Claus Diem

Institut für Experimentelle Mathematik
Essen

Galois Theory and the DL-Problem

Special thanks to G.Frey and
A. Enge, S.Galbraith, P.Gaudry, F.Hess,
S.Müller-Stach, N.Naumann, N.Smart, E.Viehweg

Let n be a prime number, q the power of a prime number. Let $k := \mathbb{F}_q$, $K := \mathbb{F}_{q^n}$ so that $K|k$ is an extension of finite fields of prime degree n.

Let $H'|K$ be a regular function field (of transcendence degree 1). ("regular" means that K is algebraically closed in H'.) Assume that H' is "cryptographically good", i.e. $\mathrm{Cl}^0(H')$ contains a large prime factor and ... .

Let $C|k$ be a regular function field such that H' is included in KC.

$$H' \hookrightarrow KC$$

This can be translated into the language of (semi-classical) algebraic geometry (the language of Silverman's book on elliptic curves) as follows:

H' is the function field of a non-singular, projective curve $\mathcal{H}'$, defined over K, C is the function field of a non-singular, projective curve $\mathcal{C}$, defined over k, and there exists a covering

$$\mathcal{C} \longrightarrow \mathcal{H}',$$

defined over K.

Consider the morphism

$$\mathsf{norm}_{C}^{KC} \circ \mathsf{con}_{H'}^{KC} : \\ \mathsf{Cl}^0(H') \longrightarrow \mathsf{Cl}^0(KC) \longrightarrow \mathsf{Cl}^0(C).$$

With this morphism, we try to transform the DL-problem in $\mathsf{Cl}^0(H')$ into the potentially easier DL-problem in $\mathsf{Cl}^0(C)$.

In order to use the map $\mathrm{norm}_C^{KC} \circ \mathrm{con}_{H'}^{KC}$ as an attack on the DL-problem in $\mathrm{Cl}^0(H')$, two conditions have to be fulfilled:

1. The kernel does not contain the large prime factor of $\mathrm{Cl}^0(H')$.

2. The genus of $\mathcal{C}$ should not be "too large" in relation to n.

Additionally, it would be helpful, if $\mathcal{C}$ had certain "nice properties", e.g. hyperelliptic, automorphisms, k-rational points ... .

For condition 1, no theoretical result is known. However, there exist methods from algebraic geometry which suggest *very strongly*, that the kernel is small under certain conditions.

To formulate the conditions, we make the following distinction:

- **A** $\mathcal{H}'$ is defined over k, i.e. there exists a regular field extension $H|k$ such that $KH = H'$

- **B** This is not the case and furthermore: The Jacobian of $\mathcal{H}'$, Jac($\mathcal{H}'$), is not K-isogenous to an abelian variety defined over k.
  If $\mathcal{H}'$ is an elliptic curve this means: $\mathcal{H}'$ is not K-isogenous to another elliptic curve defined over k.

In both cases, we assume that Jac($\mathcal{H}'$) is K-simple and End_K(Jac(H')) is commutative. If $\mathcal{H}'$ is an elliptic curve then this is fulfilled if $\mathcal{H}'$ is non-super-singular.

B – Theoretical result

The kernel of $\mathrm{norm}_C^{KC} \circ \mathrm{con}_{H'}^{KC}$ is always small.

B – Construction Let $H'|K(x)$ be a galois extension. Let $C' = H'\sigma(H')\cdots\sigma^{n-1}(H')$ be the galois closure of $H'|k(x)$.

Assume that $C'|K$ is regular.

Then by galois theory we have an exact sequence

$$1 \longrightarrow \mathrm{Gal}(H'|K(x)) \longrightarrow \mathrm{Gal}(H'|k(x)) \longrightarrow \mathrm{Gal}(K|k) \longrightarrow 1.$$

This sequence splits, every section determines a subgroup of $\mathrm{Gal}(H'|k(x))$, and the fixed field under this subgroup defines a regular extension $C|k(x)$ with $KC = C'$.

B – Examples Let H' be a hyperelliptic function field, $H'|K(x)$ a canonical extension of degree 2.

$\mathbf{q = 2^i}$ (Smart, Hess, Galbraith)

Let $H' = K(x)[y];\ y^2 + xy = f(x)$

(with special f if $g(\mathcal{H}') \geq 2$).

Then $C'|K$ is regular, $g(\mathcal{C}) \leq 2^{n-1} g(\mathcal{H}')$.

$\mathbf{q = p^i, p > 2}$

$H' = K(x)[y];\ y^2 = f(x)$

Then $C'|K$ is regular,

$$\begin{array}{rl} 2^{n-2}(2g(\mathcal{H}') + n - 3) + 1 & \leq g(\mathcal{C}) \leq \\ 2^{n-2}((2g(\mathcal{H}') + 2)n - 3) + 1 & \end{array}$$

A – Introduction Let $H|k$ be regular, $H' = KH$. $(k = \mathbb{F}_q, K = \mathbb{F}_{q^n})$ Let $H|C$ be an extension of regular function fields.

Then the kernel of $\mathrm{norm}_C^{KC} \circ \mathrm{con}_{H'}^{KC}$ is always *large*.

$$\begin{array}{ccc} KC & \text{---} & KH = H' \\ | & & | \\ C & \text{———} & H \end{array}$$

A – Main theoretical result

Now let t be an automorphism of C order n which does not fix H but fixes some place of $\overline{k}C$.

Let $\sigma \in \mathrm{Gal}(K|k)$ be the Frobenius. Then σ also operates on KC, and $H' = KH$ and $KC^{<\sigma>} = C, KH^{<\sigma>} = H$.

Let $C^t := KC^{<\sigma t>}$. C^t is the function field of the "twist" $\mathcal{C}^t$ of $\mathcal{C}$ with t.

$$\begin{array}{ccc} KC & \text{---} & KH = H' \\ | & & \\ C^t & & \end{array}$$

Then the kernel of $\mathrm{norm}^{KC}_{C^t} \circ \mathrm{con}^{KC}_{H}$ is always *small*.

Note that $\mathrm{norm}^{KC}_{C^t}$ is given by $D \mapsto \sum_{i=0}^{n-1} \sigma^i t^i(D)$.

A – Construction

Let $H|k(x)$ be an extension such that $n|[H : k(x)]$, C the galois closure of $H|k(x)$. Then C has an automorphism t of order n which does not fix H.

Assume that $C|k(x)$ is regular and that t fixes a place of $\overline{k}C$.

A – Examples

$\mathbf{n = 3}$ Let H be an elliptic function field, $j \neq 0$. Let H be the field extension defined by a "nice" Weierstrass-equation. Let C be the galois closure of $H|k(y)$.

$\mathbf{q = p^i, p > 3}$

$\mathcal{H}' : y^2 = x^3 + A_4 x + B$ ($A_4 \neq 0$)

Assume that $\zeta_3 \in k$. Then $K|k$ is a Kummer-extension, $K = k(\alpha)$, $\alpha^3 = a \in k$.

$\mathcal{C}^t : y^2 = x_1^7 + a^{-1}Bx_1^4 - \frac{A_4^3}{27a^2}x_1$

$\Longrightarrow$ $\mathcal{C}^t$ is hyperelliptic of genus 3. (The assumption $\zeta_3 \in k$ is not necessary for $\mathcal{C}^t$ being hyperelliptic.)

$\mathbf{q = 2^i}$, $K|k$ as above.

$\mathcal{H}' : y^2 + xy = x^3 + A_2x^2 + B$

$\mathcal{C}^t : a^2x_1^2x_2^2 + aA_2x_1x_2 + ax_1^3 + a^2x_2^3 + A_2^2 + A_2^4 + B = 0$ $(y = A_2^2 + ax_1x_2)$

$\Longrightarrow g(\mathcal{C}^t) = 3$, $\mathcal{C}^t$ is non-hyperelliptic

$\mathbf{q = 3^i}$. $K = k(\alpha)$, $\alpha^3 - \alpha = a \in k$. (Artin-Schreier extension)

$\mathcal{H}' : y^2 = x^3 + A_2x^2 + B$

$\mathcal{C}^t : y^2 = A_2^{-3}x_1^6 + A_2^{-1}x_1^4 + ax_1^3 + A_2x_1^2 - A_2^2x_1 + a^2A_2^3 + B$

$\Longrightarrow g(\mathcal{C}^t) = 2$

A – Examples (cont.)

Let n be arbitrary, H a hyperelliptic function field. Assume that the n-th roots of unity are contained in k.

Let $H|k(x)$ be defined by a Weierstrass equation. Consider

$$\begin{array}{c} H \\ \Big|{\scriptstyle 2} \\ k(x) \\ \Big|{\scriptstyle n} \\ k(z) \end{array}$$

Let C be the galois closure of $H|k(z)$.

$\mathbf{q = 2^i}$ H elliptic function field.

Then $C|k$ is either regular, or C is regular over the extension of degree 2 of k.

Let $\phi_2(n) :=$ ord(2) in $(\mathbb{Z}/n\mathbb{Z})^*$.

Then $g(\mathcal{C}^t) \leq 2^{2\phi_2(n)} - 1$.

In particular:

$q = 2^5$, $n = 31$. Then $\mathcal{C}^t$ is defined over $\mathbb{F}_{2^{10}}$, $g(\mathcal{C}^t) \leq 2^{10} - 1$, and t is an automorphism of $\mathcal{C}^t$ of order 31.

$q = 2^7$, $n = 127$. Then $\mathcal{C}^t$ is defined over $\mathbb{F}_{2^{14}}$, $g(\mathcal{C}^t) \leq 2^{14} - 1$, and t is an automorphism of $\mathcal{C}^t$ of order 127.

$\mathbf{q = p^i, p > 2}$ H hyperelliptic function field.

Then $C|k$ is regular,

$g(\mathcal{C}^t) \leq 2^{n-2}((2g(\mathcal{H}') + 2)n - 3) + 1$

Outline of the Proofs

Let $\mathcal{H}'$ be a curve defined over K, $\mathcal{W}$ the Weil-restriction of $\mathcal{H}'$ with respect to $K|k$.

For simplicity assume that $\mathcal{H}'$ is an elliptic curve. Then $\mathcal{W}$ is an n-dimensional abelian variety defined over k.

Let $\mathcal{C}$ be a curve defined over k.

Morphisms $a : \mathcal{C} \longrightarrow \mathcal{H}'$ defined over K are in bijection to morphisms $b : \mathcal{C} \longrightarrow \mathcal{W}$ defined over k.

The kernel of $\mathrm{norm}_C^{KC} \circ \mathrm{con}_{H'}^{KC}$ is isomorphic to the kernel of $b^* : \mathcal{W}(k) \longrightarrow \mathrm{Jac}(\mathcal{C})(k)$.

B $\mathcal{W}$ is simple. So we expect the kernel to be *small*.

A $\mathcal{W} \sim_k \mathcal{H}' \times \mathcal{A}$ and $\mathcal{A}$ is k-simple. $a : \mathcal{C} \longrightarrow \mathcal{H}'$ defined over k corresponds to a morphism $b : \mathcal{C} \longrightarrow \mathcal{W}$ whose image lies in $\mathcal{H}'$. So b^* is trivial on $\mathcal{A}$ and the kernel is *large*.

However, $\mathcal{C}^t \simeq \mathcal{C} \longrightarrow \mathcal{H}'$ corresponds to a morphism $b' : \mathcal{C}^t \longrightarrow \mathcal{W}$ whose image is not "parallel" to $\mathcal{H}'$, i.e. its projection onto $\mathcal{A}$ is a curve. This implies that b'^* preserves $\mathcal{A}$ and the kernel is *small*.

Question

Let $K|k$ be some field extension, $\mathcal{H}'$ a curve defined over K, $\mathcal{W}$ the Weil-restriction of $\mathcal{H}'$ with respect to $K|k$. Let $\mathcal{C}$ be a curve defined over k. Then the morphisms $a : \mathcal{C} \longrightarrow \mathcal{H}'$ defined over K correspond to the morphisms $b : \mathcal{C} \longrightarrow \mathcal{W}$ defined over k.

Should one try to find coverings of $\mathcal{H}'$ by searching curves on $\mathcal{W}$ or should one try to find curves on $\mathcal{W}$ by searching coverings of $\mathcal{H}'$ **?**