Computing class groups and gonalities of algebraic curves over finite fields

Maarten Derickx and Kenji Terao

July 6, 2026

Code available at: `https://github.com/nt-lib/CurveArith/`

Notation

Let k be a finite field, and X a smooth, projective, geometrically integral curve over k.

Notation

Let k be a finite field, and X a smooth, projective, geometrically integral curve over k.

Definition

Let $\operatorname{Div} X$ be the group of Weil divisors on X and $\operatorname{Princ} X$ the subgroup of principal divisors of X. The class group of X is the quotient

$$\operatorname{Cl} X = \operatorname{Div} X / \operatorname{Princ} X.$$

Notation

Let k be a finite field, and X a smooth, projective, geometrically integral curve over k.

Definition

Let $\operatorname{Div} X$ be the group of Weil divisors on X and $\operatorname{Princ} X$ the subgroup of principal divisors of X. The class group of X is the quotient

$$\operatorname{Cl} X = \operatorname{Div} X / \operatorname{Princ} X.$$

Definition

Let $k(X)$ be the function field of X. The gonality of X is

$$\operatorname{gon} X = \min_{f \in k(X) \setminus k} \deg(f).$$

Divisor enumeration

Given a divisor $D \in \operatorname{Div} X$, the Riemann-Roch space of D is defined by

$$\mathcal{L}(D) = \{0\} \cup \{f \in k(X)^\times : v_x(f) \geq -v_x(D) \quad \forall x \in X\}.$$

This is a k-vector space, and we denote by $\ell(D)$ its dimension.

Divisor enumeration

Given a divisor $D \in \operatorname{Div} X$, the Riemann-Roch space of D is defined by

$$\mathcal{L}(D) = \{0\} \cup \{f \in k(X)^\times : v_x(f) \geq -v_x(D) \quad \forall x \in X\}.$$

This is a k-vector space, and we denote by $\ell(D)$ its dimension.

We have

$$\operatorname{gon}(X) = \min_{f \in k(X) \setminus k} \deg(f)$$

Divisor enumeration

Given a divisor $D \in \operatorname{Div} X$, the Riemann-Roch space of D is defined by

$$\mathcal{L}(D) = \{0\} \cup \{f \in k(X)^\times : v_x(f) \geq -v_x(D) \quad \forall x \in X\}.$$

This is a k-vector space, and we denote by $\ell(D)$ its dimension.

We have

$$\begin{aligned} \operatorname{gon}(X) &= \min_{f \in k(X) \setminus k} \deg(f) \\ &= \min_{\substack{D \geq 0 \\ \ell(D) \geq 2}} \deg(D). \end{aligned}$$

Divisor enumeration

for $d = 1, 2, \ldots$ **do**
    for all $D \geq 0, \deg(D) = d$ **do**
        if $\ell(D) \geq 2$ **then**
            return d

Divisor enumeration

for $d = 1, 2, \ldots$ **do**
  for all $D \geq 0, \deg(D) = d$ **do**
    if $\ell(D) \geq 2$ **then**
      return d

The number of divisors which need to be considered grows exponentially with the gonality of X. However, this approach is still viable for curves of moderate genus over small fields, and is used for instance by Derickx-van Hoeij (2014), Derickx-Sutherland (2017), Najman-Orlić (2024) and Orlić (2026).

Computing Riemann-Roch spaces

Hess (2002): polynomial and ideal arithmetic

Computing Riemann-Roch spaces

Hess (2002): polynomial and ideal arithmetic

- Fast, but becomes a bottleneck when dealing with thousands or millions of divisors

Computing Riemann-Roch spaces

Hess (2002): polynomial and ideal arithmetic

- Fast, but becomes a bottleneck when dealing with thousands or millions of divisors

Instead, we exploit the redundancy that occurs when computing large numbers of Riemann-Roch spaces.

Computing Riemann-Roch spaces

If $E \leq D_0$ (i.e. $E = D_0 - D$, D effective), then

$$\mathcal{L}(E) \subseteq \mathcal{L}(D_0).$$

Computing Riemann-Roch spaces

If $E \leq D_0$ (i.e. $E = D_0 - D$, D effective), then

$$\mathcal{L}(E) \subseteq \mathcal{L}(D_0).$$

If $D = n_1 x_1 + \cdots + n_r x_r$ for some distinct $x_i \in X$, $n_i \in \mathbb{Z}_{\geq 1}$, then

$$\mathcal{L}(D_0 - D) = \mathcal{L}(D_0 - n_1 x_1) \cap \cdots \cap \mathcal{L}(D_0 - n_r x_r).$$

Computing Riemann-Roch spaces

$$\mathcal{L}(D_0)$$

Computing Riemann-Roch spaces

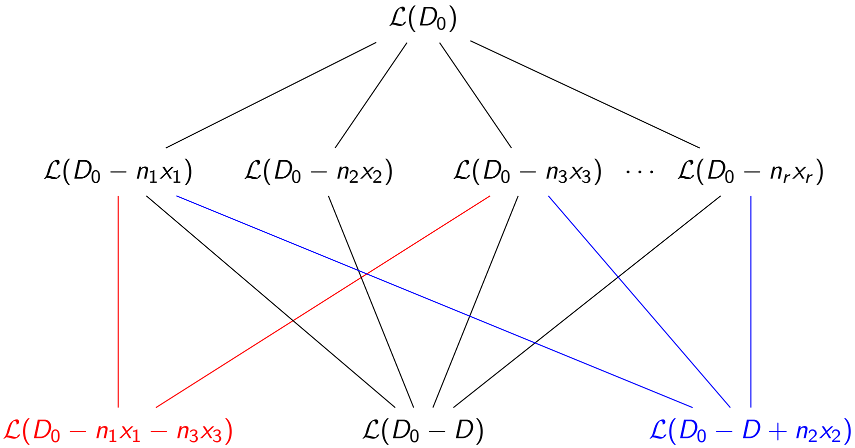
$$\mathcal{L}(D_0)$$

$$\mathcal{L}(D_0 - n_1 x_1) \qquad \mathcal{L}(D_0 - n_2 x_2) \qquad \mathcal{L}(D_0 - n_3 x_3) \quad \cdots \quad \mathcal{L}(D_0 - n_r x_r)$$

Computing Riemann-Roch spaces

$$\begin{tikzcd}[column sep=small]
 & & \mathcal{L}(D_0) \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[drr, dash] & & \\
\mathcal{L}(D_0 - n_1x_1) \arrow[drr, dash] & \mathcal{L}(D_0 - n_2x_2) \arrow[dr, dash] & \mathcal{L}(D_0 - n_3x_3) \arrow[d, dash] & \cdots & \mathcal{L}(D_0 - n_rx_r) \arrow[dll, dash] \\
 & & \mathcal{L}(D_0 - D) & &
\end{tikzcd}$$

Computing Riemann-Roch spaces



Computing Riemann-Roch spaces

We compute the subspaces $\mathcal{L}(D_0 - nx) \leq \mathcal{L}(D_0)$ using series expansions of a basis of $\mathcal{L}(D_0)$.

Computing Riemann-Roch spaces

We compute the subspaces $\mathcal{L}(D_0 - nx) \leq \mathcal{L}(D_0)$ using series expansions of a basis of $\mathcal{L}(D_0)$.

- Gives $\mathcal{L}(D_0 - nx)$ as the nullspace of a $\ell(D_0) \times n \deg(x)$ matrix.

Computing Riemann-Roch spaces

We compute the subspaces $\mathcal{L}(D_0 - nx) \leq \mathcal{L}(D_0)$ using series expansions of a basis of $\mathcal{L}(D_0)$.

- Gives $\mathcal{L}(D_0 - nx)$ as the nullspace of a $\ell(D_0) \times n \deg(x)$ matrix.
- $\ker A \cap \ker B = \ker(A \mid B)$.

Computing Riemann-Roch spaces

We compute the subspaces $\mathcal{L}(D_0 - nx) \leq \mathcal{L}(D_0)$ using series expansions of a basis of $\mathcal{L}(D_0)$.

- Gives $\mathcal{L}(D_0 - nx)$ as the nullspace of a $\ell(D_0) \times n \deg(x)$ matrix.
- $\ker A \cap \ker B = \ker(A \mid B)$.
- Requires polynomial and ideal operations.

Computing gonalities

for $d = 1, 2, \ldots$ **do**
  for all $D \geq 0, \deg(D) = d$ **do**
    if $\ell(D) \geq 2$ **then**
      return d

Computing gonalities

for $d = 1, 2, \ldots$ **do**
  for all $D \geq 0, \deg(D) = d$ **do**
    if $\ell(D) \geq 2$ **then**
      return d

$$D_0 = \sum_{\substack{x \in X \\ \deg(x) \leq d}} \left\lfloor \frac{d}{\deg(x)} \right\rfloor x.$$

Computing gonalities

for $d = 1, 2, \ldots$ **do**
  for all $D \geq 0, \deg(D) = d$ **do**
    if $\ell(D) \geq 2$ **then**
      return d

Instead, we use the Riemann-Roch theorem:

$$\ell(D) - \ell(K_X - D) = \deg(D) - g + 1,$$

where K_X is a canonical divisor on X.

Computing gonalities

for $d = 1, 2, \ldots$ **do**
  for all $D \geq 0, \deg(D) = d$ **do**
    if $\ell(K_X - D) \geq g + 1 - \deg(D)$ **then**
      return d

Instead, we use the Riemann-Roch theorem:

$$\ell(D) - \ell(K_X - D) = \deg(D) - g + 1,$$

where K_X is a canonical divisor on X.

Computing gonalities

for $d = 1, 2, \dots$ **do**
  for all $D \geq 0, \deg(D) = d$ **do**
    if $\ell(K_X - D) \geq g + 1 - \deg(D)$ **then**
      return d

Instead, we use the Riemann-Roch theorem:

$$\ell(D) - \ell(K_X - D) = \deg(D) - g + 1,$$

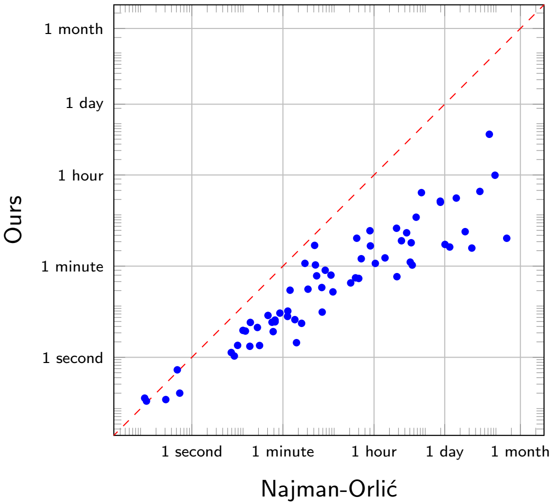
where K_X is a canonical divisor on X. Note that $\ell(K_X) = g(X)$.

Timings

Najman-Orlić (2024) compute the gonalities of 65 different modular curves $X_0(N)$ over various finite fields.

Timings

Najman-Orlić (2024) compute the gonalities of 65 different modular curves $X_0(N)$ over various finite fields.



Computing class groups

We base ourselves on the index-calculus style method developed by Hess (2005).

Computing class groups

We base ourselves on the index-calculus style method developed by Hess (2005).

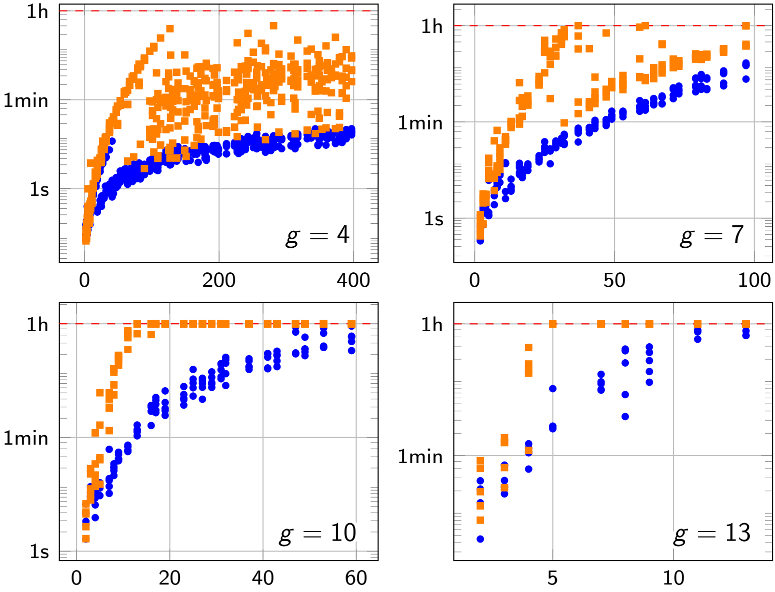
- Requires, in part, computing Riemann-Roch spaces $\mathcal{L}(D)$ for many (nearly) effective divisors D.

Computing class groups

We base ourselves on the index-calculus style method developed by Hess (2005).

- Requires, in part, computing Riemann-Roch spaces $\mathcal{L}(D)$ for many (nearly) effective divisors D.
- As for gonalities, we need to transform the set of divisors for which we compute Riemann-Roch spaces to apply our linear algebraic procedure.

Timings


1h
1min
1s
0
200
400
$g = 4$
1h
1min
1s
0
50
100
$g = 7$
1h
1min
1s
0
20
40
60
$g = 10$
1h
1min
5
10
$g = 13$

Thank you for listening!