[0,1)}^{<\infty} c_s\epsilon_s \in \bar{\mathbf{F}}_p \qquad (c_s \in \mathbf{F}_p),$$

the degree of α over $\mathbf{F}_p$ is the least common denominator of $\{s : c_s \neq 0\}$.

Defining the standard model

Each $\mathbf{F}_{p^n}$ can be written as the tensor product over $\mathbf{F}_p$ of fields $\mathbf{F}_{p^{r^k}}$, with r^k ranging over all prime powers exactly dividing n.

Defining the standard model

Each $\mathbf{F}_{p^n}$ can be written as the tensor product over $\mathbf{F}_p$ of fields $\mathbf{F}_{p^{r^k}}$, with r^k ranging over all prime powers exactly dividing n.

Hence we may restrict to the case $n = r^k$, with r prime and $k \in \mathbf{Z}_{>0}$.

Defining the standard model

To define the standard model for $\mathbf{F}_{p^n}$, one may restrict to the case $n = r^k$, with r prime and $k \in \mathbf{Z}_{>0}$.

For any two primes p and r, we shall define a tower of degree r extensions

$$\mathbf{F}_p \subset \mathbf{F}_{p^r} \subset \mathbf{F}_{p^{r^2}} \subset \dots .$$

Defining the standard model

To define the standard model for $\mathbf{F}_{p^n}$, one may restrict to the case $n = r^k$, with r prime and $k \in \mathbf{Z}_{>0}$.

For any two primes p and r, we shall define a tower of degree r extensions

$$\mathbf{F}_p \subset \mathbf{F}_{p^r} \subset \mathbf{F}_{p^{r^2}} \subset \dots .$$

Two cases: $r \neq p$ and $r = p$.

Towers of quadratic extensions

Theorem. *Let p be an odd prime, let $2^l \| (p^2-1)/8$, and let $\alpha_i \in \bar{\mathbf{F}}_p$ ($i = 0, 1, 2, \ldots$) satisfy*

$$\alpha_0 = 0, \quad \alpha_{i+1}^2 = 2 + \alpha_i \quad (i \geq 0).$$

Then $\alpha_0, \ldots, \alpha_l$ are in $\mathbf{F}_p$, and

$$[\mathbf{F}_p(\alpha_{l+k}) : \mathbf{F}_p] = 2^k \quad (k \geq 0).$$

Towers of quadratic extensions

Theorem. *Let p be an odd prime, let $2^l \| (p^2-1)/8$, and let $\alpha_i \in \bar{\mathbf{F}}_p$ ($i = 0, 1, 2, \ldots$) satisfy*

$$\alpha_0 = 0, \quad \alpha_{i+1}^2 = 2 + \alpha_i \quad (i \geq 0).$$

Then $\alpha_0, \ldots, \alpha_l$ are in $\mathbf{F}_p$, and

$$[\mathbf{F}_p(\alpha_{l+k}) : \mathbf{F}_p] = 2^k \quad (k \geq 0).$$

The proof makes use of

$$\alpha_i = \zeta_{2^{i+2}} + \zeta_{2^{i+2}}^{-1} \quad (i \geq 0).$$

The standard model for p odd, $n = 2^k$

Suppose in addition

$$\alpha_i \in \{0, 1, \ldots, (p-1)/2\}$$

for $0 \leq i \leq l$.

The standard model for p odd, $n = 2^k$

Suppose in addition

$$\alpha_i \in \{0, 1, \ldots, (p-1)/2\}$$

for $0 \le i \le l$.

Make $\mathbf{F}_p^{2^k} = \bigoplus_{i=0}^{2^k-1} \mathbf{F}_p \cdot \epsilon_{i/2^k}$ into a field by the vector space embedding $\mathbf{F}_p^{2^k} \to \bar{\mathbf{F}}_p$ that maps ϵ_s to $\prod_{j \in S} \alpha_{l+j}$ if $s = \sum_{j \in S} 2^{-j}$.

The standard model for p odd, $n = 2^k$

Suppose in addition

$$\alpha_i \in \{0, 1, \ldots, (p-1)/2\}$$

for $0 \leq i \leq l$.

Make $\mathbf{F}_p^{2^k} = \bigoplus_{i=0}^{2^k-1} \mathbf{F}_p \cdot \epsilon_{i/2^k}$ into a field by the vector space embedding $\mathbf{F}_p^{2^k} \to \bar{\mathbf{F}}_p$ that maps ϵ_s to $\prod_{j \in S} \alpha_{l+j}$ if $s = \sum_{j \in S} 2^{-j}$.

That is the standard model.

Example

For $p = 31$, $n = 4$ one finds $l = 3$,

$\alpha_0 = 0$, $\alpha_1 = 8$, $\alpha_2 = 14$, $\alpha_3 = 4$.

Example

For $p = 31$, $n = 4$ one finds $l = 3$,

$\alpha_0 = 0$, $\alpha_1 = 8$, $\alpha_2 = 14$, $\alpha_3 = 4$.

The field structure on

$\mathbf{F}_{31}^4 = \mathbf{F}_{31} \cdot \epsilon_0 \oplus \mathbf{F}_{31} \cdot \epsilon_{1/4} \oplus \mathbf{F}_{31} \cdot \epsilon_{1/2} \oplus \mathbf{F}_{31} \cdot \epsilon_{3/4}$

is determined by

$$\epsilon_0 = 1, \quad \epsilon_{1/2}^2 = 6 \quad (\text{since } \epsilon_{1/2} \mapsto \alpha_4),$$

$$\epsilon_{1/4}^2 = 2 + \epsilon_{1/2} \quad (\text{since } \epsilon_{1/4} \mapsto \alpha_5),$$

$$\epsilon_{1/4} \cdot \epsilon_{1/2} = \epsilon_{3/4}.$$

Standardizing explicit models

Theorem. *There is a polynomial-time algorithm that on input p, n, and an explicit model A for a field of size p^n, computes the standard model for a field of size p^n as well as an isomorphism ϕ_A of A with the standard model.*

Standardizing quadratic towers

Let A be an explicit model for a field of size p^n, with p odd and $n = 2^k$, $k > 0$.

Standardizing quadratic towers

Let A be an explicit model for a field of size p^n, with p odd and $n = 2^k$, $k > 0$.

Using linear algebra one can find $x \in A$ with $x^p = -x$ and $x \neq 0$. Then x^2 is a non-square in $\mathbf{F}_p$, which can be used to solve quadratic equations in A.

Standardizing quadratic towers

Using linear algebra one can find $x \in A$ with $x^p = -x$ and $x \neq 0$. Then x^2 is a non-square in $\mathbf{F}_p$, which can be used to solve quadratic equations in A.

Hence one can find $\alpha_i \in A$ for $i \leq l + k$ with $\alpha_0 = 0$, $\alpha_{i+1}^2 = 2 + \alpha_i$ $(i \geq 0)$, $\alpha_i \in \{0, 1, \ldots, (p-1)/2\}$ $(0 \leq i \leq l)$ and identify the standard model with A.

Towers of cubic extensions

For $n = 3^k$, $p \neq 3$, one can proceed similarly, replacing

$$2^l \| (p^2 - 1)/8,$$

$$\alpha_0 = 0, \quad \alpha_{i+1}^2 = 2 + \alpha_i$$

by

$$3^l \| (p^2 - 1)/3,$$

$$\alpha_0 = -1, \quad \alpha_{i+1}^3 = 3\alpha_{i+1} + \alpha_i.$$

One has $\alpha_i = \zeta_{3^{i+1}} + \zeta_{3^{i+1}}^{-1} \quad (i \geq 0)$.

Towers of degree r extensions

For $n = r^k$, $r \geq 5$ prime, and $p \neq r$, one uses $r^l \| (p^{r-1} - 1)/r$, and each α_i is replaced by a system of suitably chosen Gaussian periods.

Roots of unity

Let r be prime, and let the ring

$A = \mathbf{Z}[\zeta_r, \zeta_{r^2}, \ldots]$ be defined

by the relations

$\sum_{i=0}^{r-1} \zeta_r^i = 0, \quad \zeta_{r^{i+1}}^r = \zeta_{r^i} \quad (i \geq 0).$

Roots of unity

Let r be prime, and let the ring

$A = \mathbf{Z}[\zeta_r, \zeta_{r^2}, \ldots]$ be defined

by the relations

$\sum_{i=0}^{r-1} \zeta_r^i = 0, \quad \zeta_{r^{i+1}}^r = \zeta_{r^i} \quad (i \geq 0).$

Then $\mathrm{Aut}\, A \cong \mathbf{Z}_r^* = \Delta \times \Gamma$, with

Δ cyclic of order $\mathrm{lcm}(2, r-1)$ and

$\Gamma = 1 + 2r\mathbf{Z}_r \cong \mathbf{Z}_r$.

An extension with group $\mathbf{Z}_r$

Put $B = A^{\Delta} = \{x \in A : \forall\sigma \in \Delta : \sigma x = x\}$.

One has $\mathrm{Aut}\, B \cong \Gamma \cong \mathbf{Z}_r$, and there are subrings

$$\mathbf{Z} = B_0 \subset B_1 \subset \ldots \subset \bigcup_{i\geq 0} B_i = B$$

with $[B_{i+1} : B_i] = r \quad (i \geq 0)$.

An extension with group $\mathbf{Z}_r$

Put $B = A^{\Delta} = \{x \in A : \forall \sigma \in \Delta : \sigma x = x\}$.

One has $\mathrm{Aut}\, B \cong \Gamma \cong \mathbf{Z}_r$, and there are subrings

$$\mathbf{Z} = B_0 \subset B_1 \subset \ldots \subset \bigcup_{i \geq 0} B_i = B$$

with $[B_{i+1} : B_i] = r \quad (i \geq 0)$.

For $r = 2$ one has $B_i = \mathbf{Z}[\zeta_{2^{i+2}} + \zeta_{2^{i+2}}^{-1}]$,
and for $r = 3$ one has $B_i = \mathbf{Z}[\zeta_{3^{i+1}} + \zeta_{3^{i+1}}^{-1}]$.

For $r \geq 5$, the rings B_i are harder to describe.

Reducing modulo p

Theorem. *Let $p \neq r$ be primes, and let r^l be the largest power of r dividing $(p^{r-1}-1)/r$ if $r>2$ and $(p^2-1)/8$ if $r=2$. Then the number of prime ideals $\mathfrak{p} \subset B_l$ with $p \in \mathfrak{p}$ equals r^l. Also, for any such $\mathfrak{p}$ and any $k \geq 0$ the ring $B_{l+k} \otimes_{B_l} (B_l/\mathfrak{p})$ is a field of degree r^k over $\mathbf{F}_p$.*

Standard models for $n = r^k$, $p \neq r$

Normalizing the choice of $\mathfrak{p}$, and choosing explicit generators for the ring extensions

$$B_l \subset B_{l+1} \subset B_{l+2} \subset \dots$$

(locally at $\mathfrak{p}$), one obtains the standard models for finite fields of degree a power of r and characteristic $p \neq r$.

Standard models for $n = r^k$, $p \neq r$

Normalizing the choice of $\mathfrak{p}$, and choosing explicit generators for the ring extensions

$$B_l \subset B_{l+1} \subset B_{l+2} \subset \dots$$

(locally at $\mathfrak{p}$), one obtains the standard models for finite fields of degree a power of r and characteristic $p \neq r$.

The good algorithmic properties of these standard models are due to the connection with roots of unity.

The standard model for $n = p^k$

Theorem. *Let* p *be an odd prime, and let* $\alpha_i \in \bar{\mathbf{F}}_p$ *(*$i = 0, 1, 2, \ldots$*) satisfy*

$$\alpha_0 = 1,$$

$$\alpha_{i+1}^p = 1 + \alpha_i \cdot \textstyle\sum_{j=1}^{p-1} \alpha_{i+1}^j \quad (i \geq 0).$$

Then for all $k \geq 0$ *one has*

$$[\mathbf{F}_p(\alpha_k) : \mathbf{F}_p] = p^k.$$

The standard model for $n = p^k$

Theorem. *Let p be an odd prime, and let $\alpha_i \in \bar{\mathbf{F}}_p$ $(i = 0, 1, 2, \ldots)$ satisfy*

$$\alpha_0 = 1,$$

$$\alpha_{i+1}^p = 1 + \alpha_i \cdot \textstyle\sum_{j=1}^{p-1} \alpha_{i+1}^j \quad (i \geq 0).$$

Then for all $k \geq 0$ one has

$$[\mathbf{F}_p(\alpha_k) : \mathbf{F}_p] = p^k.$$

Proof. Use the Artin-Schreier equations

$$(\alpha_{i+1} - 1)^{-p} - (\alpha_{i+1} - 1)^{-1} + \alpha_i^{-1} = 0.$$

Practical applications

Standard models have potential applications in computer algebra.

Currently used standardizations in computational group theory depend on *Conway polynomials*. These have proven to be computationally completely intractable.

Announcement

Diamant Intercity Seminar

Standard models of finite fields

September 26, 2008

Radboud Universiteit Nijmegen

Speakers:

Wieb Bosma, Bart de Smit,

Hendrik Lenstra, Frank Lübeck

http://www.math.leidenuniv.nl/
~desmit/ic/current.html