On sharply k-transitive Galois extensions

M. Ángeles Gómez and Joan-C. Lario

STNB (UB-UAB-UPC)
January 2007

Minimal sets of roots

Given $f \in \mathbb{Q}[x]$ irreducible, and $\Omega = \{\alpha_1, \ldots, \alpha_n\}$ roots in $\overline{\mathbb{Q}}$,

Minimal sets of roots

Given $f \in \mathbb{Q}[x]$ irreducible, and $\Omega = \{\alpha_1, \ldots, \alpha_n\}$ roots in $\overline{\mathbb{Q}}$,

- find minimal $\{\alpha_{i_1}, \ldots, \alpha_{i_k}\}$ with $\mathbb{Q}_f = \mathbb{Q}(\alpha_{i_1}, \ldots, \alpha_{i_k})$;

Minimal sets of roots

Given $f \in \mathbb{Q}[x]$ irreducible, and $\Omega = \{\alpha_1, \ldots, \alpha_n\}$ roots in $\overline{\mathbb{Q}}$,

- find minimal $\{\alpha_{i_1}, \ldots, \alpha_{i_k}\}$ with $\mathbb{Q}_f = \mathbb{Q}(\alpha_{i_1}, \ldots, \alpha_{i_k})$;
- express all the roots in terms of a minimal set:

Minimal sets of roots

Given $f \in \mathbb{Q}[x]$ irreducible, and $\Omega = \{\alpha_1, \ldots, \alpha_n\}$ roots in $\overline{\mathbb{Q}}$,

- find minimal $\{\alpha_{i_1}, \ldots, \alpha_{i_k}\}$ with $\mathbb{Q}_f = \mathbb{Q}(\alpha_{i_1}, \ldots, \alpha_{i_k})$;
- express all the roots in terms of a minimal set:

$$F_1, \ldots, F_n \in \mathbb{Q}[x_1, \ldots, x_k] \text{ with } \alpha_s = F_s(\alpha_{i_1}, \ldots, \alpha_{i_k})$$

A theorem of Galois

Theorem

Assume $\deg(f) = p$ *is prime. Then,* $\mathrm{Gal}(f)$ *is solvable if and only if* $\mathbb{Q}_f = \mathbb{Q}(\alpha, \beta)$ *for every couple of roots of* f*.*

A theorem of Galois

Theorem

Assume $\deg(f) = p$ *is prime. Then,* $\mathrm{Gal}(f)$ *is solvable if and only if* $\mathbb{Q}_f = \mathbb{Q}(\alpha, \beta)$ *for every couple of roots of* f*.*

If $\alpha_1, \ldots, \alpha_p$ are the roots, then there exist polynomials

$$F_1, \ldots, F_p \in \mathbb{Q}[x, y] \text{ such that } \alpha_i = F_i(\alpha, \beta)$$

A theorem of Galois

Theorem

Assume $\deg(f) = p$ *is prime. Then,* $\mathrm{Gal}(f)$ *is solvable if and only if* $\mathbb{Q}_f = \mathbb{Q}(\alpha, \beta)$ *for every couple of roots of* f*.*

If $\alpha_1, \ldots, \alpha_p$ are the roots, then there exist polynomials

$$F_1, \ldots, F_p \in \mathbb{Q}[x, y] \text{ such that } \alpha_i = F_i(\alpha, \beta)$$

Explicit procedure to construct $F_1, \ldots, F_p$?

A theorem of Galois

Theorem

Assume $\deg(f) = p$ *is prime. Then,* $\mathrm{Gal}(f)$ *is solvable if and only if* $\mathbb{Q}_f = \mathbb{Q}(\alpha, \beta)$ *for every couple of roots of* f*.*

If $\alpha_1, \ldots, \alpha_p$ are the roots, then there exist polynomials

$$F_1, \ldots, F_p \in \mathbb{Q}[x, y] \text{ such that } \alpha_i = F_i(\alpha, \beta)$$

Explicit procedure to construct $F_1, \ldots, F_p$?

In this talk, we will focus on $\mathrm{Gal}(f)$ being sharply k-transitive.

Terminology

Let X be a nonempty set. A permutation group on X is a subgroup $G \subseteq \mathrm{Sym}(X)$. The degree of G is $|X|$.

Terminology

Let X be a nonempty set. A permutation group on X is a subgroup $G \subseteq \mathrm{Sym}(X)$. The degree of G is $|X|$.

$$\begin{array}{ccc} \mathrm{Sym}(X) & \xrightarrow{\imath^{-1}\varphi\imath} & \mathrm{Sym}(Y) \\ \uparrow & & \uparrow \\ G & \xrightarrow{\varphi} & H \end{array}$$

Terminology

Let X be a nonempty set. A permutation group on X is a subgroup $G \subseteq \mathrm{Sym}(X)$. The degree of G is $|X|$.

$$\begin{array}{ccc} \mathrm{Sym}(X) & \xrightarrow{\imath^{-1}\varphi\imath} & \mathrm{Sym}(Y) \\ \uparrow & & \uparrow \\ G & \xrightarrow{\varphi} & H \end{array}$$

G is k-transitive if for every pair of k-tuples $(x_1, \ldots, x_k)$ and $(z_1, \ldots, z_k)$ of elements of X there is $g \in G$ with $g(x_i) = z_i$.

Terminology

Let X be a nonempty set. A permutation group on X is a subgroup $G \subseteq \mathrm{Sym}(X)$. The degree of G is $|X|$.

$$\begin{array}{ccc} \mathrm{Sym}(X) & \xrightarrow{\imath^{-1}\varphi\imath} & \mathrm{Sym}(Y) \\ \uparrow & & \uparrow \\ G & \xrightarrow{\varphi} & H \end{array}$$

G is k-transitive if for every pair of k-tuples $(x_1, \ldots, x_k)$ and $(z_1, \ldots, z_k)$ of elements of X there is $g \in G$ with $g(x_i) = z_i$.

G is sharply k-transitive if the above g is unique.

Classification results

For $k \geq 2$, the classification of finite sharply k-transitive groups (up to similarity) was accomplished by:

Classification results

For $k \geq 2$, the classification of finite sharply k-transitive groups (up to similarity) was accomplished by:

- Jordan, 1873

Classification results

For $k \geq 2$, the classification of finite sharply k-transitive groups (up to similarity) was accomplished by:

- Jordan, 1873
- Dickson, 1905

Classification results

For $k \geq 2$, the classification of finite sharply k-transitive groups (up to similarity) was accomplished by:

- Jordan, 1873
- Dickson, 1905
- Zassenhaus, 1936

Theorem

Let G be a finite sharply k-transitive permutation group that is neither $\mathcal{S}_n$ or $\mathcal{A}_n$. Then,

- *necessaraly one has $k \leq 5$;*

Theorem

Let G be a finite sharply k-transitive permutation group that is neither $\mathcal{S}_n$ or $\mathcal{A}_n$. Then,

- *necessaraly one has $k \leq 5$;*
- *if $k = 5$, then G is similar to the Mathieu group M_{12};*

Theorem

Let G be a finite sharply k-transitive permutation group that is neither $\mathcal{S}_n$ or $\mathcal{A}_n$. Then,

- *necessaraly one has $k \leq 5$;*
- *if $k = 5$, then G is similar to the Mathieu group M_{12};*
- *if $k = 4$, then G is similar to the Mathieu group M_{11};*

Theorem

Let G be a finite sharply k-transitive permutation group that is neither $\mathcal{S}_n$ or $\mathcal{A}_n$. Then,

- *necessaraly one has $k \leq 5$;*
- *if $k = 5$, then G is similar to the Mathieu group M_{12};*
- *if $k = 4$, then G is similar to the Mathieu group M_{11};*
- *if $k = 3$, then G is similar to $\mathrm{PGL}_2(\mathbb{F}_q)$ or $\mathrm{PGL}_2(\mathbb{F}_q)^{\mathrm{twist}}$;*

Theorem

Let G be a finite sharply k-transitive permutation group that is neither $\mathcal{S}_n$ or $\mathcal{A}_n$. Then,

- *necessaraly one has $k \leq 5$;*
- *if $k = 5$, then G is similar to the Mathieu group M_{12};*
- *if $k = 4$, then G is similar to the Mathieu group M_{11};*
- *if $k = 3$, then G is similar to $\mathrm{PGL}_2(\mathbb{F}_q)$ or $\mathrm{PGL}_2(\mathbb{F}_q)^{\mathrm{twist}}$;*
- *if $k = 2$, then G is similar to $\mathbb{A}^1(\mathcal{F})$, where $\mathcal{F}$ is a nearfield.*

Nearfields

$\mathcal{F} = (\mathbb{F}, +, \circ)$ satisfies field axioms except one of distributive laws fails.

$$(x + y) \circ z \sim x \circ z + y \circ z$$

Nearfields

$\mathcal{F} = (\mathbb{F}, +, \circ)$ satisfies field axioms except one of distributive laws fails.

$$(x + y) \circ z \sim x \circ z + y \circ z$$

Finite nearfields are well understood:

Nearfields

$\mathcal{F} = (\mathbb{F}, +, \circ)$ satisfies field axioms except one of distributive laws fails.

$$(x + y) \circ z \sim x \circ z + y \circ z$$

Finite nearfields are well understood:

Dickson nearfields + seven exotic nearfields.

Dickson nearfields $\mathcal{F} = (\mathbb{F}, +, \circ)$

Dickson pair (q, n):

Dickson nearfields $\mathcal{F} = (\mathbb{F}, +, \circ)$

Dickson pair (q, n):
$q = p^\nu$ prime power and $n \in \mathbb{N}$ such that
for $\ell = 4$ or ℓ prime, $\ell \mid n$ implies $\ell \mid q - 1$.

Dickson nearfields $\mathcal{F} = (\mathbb{F}, +, \circ)$

Dickson pair (q, n):
$q = p^\nu$ prime power and $n \in \mathbb{N}$ such that
for $\ell = 4$ or ℓ prime, $\ell \mid n$ implies $\ell \mid q - 1$.

Let ω be a generator of the cyclic group $\mathbb{F}_{q^n}^*$, and $H =< \omega^n >$.

Dickson nearfields $\mathcal{F} = (\mathbb{F}, +, \circ)$

Dickson pair (q, n):
$q = p^\nu$ prime power and $n \in \mathbb{N}$ such that
for $\ell = 4$ or ℓ prime, $\ell \mid n$ implies $\ell \mid q - 1$.

Let ω be a generator of the cyclic group $\mathbb{F}_{q^n}^*$, and $H =< \omega^n >$.

$$\mathbb{F}_{q^n}^* = \bigcup_{i=1}^{n} H\,\omega^{(q^i-1)/(q-1)}\,.$$

Dickson nearfields $\mathcal{F} = (\mathbb{F}, +, \circ)$

Dickson pair (q, n):
$q = p^\nu$ prime power and $n \in \mathbb{N}$ such that
for $\ell = 4$ or ℓ prime, $\ell \mid n$ implies $\ell \mid q - 1$.

Let ω be a generator of the cyclic group $\mathbb{F}_{q^n}^*$, and $H =< \omega^n >$.

$$\mathbb{F}_{q^n}^* = \bigcup_{i=1}^{n} H\,\omega^{(q^i-1)/(q-1)}\,.$$

For $x \in H\,\omega^{(q^i-1)/(q-1)}$, one has $x \circ y = x \cdot y^{q^i}$.

Dickson nearfields $\mathcal{F} = (\mathbb{F}, +, \circ)$

Dickson pair (q, n):
$q = p^\nu$ prime power and $n \in \mathbb{N}$ such that
for $\ell = 4$ or ℓ prime, $\ell \mid n$ implies $\ell \mid q - 1$.

Let ω be a generator of the cyclic group $\mathbb{F}_{q^n}^*$, and $H =< \omega^n >$.

$$\mathbb{F}_{q^n}^* = \bigcup_{i=1}^{n} H\,\omega^{(q^i-1)/(q-1)}\,.$$

For $x \in H\,\omega^{(q^i-1)/(q-1)}$, one has $x \circ y = x \cdot y^{q^i}$.

$n = 1$ ordinary case $(\mathbb{F}_q, +, \cdot)$; $n > 1$ twisted case $\mathcal{F} = (\mathbb{F}_{q^n}, +, \circ)$.

The ideal I_k

Given $f \in \mathbb{Z}[x]$ irreducible, and $\Omega = \{\alpha_1, \ldots, \alpha_n\}$ roots in $\overline{\mathbb{Q}}$:
When $\mathrm{Gal}(f)$ is sharply k-transitive on Ω?

The ideal I_k

Given $f \in \mathbb{Z}[x]$ irreducible, and $\Omega = \{\alpha_1, \ldots, \alpha_n\}$ roots in $\overline{\mathbb{Q}}$:
When $\mathrm{Gal}(f)$ is sharply k-transitive on Ω?
For $k \geq 1$, consider the ideal

$$I_k = (f_1(x_1), f_2(x_1, x_2), \ldots, f_k(x_1, x_2, \ldots, x_k)) \subset \mathbb{Q}[x_1, \ldots, x_k]$$

according to the recurrence:

$$\begin{aligned} f_1(x_1) &= f(x_1), \\ f_2(x_1, x_2) &= (f(x_2) - f(x_1))/(x_2 - x_1), \\ f_i(x_1, \ldots, x_i) &= (f_{i-1}(x_1, \ldots, x_{i-2}, x_i) - f_{i-1}(x_1, \ldots, x_{i-2}, x_{i-1}))/(x_i - x_{i-1}). \end{aligned}$$

The ideal I_k

Given $f \in \mathbb{Z}[x]$ irreducible, and $\Omega = \{\alpha_1, \ldots, \alpha_n\}$ roots in $\overline{\mathbb{Q}}$:
When $\mathrm{Gal}(f)$ is sharply k-transitive on Ω?
For $k \geq 1$, consider the ideal

$$I_k = (f_1(x_1), f_2(x_1, x_2), \ldots, f_k(x_1, x_2, \ldots, x_k)) \subset \mathbb{Q}[x_1, \ldots, x_k]$$

according to the recurrence:

$$\begin{aligned} f_1(x_1) &= f(x_1), \\ f_2(x_1, x_2) &= (f(x_2) - f(x_1))/(x_2 - x_1), \\ f_i(x_1, \ldots, x_i) &= (f_{i-1}(x_1, \ldots, x_{i-2}, x_i) - f_{i-1}(x_1, \ldots, x_{i-2}, x_{i-1}))/(x_i - x_{i-1}). \end{aligned}$$

The $\{f_i\}$ form a Gröbner basis for I_k wrt: $x_k > \cdots > x_2 > x_1$.

A criterium

Theorem

Let $k \geq 1$. The Galois group $\mathrm{Gal}(f)$ is sharply k-transitive if and only if there is a "unique" family of polynomials

$$F_1, \ldots, F_n \in \mathbb{Q}[x_1, \ldots, x_k]$$

with

$$\Omega = \{F_i(\beta)\}_{i=1}^{n}$$

for every $\beta = (\beta_1, \ldots, \beta_k)$ proper k-tuple of roots of f.

"unique": modulo the ideal I_k.

Assume $\mathrm{Gal}(f)$ sharply k-transitive with $k \geq 1$.

Assume $\mathrm{Gal}(f)$ sharply k-transitive with $k \geq 1$.
Fix $\alpha = (\alpha_1, \ldots, \alpha_k)$ a k-tuple of roots of f.

Assume $\mathrm{Gal}(f)$ sharply k-transitive with $k \geq 1$.
Fix $\alpha = (\alpha_1, \ldots, \alpha_k)$ a k-tuple of roots of f.
By using the interpolating polynomials

$$\Gamma_i(x_1, ..., x_k) = \sum_{\sigma \in \mathrm{Gal}(f)} \sigma(\alpha_i) \frac{f(x_1)}{x_1 - \sigma(\alpha_1)} \frac{f(x_2)}{x_2 - \sigma(\alpha_2)} \cdots \frac{f(x_k)}{x_k - \sigma(\alpha_k)}$$

Assume $\mathrm{Gal}(f)$ sharply k-transitive with $k \geq 1$.
Fix $\alpha = (\alpha_1, \ldots, \alpha_k)$ a k-tuple of roots of f.
By using the interpolating polynomials

$$\Gamma_i(x_1, ..., x_k) = \sum_{\sigma \in \mathrm{Gal}(f)} \sigma(\alpha_i) \frac{f(x_1)}{x_1 - \sigma(\alpha_1)} \frac{f(x_2)}{x_2 - \sigma(\alpha_2)} \cdots \frac{f(x_k)}{x_k - \sigma(\alpha_k)}$$

Proposition

Let $h(x)$ and $r(x) \in \mathbb{Q}[x]$ such that $r(x)f(x) + h(x)f'(x) = 1$.
Then, the polynomials F_i can be chosen as

$$F_i(x_1, \ldots, x_k) = h(x_1) \cdots h(x_k)\, \Gamma_i(x_1, \ldots, x_k)\,.$$

ℓ-adic strategy

- Step 1. Bound the coefficients of $F_i \in \mathbb{Q}[x_1, \ldots, x_k]$

ℓ-adic strategy

- Step 1. Bound the coefficients of $F_i \in \mathbb{Q}[x_1, \ldots, x_k]$
- Step 2. Build ℓ-adic liftings from $\tilde{F}_i$ mod ℓ

ℓ-adic strategy

- Step 1. Bound the coefficients of $F_i \in \mathbb{Q}[x_1, \ldots, x_k]$
- Step 2. Build ℓ-adic liftings from $\tilde{F}_i$ mod ℓ
- Step 3. Find $\tilde{F}_i$ mod ℓ

ℓ-adic strategy

- Step 1. Bound the coefficients of $F_i \in \mathbb{Q}[x_1, \ldots, x_k]$
- Step 2. Build ℓ-adic liftings from $\tilde{F}_i$ mod ℓ
- Step 3. Find $\tilde{F}_i$ mod ℓ
- Step 4. Reconstruct $F_i \in \mathbb{Q}[x_1, \ldots, x_k]$ (standard techniques)

Bounding the remainder

Theorem

If $\mathrm{Gal}(f)$ is sharply k-transitive, then there is a unique family $F_1, \ldots, F_n$ supplying all the roots of f with

$$F_i(x_1, \ldots, x_k) = \frac{1}{\delta(f)^k} \sum_{0 \le i_k < \cdots < i_1 < n} a_{i_1, \ldots, i_k} x_1^{i_1} \ldots x_k^{i_k},$$

where $a_{i_1, \ldots, i_k} \in \mathbb{Z}$ and $|a_{i_1, \ldots, i_k}| \le C(h)^k C(\Gamma_i) \prod_{j=1}^{k} (1 + M_j)^{n-2+j}$.

Bounding the remainder

Theorem

If $\mathrm{Gal}(f)$ is sharply k-transitive, then there is a unique family $F_1, \ldots, F_n$ supplying all the roots of f with

$$F_i(x_1, \ldots, x_k) = \frac{1}{\delta(f)^k} \sum_{0 \le i_k < \cdots < i_1 < n} a_{i_1, \ldots, i_k} x_1^{i_1} \ldots x_k^{i_k},$$

where $a_{i_1,\ldots,i_k} \in \mathbb{Z}$ and $|a_{i_1,\ldots,i_k}| \le C(h)^k C(\Gamma_i) \prod_{j=1}^{k} (1 + M_j)^{n-2+j}$.

$C(h) := \max\{\text{coeffs}(h)\}$, $C(\Gamma_i) := |\mathrm{Gal}(f)|\, C(f)^{1+(n-1)k} \binom{n}{\lceil n/2 \rceil}^k$
$C(f) := \max\{|\alpha_i|\}$, $M_i := \max\{|\text{coeffs}(f_i)|\}$, $(\delta_f) \subseteq (f, f') \subseteq \mathbb{Z}[x]$

ℓ-adic liftings

Set $\gamma = (n-1, n-2, \ldots, n-k+1)$. For $H \in \mathbb{Q}[x_1, \ldots, x_k]$, let $\deg(H) < \gamma$ denote $\deg_{x_j}(H) \leq n-j$.

ℓ-adic liftings

Set $\gamma = (n-1, n-2, \ldots, n-k+1)$. For $H \in \mathbb{Q}[x_1, \ldots, x_k]$, let $\deg(H) < \gamma$ denote $\deg_{x_j}(H) \leq n-j$.
Also set $\mathbf{x} = (x_1, \ldots, x_k)$ and $I_k \otimes A := (f_1, \ldots, f_k)A[\mathbf{x}]$.

ℓ-adic liftings

Set $\gamma = (n-1, n-2, \ldots, n-k+1)$. For $H \in \mathbb{Q}[x_1, \ldots, x_k]$, let $\deg(H) < \gamma$ denote $\deg_{x_j}(H) \leq n-j$.
Also set $\mathbf{x} = (x_1, \ldots, x_k)$ and $I_k \otimes A := (f_1, \ldots, f_k)A[\mathbf{x}]$.

Proposition

Assume that $H_0 \in \mathbb{Z}[\mathbf{x}]$ *has* $\deg(H_0) < \gamma$ *and satisfies*

$$f(H_0(\mathbf{x})) \equiv 0 \bmod I_k \otimes \mathbb{F}_\ell\,.$$

Then, there exists a unique $H \in \mathbb{Z}_\ell[\mathbf{x}]$ *such that*

(i) $\deg(H) < \gamma$;

(ii) $H(\mathbf{x}) \equiv H_0(\mathbf{x}) \bmod \ell\,\mathbb{Z}[\mathbf{x}]$;

(iii) $f(H(\mathbf{x})) \equiv 0 \bmod I_k \otimes \mathbb{Z}_\ell$.

Sketch of proof

The following is a Cauchy sequence in the ℓ-adic metric:

$$\{H_i(\mathbf{x})\}_{i\geq 0}$$

where H_i is the remainder of the polynomial division of

$$H_{i-1}(\mathbf{x}) - h_{i-1}(H_{i-1}(\mathbf{x}))f(H_{i-1}(\mathbf{x}))$$

by the Gröbner basis $\{f_1(x_1), f_2(x_1, x_2), \ldots, f_k(x_1, \ldots, x_k)\}$. Here, $h_i \in \mathbb{Z}[x]$ such that $h_i(x)f'(x) \equiv 1 \bmod (l^{2^i}, f(x))\mathbb{Z}[x]$.

Sketch of proof

The following is a Cauchy sequence in the ℓ-adic metric:

$$\{H_i(\mathbf{x})\}_{i\geq 0}$$

where H_i is the remainder of the polynomial division of

$$H_{i-1}(\mathbf{x}) - h_{i-1}(H_{i-1}(\mathbf{x}))f(H_{i-1}(\mathbf{x}))$$

by the Gröbner basis $\{f_1(x_1), f_2(x_1, x_2), \ldots, f_k(x_1, \ldots, x_k)\}$. Here, $h_i \in \mathbb{Z}[x]$ such that $h_i(x)f'(x) \equiv 1 \bmod (l^{2^i}, f(x))\mathbb{Z}[x]$.One checks

(i) $\deg(H_i) < \gamma$;

(ii) $f(H_i(\mathbf{x})) \equiv 0 \bmod (l^{2^i}, f_1, \ldots, f_k)\,\mathbb{Z}[\mathbf{x}]$;

(iii) $H_i(\mathbf{x}) \equiv H_{i-1}(\mathbf{x}) \bmod l^{2^{i-1}}\,\mathbb{Z}[\mathbf{x}]$.

So far

$\mathrm{Gal}(f)$ is sharply k-transitive on $\Omega = \{\alpha_1, \ldots, \alpha_n\}$.

So far

$\mathrm{Gal}(f)$ is sharply k-transitive on $\Omega = \{\alpha_1, \ldots, \alpha_n\}$.

There are $F_1, \ldots, F_n \in \mathbb{Q}[x_1, \ldots, x_k]$ with $\alpha_i = F_i(\beta_1, \ldots, \beta_k)$.

So far

$\mathrm{Gal}(f)$ is sharply k-transitive on $\Omega = \{\alpha_1, \ldots, \alpha_n\}$.

There are $F_1, \ldots, F_n \in \mathbb{Q}[x_1, \ldots, x_k]$ with $\alpha_i = F_i(\beta_1, \ldots, \beta_k)$.

If we know the reduction $\tilde{F}_i \in \mathbb{F}_\ell[x_1, \ldots, x_k]$, we can compute $F_i \in \mathbb{Q}_\ell[x_1, \ldots, x_k]$ up to an arbitrary high accuracy.

So far

$\mathrm{Gal}(f)$ is sharply k-transitive on $\Omega = \{\alpha_1, \ldots, \alpha_n\}$.

There are $F_1, \ldots, F_n \in \mathbb{Q}[x_1, \ldots, x_k]$ with $\alpha_i = F_i(\beta_1, \ldots, \beta_k)$.

If we know the reduction $\tilde{F}_i \in \mathbb{F}_\ell[x_1, \ldots, x_k]$, we can compute $F_i \in \mathbb{Q}_\ell[x_1, \ldots, x_k]$ up to an arbitrary high accuracy.

Since we have a bound for the coefficients of $F_i \in \mathbb{Q}[x_1, \ldots, x_k]$, we can reconstruct the F_i.

So far

$\mathrm{Gal}(f)$ is sharply k-transitive on $\Omega = \{\alpha_1, \ldots, \alpha_n\}$.

There are $F_1, \ldots, F_n \in \mathbb{Q}[x_1, \ldots, x_k]$ with $\alpha_i = F_i(\beta_1, \ldots, \beta_k)$.

If we know the reduction $\tilde{F}_i \in \mathbb{F}_\ell[x_1, \ldots, x_k]$, we can compute $F_i \in \mathbb{Q}_\ell[x_1, \ldots, x_k]$ up to an arbitrary high accuracy.

Since we have a bound for the coefficients of $F_i \in \mathbb{Q}[x_1, \ldots, x_k]$, we can reconstruct the F_i.

It remains to compute the reduction $\tilde{F}_i \in \mathbb{F}_\ell[x_1, \ldots, x_k]$

$k \geq 2$: Admissible bijections

There is a bijection $\imath\colon X \to \Omega$ and an isomorphism φ rending the diagram

$$\begin{array}{ccc} \mathrm{Sym}(X) & \xrightarrow{\varphi_\imath} & \mathrm{Sym}(\Omega) \\ \uparrow & & \uparrow \\ G & \xrightarrow{\varphi} & \mathrm{Gal}(f) \end{array}$$

commutative, where $\varphi_\imath(\sigma) = \imath\sigma\imath^{-1}$ for $\sigma \in \mathrm{Sym}(X)$.

$k \geq 2$: Admissible bijections

There is a bijection $\imath\colon X \to \Omega$ and an isomorphism φ rending the diagram

$$\begin{array}{ccc} \mathsf{Sym}(X) & \xrightarrow{\varphi_\imath} & \mathsf{Sym}(\Omega) \\ \uparrow & & \uparrow \\ G & \xrightarrow{\varphi} & \mathrm{Gal}(f) \end{array}$$

commutative, where $\varphi_\imath(\sigma) = \imath\sigma\imath^{-1}$ for $\sigma \in \mathsf{Sym}(X)$.

$$\varphi_\imath(G) = \varphi_{\imath'}(G) \text{ iff } \imath^{-1}\imath' \in N_{\mathsf{Sym}(X)}(G).$$

Admissible bijections: $\varphi_\imath(G) = \mathrm{Gal}(f)$.

Strategy

Denote $X = \{\xi_1, \ldots, \xi_k, \xi_{k+1}, \ldots, \xi_n\}$. For $k+1 \leq j \leq n$,

$$\mathcal{G}_j(x_1, \ldots, x_k) = \sum_{g \in G} a[g(\xi_j)] \frac{\prod_{\xi \in X}(x_1 - a[\xi])}{x_1 - a[g(\xi_1)]} \cdots \frac{\prod_{\xi \in X}(x_k - a[\xi])}{x_k - a[g(\xi_k)]},$$

with coefficients in $\mathbb{Z}$, variables $a[\xi_i]'s$ and $x_1, \ldots, x_k$.
An admissible bijection $\imath$ transforms $\mathcal{G}_j$ into

$$\Gamma_j(x_1, \ldots, x_k) = \sum_{\sigma \in \mathrm{Gal}(f)} \sigma(\gamma_j) \frac{f(x_1)}{x_1 - \sigma(\gamma_1)} \cdots \frac{f(x_k)}{x_k - \sigma(\gamma_k)},$$

where $\gamma_s = \imath(\xi_s)$, and $F_j(x_1, ..., x_k) = h(x_1) \ldots h(x_k)\Gamma_j(x_1, ..., x_k)$ satisfies $\gamma_j = F_j(\gamma_1, ..., \gamma_k)$.

Fix a Fröbenius automorphism, call it τ

Let $\mathfrak{L}|\ell$ be a prime ideal of $\mathbb{Q}_f$ with $\ell \nmid \Delta(f)$.
To the factorization

$$f(x) \equiv \varphi_1(x) \dots \varphi_r(x) \bmod \ell$$

corresponds a Fröbenius automorphism $\tau \in \mathrm{Gal}(f)$ such that

$$\tau = (\alpha_{11}, \dots, \alpha_{1\,\deg\varphi_1}) \dots (\alpha_{r1}, \dots, \alpha_{r\,\deg\varphi_r}) \in \mathrm{Sym}(\Omega)$$

with $\alpha_{i\,t+1} \equiv \alpha_{i1}^{\ell^t} \bmod \mathfrak{L}$, for $0 \le t < \deg(\varphi_i)$ and $1 \le i \le r$.

$$[\tau] := \text{cycle type of } \tau = [\deg\varphi_1, \dots, \deg\varphi_r]\,.$$

Admissible bijections adapted to τ

Let $\mathcal{I}_\tau = \{\text{ bijections } \imath : X \to \Omega \colon \imath\,\sigma\imath^{-1} = \tau \text{ for some } \sigma \in G\}$,

Lemma

Let $i, i' \in \mathcal{I}_\tau$. Let us denote $\sigma = i^{-1}\tau i$, $\sigma' = i'^{-1}\tau i' \in G$.

(i) *If $i \equiv i' \bmod N_{\mathrm{Sym}(X)}(G)$, then*

$$\sigma \text{ and } \sigma' \text{ are } N_{\mathrm{Sym}(X)}(G)\text{-conjugate.}$$

(ii) *If σ and σ' are $N_{\mathrm{Sym}(X)}(G)$-conjugate,*

$$\text{then } i' \in i\,C(\sigma)\,N_{\mathrm{Sym}(X)}(G).$$

Here, $C(\sigma)$ denotes the centralizer of σ in $\mathrm{Sym}(X)$.

Test

Remember

$$\tau = (\alpha_{11}, \ldots, \alpha_{1\,\deg\varphi_1}) \ldots (\alpha_{r1}, \ldots, \alpha_{r\,\deg\varphi_r}) \in \mathsf{Sym}(\Omega)\,.$$

For each conjugacy class $\mathcal{C}$ in $N_{\mathsf{Sym}(X)}(G)$ of elements of G with cycle type $[\deg(\varphi_1), \ldots, \deg(\varphi_r)]$, we choose a representative

$$\sigma_{\mathcal{C}} = (\xi_{11}, \ldots, \xi_{1\,\deg\varphi_1}) \ldots (\xi_{r1}, \ldots, \xi_{r\,\deg\varphi_r}) \in G\,.$$

Then, for all coherent matches ξ_{t1} with α_{s1}, check whether the reduction of $\mathcal{G}_j$ replacing $a[\xi_{t\,u+1}]$ by $\alpha_{s1}^{\ell^u}$ modulo $\varphi_s(\alpha_{s1})$ and mod ℓ belongs to $\mathbb{F}_\ell[x_1, \ldots, x_k]$.

Number of tests

Proposition

Fix $\tau \in \mathrm{Gal}(f)$ as above. The number of tests necessary to find one of the F mod ℓ is less or equal to

$$M(\tau) := \frac{n_\tau}{d_1} \prod_{d \in D} d^{n_d} n_d!\,,$$

$$\begin{aligned} n_\tau &= \#\{\mathcal{C} \text{ in } N_{\mathrm{Sym}(X)}(G) \text{ of elements of } G \text{ with cycle type } [\tau]\},\\ D &= \{\text{distinct lengths in } [\tau]\},\\ n_d &= \#\text{occurrences of length } d \text{ in } [\tau],\\ d_1 &= \#C(\sigma) \bigcap N_{\mathrm{Sym}(X)}(G), \text{ for any } \sigma \in \mathrm{Sym}(X) \text{ with } [\sigma] = [\tau]. \end{aligned}$$

$M(\tau)$ tests: Case sharply 2-transitive

$\deg(f)$	$\mathrm{Gal}(f)$	$[\tau]$	$M(\tau)$
5	**5T3**	$[5]$	1
7	**7T4**	$[7]$	1
8	**8T25**	$[1,7]$	2
9	**9T14***	$[1,4,4]$	4
9	**9T15**	$[1,8]$	2
11	**11T4**	$[11]$	1
	...		
23	**23T4**	$[23]$	1
25	**25T41****	$[1,6,6,6,6]$	2592
25	**25T45***	$[1,12,12]$	24
25	**25T47**	$[1,24]$	4

$M(\tau)$ tests: Case sharply 3-transitive

$\deg(f)$	$\mathrm{Gal}(f)$	$[\tau]$	$M(\tau)$
5	$\mathcal{A}_5$	$[5]$	1
6	**6T14**	$[6]$	1
8	**8T43**	$[8]$	2
9	**9T27**	$[9]$	1
10	**10T30**	$[10]$	1
10	**10T31***	$[8,2]$	2
12	**12T218**	$[12]$	2
14	**14T39**	$[14]$	3
17	**17T6**	$[17]$	2
20	**20T362**	$[20]$	4
24	**24T10255**	$[24]$	4

More general

- Ordinary s2t:
  $\mathrm{Gal}(f) \sim \mathbb{A}^1(\mathbb{F}_q)$, $[\tau] = [1, q-1]$, $M(\tau) \leq \frac{\varphi(q-1)}{\nu}$, $q = p^\nu$.

More general

- Ordinary s2t:
  $\mathrm{Gal}(f) \sim \mathbb{A}^1(\mathbb{F}_q)$, $[\tau] = [1, q-1]$, $M(\tau) \leq \frac{\varphi(q-1)}{\nu}$, $q = p^\nu$.
- Twisted s2t: $\mathrm{Gal}(f) \sim \mathbb{A}^1(\mathcal{F})$, $[\tau] = \left[1, \frac{q^n-1}{n}, \ldots, \frac{q^n-1}{n}\right]$,
  $M(\tau) \leq \phi((q^n-1)/n)\left(\frac{q^n-1}{n}\right)^{n-1} n!$.

More general

- Ordinary s2t:
  $\mathrm{Gal}(f) \sim \mathbb{A}^1(\mathbb{F}_q)$, $[\tau] = [1, q-1]$, $M(\tau) \leq \frac{\varphi(q-1)}{\nu}$, $q = p^\nu$.
- Twisted s2t: $\mathrm{Gal}(f) \sim \mathbb{A}^1(\mathcal{F})$, $[\tau] = \left[1, \frac{q^n-1}{n}, \ldots, \frac{q^n-1}{n}\right]$,
  $M(\tau) \leq \phi((q^n-1)/n)\left(\frac{q^n-1}{n}\right)^{n-1} n!$.
- Ordinary s3t:
  $\mathrm{Gal}(f) \sim \mathrm{PGL}_2(\mathbb{F}_q)$, $[\tau] = [q+1]$, $M(\tau) \leq \frac{\varphi(q+1)}{2\,\nu}$.

More general

- Ordinary s2t:
  $\mathrm{Gal}(f) \sim \mathbb{A}^1(\mathbb{F}_q)$, $[\tau] = [1, q-1]$, $M(\tau) \leq \frac{\varphi(q-1)}{\nu}$, $q = p^\nu$.
- Twisted s2t: $\mathrm{Gal}(f) \sim \mathbb{A}^1(\mathcal{F})$, $[\tau] = \left[1, \frac{q^n-1}{n}, \ldots, \frac{q^n-1}{n}\right]$,
  $M(\tau) \leq \phi((q^n-1)/n)\left(\frac{q^n-1}{n}\right)^{n-1} n!$.
- Ordinary s3t:
  $\mathrm{Gal}(f) \sim \mathrm{PGL}_2(\mathbb{F}_q)$, $[\tau] = [q+1]$, $M(\tau) \leq \frac{\varphi(q+1)}{2\,\nu}$.
- Mathieu group M_{11}: $[\tau] = [11]$, $M(\tau) = 2$.

More general

- Ordinary s2t:
  $\mathrm{Gal}(f) \sim \mathbb{A}^1(\mathbb{F}_q)$, $[\tau] = [1, q-1]$, $M(\tau) \leq \frac{\varphi(q-1)}{\nu}$, $q = p^\nu$.
- Twisted s2t: $\mathrm{Gal}(f) \sim \mathbb{A}^1(\mathcal{F})$, $[\tau] = \left[1, \frac{q^n-1}{n}, \ldots, \frac{q^n-1}{n}\right]$,
  $M(\tau) \leq \phi((q^n-1)/n)\left(\frac{q^n-1}{n}\right)^{n-1} n!$.
- Ordinary s3t:
  $\mathrm{Gal}(f) \sim \mathrm{PGL}_2(\mathbb{F}_q)$, $[\tau] = [q+1]$, $M(\tau) \leq \frac{\varphi(q+1)}{2\,\nu}$.
- Mathieu group M_{11}: $[\tau] = [11]$, $M(\tau) = 2$.
- Mathieu group M_{12}: $[\tau] = [1, 11]$ or $[2, 10]$, $M(\tau) = 2$.

9T15

$$f = x^9 - 9\,x^7 - 21\,x^6 + 72\,x^5 + 99\,x^4 - 99\,x^3 - 585\,x^2 + 549\,x + 166\,.$$

$$\mathrm{Gal}(f) = 9\mathrm{T}15 \text{ similar to } \mathbb{A}^1(\mathbb{F}_9)\,.$$

$$\Delta(f) = 2^8 3^{20} 17^7 2843^2, \text{ and } \delta(f) = 2^3 3^4 17^1 2843^2\,.$$

$$f \equiv (x+1)\left(x^8 + 4\,x^7 + 2\,x^6 + 2\,x^5 + 4\,x^3 + 2\,x^2 + 3\,x + 1\right) \bmod 5\,.$$

Bound for the coefficients: $2.14675015918 \times 10^{73} \in [5^{2^6}, 5^{2^7}]$, ergo 7 iterations needed.

9T15 cont'd

$$\tilde{F}(x_1, x_2) = h(x_1)h(x_2)\tilde{\Gamma}(x_1, x_2)\,,$$

$$h(x_1) = (2 + x_1)^4 \left(4 + x_1 + 2\,x_1^2 + 4\,x_1^3 + x_1^4\right) \bmod 5,$$

$$\tilde{\Gamma}(x_1, x_2) = \sum_{\sigma \in \mathrm{Gal}(f)} \sigma(\alpha) \frac{f(x_1)}{x_1 - \sigma(\beta)} \frac{f(x_2)}{x_2 - \sigma(\gamma)}$$

where α, β, and γ are three roots of f mod 5.
Let ω be a generator of $\mathbb{F}_9^*$. Consider the polynomial

$$\mathcal{G}(x_1, x_2) = \sum_{\sigma \in \mathbb{A}^1(\mathbb{F}_9)} a[\sigma(\omega)] \frac{\prod_{\xi \in \mathbb{F}_9} (x_1 - a[\xi])}{x_1 - a[\sigma(1)]} \frac{\prod_{\xi \in \mathbb{F}_9} (x_2 - a[\xi])}{x_2 - a[\sigma(0)]}\,.$$

A Fröbenius $\tau \in \mathrm{Gal}(f)$ at 5 is

$$(\alpha_0)(\alpha_1, \alpha_\omega, \ldots, \alpha_{\omega^7})$$

with $\alpha_0 \equiv -1$ and $\alpha_{\omega^i} \equiv \alpha_1^{5^i}$ modulo a prime ideal over 5.

Here, α_1 is a root of $x^8 + 4x^7 + 2x^6 + 2x^5 + 4x^3 + 2x^2 + 3x + 1$ mod 5.

$$\sigma_{m,n}\colon x \mapsto m\,x + n \in \mathbb{A}^1(\mathbb{F}_9)$$

There are two conjugacy classes in $N_{\mathrm{Sym}(\mathbb{F}_9)}(\mathbb{A}^1(\mathbb{F}_9))$ of elements in $\mathbb{A}^1(\mathbb{F}_9)$ with cycle type $[1, 8]$:

$$\sigma_{\omega,0}\colon x \mapsto \omega x, \text{ and } \sigma_{\omega^5,0}\colon x \mapsto \omega^5 x.$$

An admissible $\imath\colon \mathbb{F}_9 \to \Omega$ must identify τ (up to conjugation) with either $\sigma_{\omega,0} = (0)(1, \omega, \ldots, \omega^7)$ or $\sigma_{\omega^5,0}$.

After replacing $a[0]$ by -1 and $a[\omega^i]$ by $\alpha_1^{5^i}$ in $\mathcal{G}(x_1, x_2)$, one gets

$$\tilde{\Gamma}(x_1,x_2) = 1 + 3\,x_1 + 2\,x_1^2 + 3\,x_1^3 + 4\,x_1^4 + 2\,x_1^6 + 4\,x_1^7 + 4\,x_1^8 + 4\,x_2 + 2\,x_1\,x_2 + x_1^3\,x_2 + 2\,x_1^4\,x_2 + 4\,x_1^5\,x_2 + x_1^6\,x_2 + 4\,x_1^7\,x_2 + 2\,x_1^8\,x_2 + 2\,x_2^2 + 3\,x_1\,x_2^2 + 4\,x_1^3\,x_2^2 + 4\,x_1^4\,x_2^2 + 4\,x_1^6\,x_2^2 + 3\,x_1^7\,x_2^2 + 3\,x_2^3 + 3\,x_1\,x_2^3 + 2\,x_1^2\,x_2^3 + 3\,x_1^3\,x_2^3 + 3\,x_1^4\,x_2^3 + x_1^5\,x_2^3 + x_1^6\,x_2^3 + 3\,x_1^7\,x_2^3 + x_1^8\,x_2^3 + 4\,x_2^4 + 2\,x_1\,x_2^4 + x_1^2\,x_2^4 + x_1^4\,x_2^4 + 2\,x_1^5\,x_2^4 + 2\,x_1^6\,x_2^4 + 3\,x_1^7\,x_2^4 + 2\,x_2^5 + 4\,x_1\,x_2^5 + 2\,x_1^2\,x_2^5 + 4\,x_1^3\,x_2^5 + 2\,x_1^5\,x_2^5 + 3\,x_1^6\,x_2^5 + 3\,x_1^8\,x_2^5 + 3\,x_2^6 + 3\,x_1\,x_2^6 + 3\,x_1^2\,x_2^6 + 4\,x_1^3\,x_2^6 + 4\,x_1^4\,x_2^6 + 3\,x_1^5\,x_2^6 + 4\,x_1^6\,x_2^6 + 2\,x_1^8\,x_2^6 + 4\,x_2^7 + 2\,x_1\,x_2^7 + x_1^2\,x_2^7 + 2\,x_1^4\,x_2^7 + 2\,x_1^7\,x_2^7 + 2\,x_1^8\,x_2^7 + 4\,x_2^8 + 2\,x_1\,x_2^8 + x_1^3\,x_2^8 + 3\,x_1^5\,x_2^8 + 2\,x_1^6\,x_2^8 + 2\,x_1^7\,x_2^8\,.$$

$$\tilde{\Gamma}(x_1,x_2) \rightsquigarrow \tilde{F}(x_1,x_2) \bmod 5 \rightsquigarrow F(x_1,x_2) \text{ 5-adic} \rightsquigarrow F(x_1,x_2) \text{ rational}\,.$$

9T14

$$f = x^9 - 3x^8 + 12x^7 - 12x^6 + 12x^5 - 12x^4 + 12x^3 - 12x^2 + 9x - 3$$

$\mathrm{Gal}(f) = 9\mathsf{T}14$ similar to $\mathbb{A}^1(\mathcal{F})$,

$\mathcal{F} = (\mathbb{F}_9, +, \circ)$ is the twisted Dickson nearfield of 9 elements.

9T14 cont'd

$$F(x_1, x_2) = \frac{1}{2904}\Big(-552 + 1425\,x_1 + 6879\,{x_1}^2 - 411\,{x_1}^3 - 4566\,{x_1}^4 - 3804\,{x_1}^5 + 4815\,{x_1}^6 - 1512\,{x_1}^7 + 474\,{x_1}^8 + \Big(-5586 + 16692\,x_1 - 26283\,{x_1}^2 + 11862\,{x_1}^3 - 5169\,{x_1}^4 + 28059\,{x_1}^5 - 24813\,{x_1}^6 + 7155\,{x_1}^7 - 2069\,{x_1}^8\Big)\,x_2 + (5673 - 15171\,x_1 + 17661\,{x_1}^2 - 3009\,{x_1}^3 + 13083\,{x_1}^4 - 19170\,{x_1}^5 + 15291\,{x_1}^6 - 4138\,{x_1}^7 + 1140\,{x_1}^8)\,{x_2}^2 + \Big(6348 - 12642\,x_1 + 9249\,{x_1}^2 - 14166\,{x_1}^3 + 11424\,{x_1}^4 - 507\,{x_1}^5 + 16903\,{x_1}^6 - 3391\,{x_1}^7 + 1842\,{x_1}^8\Big)\,{x_2}^3 + \Big(-1209 - 5184\,x_1 + 20073\,{x_1}^2 - 12582\,{x_1}^3 + 5550\,{x_1}^4 - 12651\,{x_1}^5 + 27111\,{x_1}^6 - 6691\,{x_1}^7 + 2711\,{x_1}^8\Big)\,{x_2}^4 + \Big(3480 + 1473\,x_1 - 9039\,{x_1}^2 - 8847\,{x_1}^3 + 10309\,{x_1}^4 + 22172\,{x_1}^5 + 16407\,{x_1}^6 - 1860\,{x_1}^7 + 2341\,{x_1}^8\Big)\,{x_2}^5 + (-567 - 1236\,x_1 + 3741\,{x_1}^2 + 582\,{x_1}^3 - 1455\,{x_1}^4 - 5879\,{x_1}^5 - 1197\,{x_1}^6 - 169\,{x_1}^7 - 272\,{x_1}^8)\,{x_2}^6 + \Big(291 + 183\,x_1 - 637\,{x_1}^2 - 1189\,{x_1}^3 + 1152\,{x_1}^4 + 2228\,{x_1}^5 + 2323\,{x_1}^6 - 334\,{x_1}^7 + 311\,{x_1}^8\Big)\,{x_2}^7\Big)\ .$$

The nine roots of f are represented by

$$x_1\,, \qquad x_2\,, \qquad F(x_1,x_2)\,,$$
$$F(x_2,x_1)\,, \qquad F(F(x_1,x_2),x_1)\,, \qquad F(F(x_2,x_1),x_2)\,,$$
$$F(x_2,F(x_1,x_2))\,, \qquad F(x_1,F(x_2,x_1))\,, \qquad F(x_1,F(x_1,x_2))\,.$$

Further questions

- Are all sharply k-transitive groups realizable as Galois groups over $\mathbb{Q}$?

Further questions

- Are all sharply k-transitive groups realizable as Galois groups over $\mathbb{Q}$?
- j-invariants of p-isogenous elliptic curves are sharply 3-transitive, ...

Further questions

- Are all sharply k-transitive groups realizable as Galois groups over $\mathbb{Q}$?
- j-invariants of p-isogenous elliptic curves are sharply 3-transitive, ...
- Known applications of nearfields to criptography?