Infrastructure, Arithmetic, and Class Number Computations in Purely Cubic Function Fields of Characteristic at Least 5

Eric Landquist

University of Illinois at Urbana-Champaign

January 27, 2009

Outline

Motivation

- Cryptography

Motivation

- Cryptography
  - Elliptic Curves over $\mathbb{F}_q$: $Y^2 = x^3 + ax + b$
    [Miller, 1986; Koblitz, 1987]

Motivation

- Cryptography
  - Elliptic Curves over $\mathbb{F}_q$: $Y^2 = x^3 + ax + b$
    [Miller, 1986; Koblitz, 1987]
  - Jacobians of Hyperelliptic Curves over $\mathbb{F}_q$: $Y^2 + h(x)Y = f(x)$
    [Koblitz, 1989]

Motivation

- Cryptography
  - Elliptic Curves over $\mathbb{F}_q$: $Y^2 = x^3 + ax + b$ [Miller, 1986; Koblitz, 1987]
  - Jacobians of Hyperelliptic Curves over $\mathbb{F}_q$: $Y^2 + h(x)Y = f(x)$ [Koblitz, 1989]
  - Can the Jacobians of other curves be used?

Motivation

- Cryptography
  - Elliptic Curves over $\mathbb{F}_q$: $Y^2 = x^3 + ax + b$
    [Miller, 1986; Koblitz, 1987]
  - Jacobians of Hyperelliptic Curves over $\mathbb{F}_q$: $Y^2 + h(x)Y = f(x)$
    [Koblitz, 1989]
  - Can the Jacobians of other curves be used?
  - Probably not: too slow, less secure, and the order of the Jacobian is difficult to compute.

Motivation

- Cryptography
  - Elliptic Curves over $\mathbb{F}_q$: $Y^2 = x^3 + ax + b$ [Miller, 1986; Koblitz, 1987]
  - Jacobians of Hyperelliptic Curves over $\mathbb{F}_q$: $Y^2 + h(x)Y = f(x)$ [Koblitz, 1989]
  - Can the Jacobians of other curves be used?
  - Probably not: too slow, less secure, and the order of the Jacobian is difficult to compute.
- Important problems in Algebraic Number Theory

Motivation

- Cryptography
  - Elliptic Curves over $\mathbb{F}_q$: $Y^2 = x^3 + ax + b$
    [Miller, 1986; Koblitz, 1987]
  - Jacobians of Hyperelliptic Curves over $\mathbb{F}_q$: $Y^2 + h(x)Y = f(x)$
    [Koblitz, 1989]
  - Can the Jacobians of other curves be used?
  - Probably not: too slow, less secure, and the order of the Jacobian is difficult to compute.
- Important problems in Algebraic Number Theory
  - "The determination of the structure of $Cl(K)$ and in particular of the class number $h(K)$ is one of the main problems in algorithmic algebraic number theory." (Cohen)

Motivation

- Cryptography
  - Elliptic Curves over $\mathbb{F}_q$: $Y^2 = x^3 + ax + b$ [Miller, 1986; Koblitz, 1987]
  - Jacobians of Hyperelliptic Curves over $\mathbb{F}_q$: $Y^2 + h(x)Y = f(x)$ [Koblitz, 1989]
  - Can the Jacobians of other curves be used?
  - Probably not: too slow, less secure, and the order of the Jacobian is difficult to compute.
- Important problems in Algebraic Number Theory
  - "The determination of the structure of $Cl(K)$ and in particular of the class number $h(K)$ is one of the main problems in algorithmic algebraic number theory." (Cohen)
  - The infrastructure of a global field is not very well understood.

Cubic Function Fields

General cubic curve (standard form):

$$C : F(x,\ Y) = Y^3 - AY + B = 0\ , \quad A,\ B \in \mathbb{F}_q[x]$$

$F(x,\ Y)$ abs. irred. and $\nexists Q \in \mathbb{F}_q[x] \setminus \mathbb{F}_q : Q^2 \mid A,\ Q^3 \mid B$.

Purely cubic curve:

$$C : Y^3 = GH^2\ , \quad G,\ H \in \mathbb{F}_q[x] \text{ co-prime, monic, square-free}$$

- $K = K_x = \mathbb{F}_q(C) = \mathbb{F}_q(x,\ y)$, with $F(x,\ y) = 0$
- $\mathcal{O} = \mathbb{F}_q[C]$: Maximal order of K with unit rank $r \in \{0,\ 1,\ 2\}$
- If $3 \nmid \deg\left(GH^2\right)$ then $r = 0$, $\mathrm{sig}(K) = (3,1)$.
- If $3 \mid \deg\left(GH^2\right)$ and $q \equiv 2 \pmod 3$, then $r = 1$, $\mathrm{sig}(K) = (1,1;1,2)$.
- If $3 \mid \deg\left(GH^2\right)$ and $q \equiv 1 \pmod 3$, then $r = 2$.

Notation

- $\mathcal{O} = [1, \rho, \omega]$, $\rho^3 = GH^2$, $\omega = \rho^2/H$
- $S = \{\infty_0, \ldots, \infty_r\}$: Set of infinite places of K
- $\mathcal{D}$: The group of divisors of K
- D^+: The effective part of $D \in \mathcal{D}$; $D^+ \geq 0$, $(D - D^+) \leq 0$
- D_S: The finite part of $D \in \mathcal{D}$
- D^S: The infinite part of $D \in \mathcal{D}$; $D = D_S + D^S$
- $\mathcal{D}_0 = \{D \in \mathcal{D} \mid \deg(D) = 0\}$
- $\mathcal{D}^S = \left\{D \in \mathcal{D} \mid D = D^S\right\}$
- $\mathcal{D}_0^S = \mathcal{D}_0 \cap \mathcal{D}^S$
- $\mathcal{P}$: The subgroup of $\mathcal{D}_0$ of principal divisors
- $\mathcal{P}^S = \mathcal{P} \cap \mathcal{D}_0^S$

Notation

- $\mathcal{J}_K = \mathcal{D}_0/\mathcal{P}$: divisor class group of K; $h = |\mathcal{J}_K|$
- $Cl(\mathcal{O}) = \mathcal{I}(\mathcal{O})/\mathcal{P}(\mathcal{O})$: ideal class group of $\mathcal{O}$; $h_x = |Cl(\mathcal{O})|$
- $R^S = \left|\mathcal{D}_0^S/\mathcal{P}^S\right|$: S-regulator of K

$$\Phi : \mathcal{D}_S \to \mathcal{I}(\mathcal{O}),\ \ D_S \mapsto \{\alpha \in K^* \mid \mathrm{div}(\alpha)_S \geq D_S\} \tag{2.4}$$

$$\Phi^{-1} : \mathcal{I}(\mathcal{O}) \to \mathcal{D}_S,\ \ \mathfrak{f} \mapsto \sum_{\mathfrak{p} \notin S} m_{\mathfrak{p}}\mathfrak{p}\ \ , \tag{2.5}$$

where $m_{\mathfrak{p}} = \min\{v_{\mathfrak{p}}(\alpha) \mid \alpha \in \mathfrak{f} \setminus \{0\}\}$.

$$\Psi : \mathcal{D}_0 \to \mathcal{I}(\mathcal{O}),\ \ D = D_S - \deg(D_S)\infty_0 \mapsto \Phi(D_S)$$

The Divisor-Theoretic Foundation of Infrastructures

Case $r = 1$:

- $\mathcal{O}^* = \langle \eta \rangle$, $\deg(\eta) > 0$
- $\mathcal{D}_0^S = \langle \infty_1 - 2\infty_0 \rangle \cong \mathbb{Z}$
- $\mathcal{P}^S = \langle \mathrm{div}(\eta) \rangle = \left\langle R^S(\infty_1 - 2\infty_0) \right\rangle \cong \Lambda = R^S\mathbb{Z} \subseteq \mathbb{Z}$
- $\mathcal{D}_0^S / \mathcal{P}^S \cong \mathbb{Z}/\Lambda$ is a circle.

Case $r = 2$:

- $\mathcal{O}^* = \langle \eta_1, \eta_2 \rangle$
- $\{\eta_1, \eta_2\}$ found via HNF from any $\{\epsilon_1, \epsilon_2\}$
- $\mathcal{D}_0^S = \langle \infty_1 - \infty_0, \infty_0 - \infty_2 \rangle \cong \mathbb{Z}^2$
- $\mathcal{P}^S = \langle \mathrm{div}(\eta_1), \mathrm{div}(\eta_2) \rangle \cong \Lambda \subseteq \mathbb{Z}^2$
- $\mathcal{D}_0^S / \mathcal{P}^S \cong \mathbb{Z}^2/\Lambda$ is a torus.

The Divisor-Theoretic Foundation of Infrastructures

From [Schmidt, 1931]:

$$(0) \to \mathcal{D}_0^S/\mathcal{P}^S \to \mathcal{J}_K \to Cl(\mathcal{O}) \to \mathbb{Z}/f\mathbb{Z} \to (0) \qquad (2.6)$$

$f = \mathrm{gcd}(\mathrm{deg}(\infty_0), \ldots, \mathrm{deg}(\infty_r))$

$$fh = R^S h_x \quad .$$

In our cases, $f = 1$, so

$$(0) \to \mathcal{D}_0^S/\mathcal{P}^S \to \mathcal{J}_K \to Cl(\mathcal{O}) \to (0) \quad .$$

Reduced Divisors

Definition (Sections 2.5.4 and 3.3.1)

- A divisor $D \in \mathcal{D}$ is *finitely effective* if $D_S \geq 0$.
- A finitely effective divisor $D \in \mathcal{D}$ is *semi-reduced* if there is no non-empty subsum of D_S of the form $\text{div}(a(x))_S$ for some $a(x) \in \mathbb{F}_q[x] \setminus \mathbb{F}_q$.
- A semi-reduced divisor $D \in \mathcal{D}$ is called *reduced* if $\deg(D^+) \leq g$

An ideal $\mathfrak{a}$ is primitive iff $\Phi^{-1}(\mathfrak{a})$ is semi-reduced.

Distinguished Divisors

Definition (Definitions 3.3.5 and 3.3.10)

Let $K = K_x$ be a cubic function field such that $\deg(\infty_i) = 1$. We call a finitely effective divisor $D \in \mathcal{D}_0$ *i-distinguished* if

- D is of the form $D = D^+ - \deg(D^+)\infty_i$, and
- for any other divisor $E = E^+ - \deg\left(E^+\right)\infty_i \in \mathcal{D}_0$ equivalent to D, such that $\deg\left(E^+\right) \leq \deg\left(D^+\right)$, we have $D = E$.

We call D *distinguished* if $\deg(\infty_0) = 1$ and

- D is of the form $D = D_S - \deg(D_S)\infty_0$, and
- for any other finitely effective divisor $E \sim D$, such that $\deg\left(E_S\right) \leq \deg\left(D_S\right)$ and $E^S \geq D^S$, we have $D = E$.

Reduced and Distinguished Ideals

Definition (Definitions 3.3.5 and 3.3.10 and Lemma 3.3.11)

- An ideal $\mathfrak{a}$ is *reduced*, *distinguished*, or *i-distinguished* if $\Psi^{-1}(\mathfrak{a})$ is.
- A fractional ideal $\mathfrak{f}$ is *reduced*, *distinguished*, or *i-distinguished* if $-\Psi^{-1}(\mathfrak{f})$ is.

Results on ($i-$)Distinguished Divisors

Theorem (Lemma 3.3.12 and Theorem 3.3.15)

If $K = K_x$ is a cubic function field such that $\deg(\infty_0) = 1$, *then there is a hierarchy of divisors:*
distinguished $\implies$ *0-distinguished* $\implies$ *reduced* $\implies$ *semi-reduced* $\implies$ *finitely effective.*

Theorem (Theorem 3.3.16)

If $K = K_x$ is a cubic function field such that $\deg(\infty_i) = 1$, *for some $\infty_i \in S$, then every divisor class of $\mathcal{D}_0$ contains a unique i-distinguished divisor.*

Proof of Theorem 3.3.16 (Sketch)

- Each divisor class contains a reduced divisor of the form: $E = E^{+} - \deg(E^{+})\infty_i$ (Lemma 3.3.4).

Proof of Theorem 3.3.16 (Sketch)

- Each divisor class contains a reduced divisor of the form: $E = E^+ - \deg(E^+)\infty_i$ (Lemma 3.3.4).
- If E is principal, then $E \sim 0$; done.

Proof of Theorem 3.3.16 (Sketch)

- Each divisor class contains a reduced divisor of the form: $E = E^+ - \deg(E^+)\infty_i$ (Lemma 3.3.4).
- If E is principal, then $E \sim 0$; done.
- If E is not principal, then $\dim_{\mathbb{F}_q}(L(E)) = l(E) = 0$.

Proof of Theorem 3.3.16 (Sketch)

- Each divisor class contains a reduced divisor of the form: $E = E^+ - \deg(E^+)\infty_i$ (Lemma 3.3.4).
- If E is principal, then $E \sim 0$; done.
- If E is not principal, then $\dim_{\mathbb{F}_q}(L(E)) = l(E) = 0$.
- Set $E_m := E + m\infty_i$, for $m \in \mathbb{N}$.

Proof of Theorem 3.3.16 (Sketch)

- Each divisor class contains a reduced divisor of the form: $E = E^+ - \deg(E^+)\infty_i$ (Lemma 3.3.4).
- If E is principal, then $E \sim 0$; done.
- If E is not principal, then $\dim_{\mathbb{F}_q}(L(E)) = l(E) = 0$.
- Set $E_m := E + m\infty_i$, for $m \in \mathbb{N}$.
- $0 = l(E) = l(E_0) \leq l(E_1) \leq l(E_2) \leq \dots$

Proof of Theorem 3.3.16 (Sketch)

- Each divisor class contains a reduced divisor of the form: $E = E^+ - \deg(E^+)\infty_i$ (Lemma 3.3.4).
- If E is principal, then $E \sim 0$; done.
- If E is not principal, then $\dim_{\mathbb{F}_q}(L(E)) = l(E) = 0$.
- Set $E_m := E + m\infty_i$, for $m \in \mathbb{N}$.
- $0 = l(E) = l(E_0) \leq l(E_1) \leq l(E_2) \leq \dots$
- Use Riemann-Roch to show $0 \leq l(E_{m+1}) - l(E_m) \leq 1$.

Proof of Theorem 3.3.16 (Sketch)

- Since E is reduced, via Riemann-Roch: $l(E_g) \geq 1$.

Proof of Theorem 3.3.16 (Sketch)

- Since E is reduced, via Riemann-Roch: $l(E_g) \geq 1$.
- There is minimal $0 < m \leq g$ with $0 \leq l(E_{m-1}) < l(E_m) = 1$.

Proof of Theorem 3.3.16 (Sketch)

- Since E is reduced, via Riemann-Roch: $l(E_g) \geq 1$.
- There is minimal $0 < m \leq g$ with $0 \leq l(E_{m-1}) < l(E_m) = 1$.
- $L(E_m) = \mathbb{F}_q\alpha$, for some $\alpha \in K^*$, so $\mathrm{div}(\alpha) \geq -E_m$.

Proof of Theorem 3.3.16 (Sketch)

- Since E is reduced, via Riemann-Roch: $l(E_g) \geq 1$.
- There is minimal $0 < m \leq g$ with $0 \leq l(E_{m-1}) < l(E_m) = 1$.
- $L(E_m) = \mathbb{F}_q\alpha$, for some $\alpha \in K^*$, so $\mathrm{div}(\alpha) \geq -E_m$.
- $D := E + \mathrm{div}(\alpha)$, $D \sim E$, $D^+ = D + m\infty_i$, $\deg(D^+) = m$

Proof of Theorem 3.3.16 (Sketch)

- Since E is reduced, via Riemann-Roch: $l(E_g) \geq 1$.
- There is minimal $0 < m \leq g$ with $0 \leq l(E_{m-1}) < l(E_m) = 1$.
- $L(E_m) = \mathbb{F}_q\alpha$, for some $\alpha \in K^*$, so $\mathrm{div}(\alpha) \geq -E_m$.
- $D := E + \mathrm{div}(\alpha)$, $D \sim E$, $D^+ = D + m\infty_i$, $\deg(D^+) = m$
- Apply the definition to show that D is i-distinguished. $\square$

Infrastructure

Definition (Definition 3.4.1)

If $K = \mathbb{F}_q(C)$ is a cubic function field with $r > 0$, $\mathcal{O} = \mathbb{F}_q[C]$, and $\mathbf{C} \in Cl(\mathcal{O})$, then

$$\mathcal{R}_{\mathbf{C}} = \{D \in \mathcal{D}_0 \mid D \text{ is distinguished and } \Psi(D) \in \mathbf{C}\}$$

is the *infrastructure* of $\mathbf{C}$.

$\mathcal{R} = \mathcal{R}_{[\mathcal{O}]}$ is the *(principal) infrastructure* of K.

- If $D_1 \in \mathcal{R}_{\mathbf{C}_1}$ and $D_2 \in \mathcal{R}_{\mathbf{C}_2}$, then $D_1 \nsim D_2$.

Results on $(i-)$Distinguished Divisors

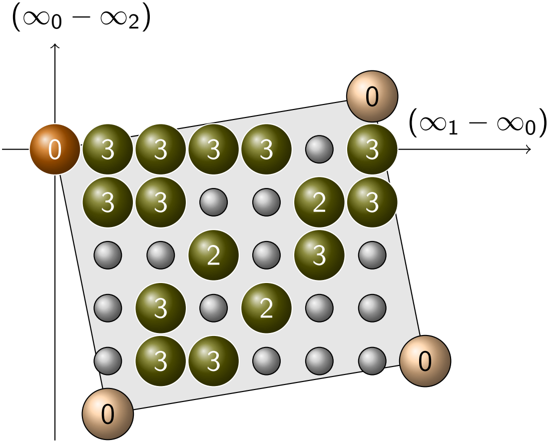
Theorem (Theorem 3.3.18)

If $\deg(\infty_i) = 1$, then for each ideal class $\mathbf{C} \in Cl(\mathcal{O})$, there is a one-to-one correspondence between the i-distinguished divisors, D, with $\Psi(D) \in \mathbf{C}$ and the elements of $\mathcal{D}_0^S / \mathcal{P}^S$.

Allows us to:

- establish the distance measure on $\mathcal{R}_{\mathbf{C}}$ for $r = 2$,
- improve bounds on the baby step operation, and
- identify the structure of infrastructures.

$\mathcal{R} = \mathcal{R}(\mathbb{F}_7(C)),\ C : Y^3 = x^6 + x^5 + x^4 - 2x^3 + x^2,\ r = 2$



Divisors:

0: identity of $\mathcal{R}$

nontrivial units

distinguished

0-**distinguished**

3 $\deg(D_S),\ D \in \mathcal{R}$

$g = 3$

$R^S = |\mathcal{D}_0^S/\mathcal{P}^S| = 31$

$|\mathcal{R}| = 16$

$h = 279,\ h_x = 9$

Properties

Proposition (Proposition 3.4.3)

If $D \in \mathcal{R}_{\mathbf{C}}$, then $\deg(D_S) \leq g$ and this bound is sharp.

Proposition (Proposition 3.4.4)

$|\mathcal{R}_{\mathbf{C}}| \leq R^S$

Minima and Infrastructures

Definition (Section 3.3.2)

The *normed body* of θ in $\mathfrak{f}$ is

$$\mathcal{N}_{\mathfrak{f}}(\theta) = \left\{\alpha \in \mathfrak{f} \setminus \{0\} \mid \operatorname{div}(\alpha)^S \geq \operatorname{div}(\theta)^S\right\} \cup \{0\} \tag{3.5}$$

If $\mathcal{N}_{\mathfrak{f}}(\theta) = \mathbb{F}_q\theta$, then θ is called a *minimum* in $\mathfrak{f}$.

Theorem (Theorem 3.3.7)

$\mathfrak{f}$ is distinguished iff 1 is a minimum in $\mathfrak{f}$.

- Correspondence between divisor- and ideal-theoretic definitions of $\mathcal{R}$.

Proof of Theorem 3.3.7, $\Rightarrow$

Theorem (Theorem 3.3.7)

$\mathfrak{f}$ *is distinguished iff* 1 *is a minimum in* $\mathfrak{f}$.

- Suppose that $\mathfrak{f}$ is distinguished, $D := -\Psi^{-1}(\mathfrak{f})$.

Proof of Theorem 3.3.7, $\Rightarrow$

Theorem (Theorem 3.3.7)

$\mathfrak{f}$ *is distinguished iff* 1 *is a minimum in* $\mathfrak{f}$.

- Suppose that $\mathfrak{f}$ is distinguished, $D := -\Psi^{-1}(\mathfrak{f})$.
- Choose $\alpha \in \mathfrak{f}$ with $\operatorname{div}(\alpha)^S \geq 0$, so $\alpha \in \mathcal{N}_{\mathfrak{f}}(1)$.

Proof of Theorem 3.3.7, $\Rightarrow$

Theorem (Theorem 3.3.7)

$\mathfrak{f}$ is distinguished iff 1 is a minimum in $\mathfrak{f}$.

- Suppose that $\mathfrak{f}$ is distinguished, $D := -\Psi^{-1}(\mathfrak{f})$.
- Choose $\alpha \in \mathfrak{f}$ with $\mathrm{div}(\alpha)^S \geq 0$, so $\alpha \in \mathcal{N}_{\mathfrak{f}}(1)$.
- If $E = D + \mathrm{div}(\alpha)$, then $E^S = D^S + \mathrm{div}(\alpha)^S \geq D^S$.

Proof of Theorem 3.3.7, $\Rightarrow$

Theorem (Theorem 3.3.7)

$\mathfrak{f}$ is distinguished iff 1 is a minimum in $\mathfrak{f}$.

- Suppose that $\mathfrak{f}$ is distinguished, $D := -\Psi^{-1}(\mathfrak{f})$.
- Choose $\alpha \in \mathfrak{f}$ with $\mathrm{div}(\alpha)^S \geq 0$, so $\alpha \in \mathcal{N}_{\mathfrak{f}}(1)$.
- If $E = D + \mathrm{div}(\alpha)$, then $E^S = D^S + \mathrm{div}(\alpha)^S \geq D^S$.
- $\deg(\mathrm{div}(\alpha)_S) \leq 0$, so $\deg(E_S) \leq \deg(D_S)$.

Proof of Theorem 3.3.7, $\Rightarrow$

Theorem (Theorem 3.3.7)

$\mathfrak{f}$ *is distinguished iff* 1 *is a minimum in* $\mathfrak{f}$.

- Suppose that $\mathfrak{f}$ is distinguished, $D := -\Psi^{-1}(\mathfrak{f})$.
- Choose $\alpha \in \mathfrak{f}$ with $\operatorname{div}(\alpha)^S \geq 0$, so $\alpha \in \mathcal{N}_{\mathfrak{f}}(1)$.
- If $E = D + \operatorname{div}(\alpha)$, then $E^S = D^S + \operatorname{div}(\alpha)^S \geq D^S$.
- $\deg(\operatorname{div}(\alpha)_S) \leq 0$, so $\deg(E_S) \leq \deg(D_S)$.
- D distinguished implies $E = D$, so $\operatorname{div}(\alpha) = 0$ and $\alpha \in \mathbb{F}_q^*$.

Proof of Theorem 3.3.7, $\Rightarrow$

Theorem (Theorem 3.3.7)

$\mathfrak{f}$ is distinguished iff 1 is a minimum in $\mathfrak{f}$.

- Suppose that $\mathfrak{f}$ is distinguished, $D := -\Psi^{-1}(\mathfrak{f})$.
- Choose $\alpha \in \mathfrak{f}$ with $\mathrm{div}(\alpha)^S \geq 0$, so $\alpha \in \mathcal{N}_{\mathfrak{f}}(1)$.
- If $E = D + \mathrm{div}(\alpha)$, then $E^S = D^S + \mathrm{div}(\alpha)^S \geq D^S$.
- $\deg(\mathrm{div}(\alpha)_S) \leq 0$, so $\deg(E_S) \leq \deg(D_S)$.
- D distinguished implies $E = D$, so $\mathrm{div}(\alpha) = 0$ and $\alpha \in \mathbb{F}_q^*$.
- 1 is a minimum in $\mathfrak{f}$.

Proof of Theorem 3.3.7, $\Leftarrow$

Theorem (Theorem 3.3.7)

$\mathfrak{f}$ *is distinguished iff* 1 *is a minimum in* $\mathfrak{f}$.

- Suppose that 1 is a minimum in $\mathfrak{f}$.

Proof of Theorem 3.3.7, $\Leftarrow$

Theorem (Theorem 3.3.7)

$\mathfrak{f}$ is distinguished iff 1 is a minimum in $\mathfrak{f}$.

- Suppose that 1 is a minimum in $\mathfrak{f}$.
- Suppose $E \sim D$ with $\deg(E_S) \leq \deg(D_S)$ and $E^S \geq D^S$.

Proof of Theorem 3.3.7, $\Leftarrow$

Theorem (Theorem 3.3.7)

$\mathfrak{f}$ is distinguished iff 1 is a minimum in $\mathfrak{f}$.

- Suppose that 1 is a minimum in $\mathfrak{f}$.
- Suppose $E \sim D$ with $\deg(E_S) \leq \deg(D_S)$ and $E^S \geq D^S$.
- $E = D + \operatorname{div}(\alpha)$, for some $\alpha \in K^*$.

Proof of Theorem 3.3.7, $\Leftarrow$

Theorem (Theorem 3.3.7)

$\mathfrak{f}$ is distinguished iff 1 is a minimum in $\mathfrak{f}$.

- Suppose that 1 is a minimum in $\mathfrak{f}$.
- Suppose $E \sim D$ with $\deg(E_S) \leq \deg(D_S)$ and $E^S \geq D^S$.
- $E = D + \mathrm{div}(\alpha)$, for some $\alpha \in K^*$.
- $\mathrm{div}(\alpha)^S = E^S - D^S \geq 0$ and $0 \leq E_S = D_S + \mathrm{div}(\alpha)_S$.

Proof of Theorem 3.3.7, $\Leftarrow$

Theorem (Theorem 3.3.7)

$\mathfrak{f}$ *is distinguished iff* 1 *is a minimum in* $\mathfrak{f}$*.*

- Suppose that 1 is a minimum in $\mathfrak{f}$.
- Suppose $E \sim D$ with $\deg(E_S) \leq \deg(D_S)$ and $E^S \geq D^S$.
- $E = D + \operatorname{div}(\alpha)$, for some $\alpha \in K^*$.
- $\operatorname{div}(\alpha)^S = E^S - D^S \geq 0$ and $0 \leq E_S = D_S + \operatorname{div}(\alpha)_S$.
- $\operatorname{div}(\alpha)_S \geq -D_S = \Phi^{-1}(\mathfrak{f})$, $\alpha \in \mathfrak{f}$, and $\alpha \in \mathcal{N}_{\mathfrak{f}}(1)$.

Proof of Theorem 3.3.7, $\Leftarrow$

Theorem (Theorem 3.3.7)

$\mathfrak{f}$ is distinguished iff 1 is a minimum in $\mathfrak{f}$.

- Suppose that 1 is a minimum in $\mathfrak{f}$.
- Suppose $E \sim D$ with $\deg(E_S) \leq \deg(D_S)$ and $E^S \geq D^S$.
- $E = D + \operatorname{div}(\alpha)$, for some $\alpha \in K^*$.
- $\operatorname{div}(\alpha)^S = E^S - D^S \geq 0$ and $0 \leq E_S = D_S + \operatorname{div}(\alpha)_S$.
- $\operatorname{div}(\alpha)_S \geq -D_S = \Phi^{-1}(\mathfrak{f})$, $\alpha \in \mathfrak{f}$, and $\alpha \in \mathcal{N}_{\mathfrak{f}}(1)$.
- $\alpha \in \mathbb{F}_q^*$, so $\operatorname{div}(\alpha) = 0$ and $E = D$.

Proof of Theorem 3.3.7, $\Leftarrow$

Theorem (Theorem 3.3.7)

$\mathfrak{f}$ is distinguished iff 1 *is a minimum in* $\mathfrak{f}$*.*

- Suppose that 1 is a minimum in $\mathfrak{f}$.
- Suppose $E \sim D$ with $\deg(E_S) \leq \deg(D_S)$ and $E^S \geq D^S$.
- $E = D + \operatorname{div}(\alpha)$, for some $\alpha \in K^*$.
- $\operatorname{div}(\alpha)^S = E^S - D^S \geq 0$ and $0 \leq E_S = D_S + \operatorname{div}(\alpha)_S$.
- $\operatorname{div}(\alpha)_S \geq -D_S = \Phi^{-1}(\mathfrak{f})$, $\alpha \in \mathfrak{f}$, and $\alpha \in \mathcal{N}_{\mathfrak{f}}(1)$.
- $\alpha \in \mathbb{F}_q^*$, so $\operatorname{div}(\alpha) = 0$ and $E = D$.
- D, and hence $\mathfrak{f}$, is distinguished. $\square$

Distance: A Measure on $\mathcal{R}_{\mathbf{C}}$

- Fix $E \in \mathcal{R}_{\mathbf{C}}$ and let $\mathfrak{b} = \Psi(E)$. If $\mathbf{C} = [\mathcal{O}]$, then $E = 0$.
- If $D \in \mathcal{R}_{\mathbf{C}}$ and $\mathfrak{a} = \Psi(D)$, then $\mathfrak{a} = \langle \alpha \rangle \, \mathfrak{b}$ for some $\alpha \in K^*$.
- Choose α so $\mathrm{div}(\alpha) = (D - E) + A_\infty$, where $A_\infty \in \mathcal{D}_0^S$ is "minimal" in $\mathcal{D}_0^S / \mathcal{P}^S$.

Definition (Section 3.4.2)

The *distance* of D with respect to E in $r = 1$ and $r = 2$, resp. is

$$\delta_E(D) := \delta_0(D) := \deg(\alpha)$$
$$\delta_E(D) := (\delta_0(D), \delta_1(D), \delta_2(D)) := \left(\deg(\alpha), \deg\left(\alpha'\right), \deg\left(\alpha''\right)\right)$$

Ideal Inversion, Section 4.3

Lemma (Lemma 4.3.3)

If $\mathfrak{a} = [s,\, s'(u+\rho),\, s''(v+w\rho+\omega)]$*, then*

$$\overline{\mathfrak{a}} = \langle s \rangle\, \mathfrak{a}^{-1} = [S,\, S'(U+\rho),\, S''(V+W\rho+\omega)] \ ,$$

$$S = s \ , \quad S' = \frac{s}{s' s_H} \ , \quad S'' = \frac{s_H}{s''} \ , \quad U \equiv -wH \pmod{\tfrac{S}{S'}} \ ,$$

$$W \equiv -ur_1 \pmod{S'} \ , \quad V \equiv -wWH - vs'' r_2 \pmod{\tfrac{S}{S''}} \ ,$$

$r_1 H \equiv 1 \pmod{S'}$, $r_2 s'' \equiv 1 \pmod{s/s_H}$*, and* $s_H = \gcd(s,\, H)$.

Example: Ideal Inversion, Section 4.3

$$K = \mathbb{F}_7(C),\ C : Y^3 = (x^4 + x^3 + x^2 - 2x^2 + 1)x^2$$

$$\mathfrak{a} = \left[(x^2 + 4x + 5),\ (x^2 + 4x + 5)\rho,\ (x + 6) + (3x + 3)\rho + \omega\right]$$

$$\overline{\mathfrak{a}} = \left[S,\ S'(U + \rho),\ S''(V + W\rho + \omega)\right]$$

$S = x^2 + 4x + 5,$
$S' = S'' = 1,$
$U \equiv -wH = 4x^2 + 4x \equiv 2x + 1 \pmod{S/S'},$
$W \equiv -ur_1 \equiv 0 \pmod{S'}$, and
$V \equiv -wWH - vs''r_2 \equiv 6x + 1 \pmod{S/S''}.$

$$\overline{\mathfrak{a}} = \left[(x^2 + 4x + 5),\ (2x + 1) + \rho,\ (6x + 1) + \omega\right] = \mathfrak{p}'$$

Example: Ideal Multiplication, Theorem 4.4.5

$K = \mathbb{F}_7(C),\ C : Y^3 = (x^4 + x^3 + x^2 - 2x^2 + 1)x^2$

$$\mathfrak{a}_1 = \left[(x^2 + 4x + 5),\ (x^2 + 4x + 5)\rho,\ (x + 6) + (3x + 3)\rho + \omega\right]$$
$$\mathfrak{a}_2 = \left[(x^2 + 4x + 5),\ (x^2 + 4x + 5)\rho,\ (4x + 3) + (6x + 6)\rho + \omega\right]$$

$$\mathfrak{a}_1\mathfrak{a}_2 = (\mathfrak{p}\mathfrak{p}'')(\mathfrak{p}\mathfrak{p}') = (\mathfrak{p}\mathfrak{p}'\mathfrak{p}'')\mathfrak{p} = \langle P \rangle\, \mathfrak{p}$$

$d'' = d_4 = d_5 = 1$
$d_1 = \gcd(s_1/(s_1' s_{1,H}),\ \ldots) = 1 = \gcd(s_2/(s_2' s_{2,H}),\ \ldots) = d_2$
$d_3 = \gcd(x^2+4x+5,\ x^2+4x+5,\ 4x^3+x^2+2x+2) = x^2+4x+5 = d$

$$\mathfrak{a}_1\mathfrak{a}_2 = \left\langle x^2 + 4x + 5 \right\rangle \mathfrak{a} = \left\langle x^2 + 4x + 5 \right\rangle \widetilde{\mathfrak{a}_1}\,\widetilde{\mathfrak{a}_2}\,\widetilde{\mathfrak{a}_3}$$

Example: Ideal Multiplication, Theorem 4.4.5

$$\mathfrak{a}_1\mathfrak{a}_2 = \left\langle x^2+4x+5\right\rangle \mathfrak{a} = \left\langle x^2+4x+5\right\rangle \widetilde{\mathfrak{a}_1}\widetilde{\mathfrak{a}_2}\widetilde{\mathfrak{a}_3}$$

$$\begin{aligned}
\widetilde{\mathfrak{a}_1} &= [1,\ \rho,\ (x+6)+(3x+3)\rho+\omega] = \mathcal{O} \\
\widetilde{\mathfrak{a}_2} &= [1,\ \rho,\ (4x+3)+(6x+6)\rho+\omega] = \mathcal{O} \\
\widetilde{\mathfrak{a}_3} &= \left[d_3 d'',\ (w_1+w_2)H+\rho,\ -w_1w_2H+\omega\right] \\
&= \left[x^2+4x+5,\ (2x^2+2x)+\rho,\ (3x^3+6x^2+3x)+\omega\right] \\
&= \left[x^2+4x+5,\ (x+4)+\rho,\ (5x+2)+\omega\right] = \mathfrak{p}
\end{aligned}$$

$$\begin{aligned}
\mathfrak{a}_1\mathfrak{a}_2 &= \left\langle x^2+4x+5\right\rangle \left[x^2+4x+5,\ (x+4)+\rho,\ (5x+2)+\omega\right] \\
&= \langle P\rangle\, \mathfrak{p}
\end{aligned}$$

Ideal Reduction for $r = 0$

Lemma (Lemma 4.5.6; Lemma 8 of [Galbraith, Paulus, Smart, 2008])

If α is the element in $\overline{\mathfrak{a}}$ whose norm has minimal degree, then $\langle\alpha\rangle/\overline{\mathfrak{a}}$ is the unique distinguished ideal in $[\mathfrak{a}]$.

Algorithm (Alg. 4.5.7, 10.1 of [Bauer, 2004]: *Reduce*($\mathfrak{a}$))

1. *Compute* $\overline{\mathfrak{a}}$.
2. *Find* $\alpha \in \overline{\mathfrak{a}}$ *with* $\deg(N(\alpha))$ *minimal.*
3. *Compute* $\langle\alpha\rangle = \langle d_1\rangle [s, s'(u+\rho), s''(v+w\rho+\omega)]$.
4. *Multiply* $\mathfrak{a}[s, s'(u+\rho), s''(v+w\rho+\omega)] = \langle d_2\rangle \mathfrak{b}$.
5. *Output* $\mathfrak{b}$.

Ideal Reduction for $r = 0$

Theorem (Theorem 4.5.2)

Every nonzero $\mathfrak{a}$ has a unique element, α, with $\deg(N(\alpha))$ minimal.

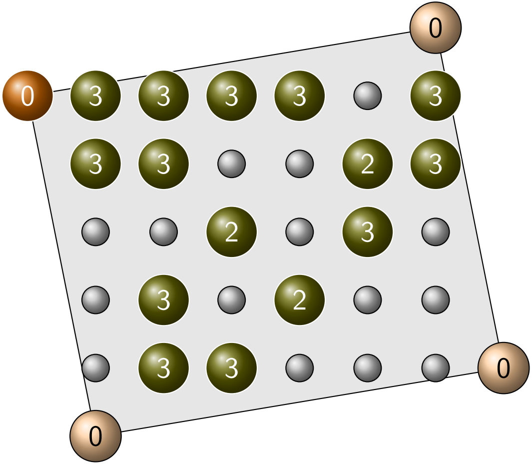
α is found via Algorithm 4.5.3.

Proposition (Proposition 4.5.5)

Algorithm 4.5.4 computes
$\langle \alpha \rangle = \langle d_1 \rangle [s, s'(u + \rho), s''(v + w\rho + \omega)]$.

These results generalize those of [Bauer, 2004] to all purely cubic function fields, K, with $\mathrm{char}(K) \neq 3$.

$\mathcal{R} = \mathcal{R}(\mathbb{F}_7(C)),\ C : Y^3 = x^6 + x^5 + x^4 - 2x^3 + x^2,\ r = 2$



Divisors:

0: identity of $\mathcal{R}$

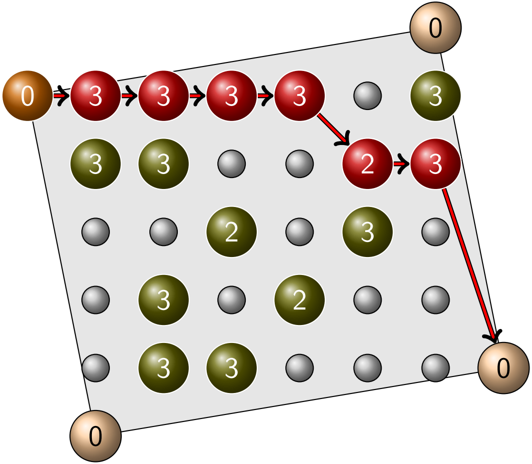
units

distinguished

0-**distinguished**

3 $\deg(D_S),\ D \in \mathcal{R}$

$\mathcal{R} = \mathcal{R}(\mathbb{F}_7(C)),\ C : Y^3 = x^6 + x^5 + x^4 - 2x^3 + x^2,\ r = 2$



Divisors:

units

0-**chain**

distinguished

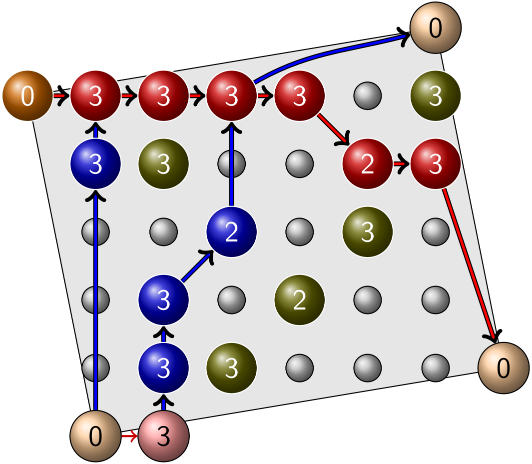
0-**distinguished**

3 $\deg(D_S),\ D \in \mathcal{R}$

Baby Steps:

0-**step**

$\mathcal{R} = \mathcal{R}(\mathbb{F}_7(C)),\ C : Y^3 = x^6 + x^5 + x^4 - 2x^3 + x^2,\ r = 2$



Divisors:

units

0-**chain**

2-**chain**

distinguished

0-**distinguished**

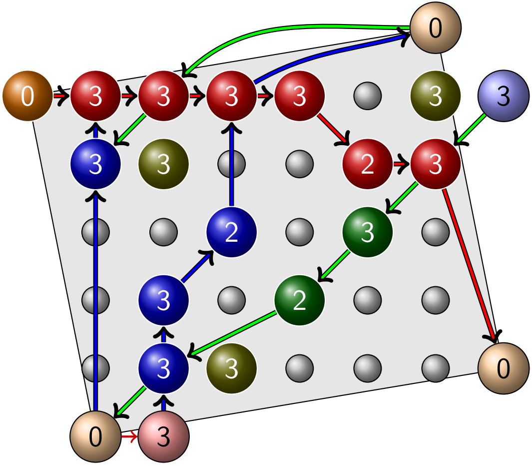
3 $\deg(D_S),\ D \in \mathcal{R}$

Baby Steps:

0-**step**

2-**step**

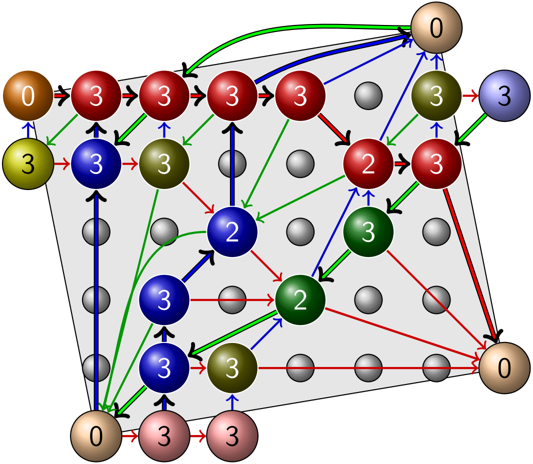
$\mathcal{R} = \mathcal{R}(\mathbb{F}_7(C))$, $C : Y^3 = x^6 + x^5 + x^4 - 2x^3 + x^2$, $r = 2$



Divisors:
units
0-chain
1-chain
2-chain
distinguished
0-distinguished
3 $\deg(D_S)$, $D \in \mathcal{R}$

Baby Steps:
0-step
1-step
2-step

$\mathcal{R} = \mathcal{R}(\mathbb{F}_7(C)),\ C : Y^3 = x^6 + x^5 + x^4 - 2x^3 + x^2,\ r = 2$



Divisors:
- units
- 0-chain
- 1-chain
- 2-chain
- distinguished
- 0-distinguished
- $\boxed{3}$ $\deg(D_S),\ D \in \mathcal{R}$

Baby Steps:
- 0-step
- 1-step
- 2-step

Degree Bounds on a Baby Step in $\mathcal{R}$

Theorem (Theorem 5.3.10)

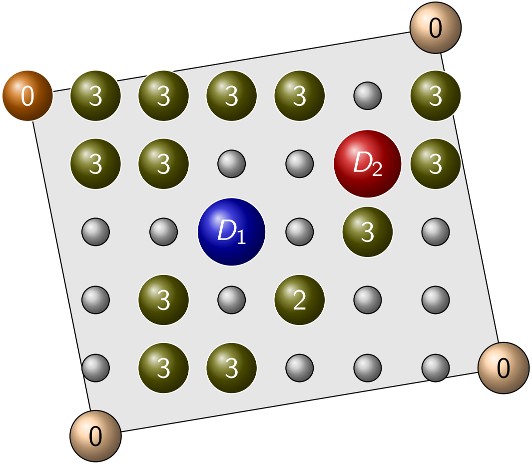
Let $D \in \mathcal{R}_{\mathbf{C}}$ *and* $E = bs_i(D)$*, for some* $i \in \{0, 1, 2\}$.
If $r = 1$*, then* $i = 0$ *and*

- $1 \leq \delta_D(E) \leq g + 2 - \deg(D_S) \leq g + 2$*; and*
- $\deg(D_S) \leq \deg(E_S) + 1 \Rightarrow \deg(E_S) - \deg(D_S) + 2 \leq \delta_D(E)$.

If $r = 2$*, then*

- $1 \leq \delta_{D,i}(E) \leq g + 1 - \deg(D_S) \leq g + 1$*; and*
- $\deg(D_S) \leq \deg(E_S) \Rightarrow \deg(E_S) - \deg(D_S) + 1 \leq \delta_{D,i}(E)$.

Giant Steps: Computing $D_1 \oplus D_2$ in $\mathcal{R}$



Divisors:

$D_1 = \mathfrak{p}' - 2\infty_0$

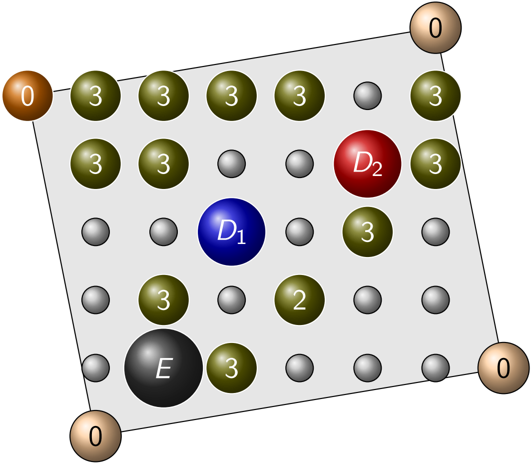
$D_2 = \mathfrak{p}'' - 2\infty_0$

Distances:

$\delta(D_1) = (7, -3, -2)$

$\delta(D_2) = (8, -5, -1)$

Giant Steps: Computing $D_1 \oplus D_2$ in $\mathcal{R}$



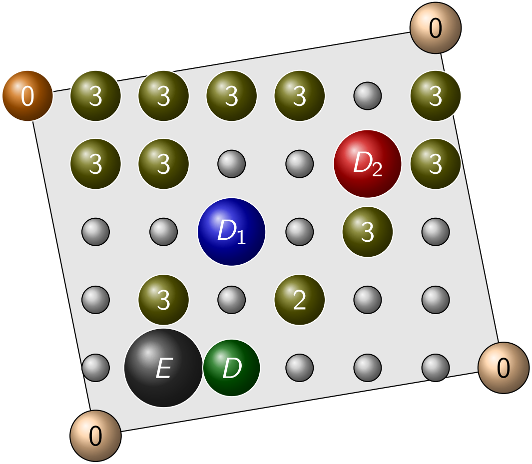
Divisors:

$D_1 = \mathfrak{p}' - 2\infty_0$
$D_2 = \mathfrak{p}'' - 2\infty_0$
$E = D_1 + D_2$
$E = \mathfrak{p}' + \mathfrak{p}'' - 4\infty_0$

Distances:

$\delta(D_1) = (7, -3, -2)$
$\delta(D_2) = (8, -5, -1)$
$\delta(D_1) + \delta(D_2) \sim (10, -2, -4)$

Giant Steps: Computing $D_1 \oplus D_2$ in $\mathcal{R}$



Divisors:

$D_1 = \mathfrak{p}' - 2\infty_0$
$D_2 = \mathfrak{p}'' - 2\infty_0$
$E = D_1 + D_2$
$E = \mathfrak{p}' + \mathfrak{p}'' - 4\infty_0$
$D = D_1 \oplus D_2$
$D = \mathfrak{q} - 3\infty_0$

Distances:

$\delta(D_1) = (7, -3, -2)$
$\delta(D_2) = (8, -5, -1)$
$\delta(D_1) + \delta(D_2) \sim (10, -2, -4)$
$\delta(D) = (10, -3, -4)$

Complexity of S-Regulator Computation via Baby Steps

Proposition (Proposition 6.1.6)

If $r = 1$, then Algorithm 6.1.5 (Algorithm 6.7 of [Scheidler, Stein, 2000]) requires at most $R^S = O(q^g)$ baby steps in $\mathcal{R}$ to compute R^S.

Proposition (Proposition 6.1.8)

If $r = 2$, then Algorithm 6.1.7 (Algorithm 6.1 of [Lee, Scheidler, Yarrish, 2003]) requires at most $2R^S = O(q^g)$ baby steps in $\mathcal{R}$ to compute R^S. The storage requirement is at most $R^S = O(q^g)$ divisors and at most $2R^S = O(q^g)$ integers.

Idea to Compute h and R^S, $r = 0$ or $r = 1$

Algorithm (Algorithm 6.3.1, [Scheidler and Stein, 2007])

1. *Compute E and U such that $h \in (E - U, E + U)$.*
2. *Determine extra information about h: congruences or distribution of h in $(E - U, E + U)$.*
3. *Search $(E - U, E + U)$ for h via the Baby Step-Giant Step or Kangaroo method.*
4. *If $r = 1$, then determine $R^S \mid h$: minimal with $D\left(2R^S\right) = 0$.*

- $D(n) \in \mathcal{R}$ with $\delta(D(n)) \leq n < \delta(bs(D(n)))$ (Alg. 5.3.26)

Step 1: Zeta Functions, Section 6.3.3

$$\zeta_K(s) = \sum_{D \in \mathcal{D}^+} q^{-\deg(D)s}$$

Let $u = q^{-s}$. Then:

$$\zeta_K(s) = Z_K(u) = \prod_{\mathfrak{P} \in \mathbb{P}_K} \frac{1}{1 - u^{\deg(\mathfrak{P})}} = \frac{L_K(u)}{(1-u)(1-qu)}$$

Write

$$Z_K(u) = Z_K^{\infty}(u) Z_K^{x}(u)$$

with

$$Z_K^{\infty}(u) = \prod_{i=0}^{r} \frac{1}{1 - u^{\deg(\infty_i)}} \quad \text{and} \quad Z_K^{x}(u) = \prod_{P} \prod_{\mathfrak{p} | \langle P \rangle} \frac{1}{1 - u^{\deg(\mathfrak{p})}}$$

Step 1: h and the L-Function, Section 6.3.3

$$
\begin{aligned}
h = L_K(1) &= q^g L_K(1/q) \\
&= \frac{q^{g+2}}{(q-x_1)(q-x_2)} \prod_{\nu=1}^{\infty} \prod_{\deg(P)=\nu} \frac{q^{2\nu}}{(q^\nu - z_1(P))(q^\nu - z_2(P))}
\end{aligned}
\tag{6.5}
$$

- x_1 and x_2 depend on the splitting of ∞.
- $z_1(P)$ and $z_2(P)$ depend on the splitting of $\langle P \rangle$.
- $P \in \mathbb{F}_q[x]$ is irreducible.

Step 1: h and the L-Function, Section 6.3.3

$$A(K) = \log\left(\frac{q^{g+2}}{(q-x_1)(q-x_2)}\right) = (g+2)\log(q) - \log(q^2 + s_1 q + s_2)$$

and

$$S_\nu(n) = \sum_{\deg(P)=\nu} \left(z_1^n(P) + z_2^n(P)\right)$$

Theorem (Theorem 6.3.4; Theorem 4.12 of [Scheidler, Stein, 2007])

$$\log(h) = A(K) + \sum_{n=1}^{\infty} \frac{1}{nq^n} \sum_{\nu | n} \nu S_\nu\left(\frac{n}{\nu}\right)$$

Step 1: Two Approximations of h, Section 6.3.4

Fix a degree bound, λ.

$$E_1 = \left\lceil \exp\left(A(K) + \sum_{n=1}^{\lambda} \frac{1}{nq^n} \sum_{\nu \mid n} \nu S_\nu \left(\frac{n}{\nu}\right) \right) \right\rfloor$$

$$E_2 = \left\lceil \exp\left(A(K) + \sum_{n=1}^{\infty} \frac{1}{nq^n} \sum_{\substack{\nu \mid n \\ \nu \le \lambda}} \nu S_\nu \left(\frac{n}{\nu}\right) \right) \right\rfloor$$

U_1, U_2, and U_3 bound the tail of the Euler product of h.

- E_2 is a slightly better estimate than E_1 in practice. (Table 6.3)

Phase 2: Distribution of h in $(E_i - U_i,\, E_i + U_i)$

- $\alpha_i(q, g) = Mean(|h - E_i|/U_i)$, over all cubic $K/\mathbb{F}_q(x)$ of genus g.
- $\alpha_i(q, g)$ is difficult to compute precisely.
- $\hat{\alpha}_i(q, g) = Mean_n(|h - E_i|/U_i)$, over a sampling of n such K:

q	g	λ	$\hat{\alpha}_1(q, g)$	$\hat{\alpha}_2(q, g)$	$\hat{\alpha}_3(q, g)$	n
100003	3	1	0.27227076	0.20408453	0.27187490	10000
10009	4	1	0.19252978	0.15379110	0.19186318	10000
997	5	2	0.19188423	0.18894457	0.19190607	10000
463	6	2	0.15992960	0.15676849	0.15975657	10000
97	7	2	0.12684120	0.12176623	0.12602172	10000

Phase 3: Baby Step-Giant Step and Kangaroo

- BS-GS is deterministic, requires time and storage $O\left(\sqrt{U}\right)$.
- Kangaroo is heuristic, expected time $O\left(\sqrt{U}\right)$, parallelizable, little storage by setting *traps* every θ steps on average.
- Expected times improve by using the $\hat{\alpha}_i(q, g)$.
- For BS-GS, can take advantage of faster inverses.
- In $Cl(\mathcal{O})$, can take advantage of congruences, $h \equiv a \pmod{b}$.
- In $\mathcal{R}$, can take advantage of faster baby steps.

Phase 3: Kangaroos in $\mathcal{R}$, $r = 1$

- $\tau_3 = T_G / T_B =$ giant step time/baby step time; $\tau_3 \approx g$.
- m processors

Under reasonable heuristic assumptions:

Proposition (Proposition 6.2.12)

The expected heuristic running time to compute a multiple, h_0, of R^S is minimized by choosing an average jump distance of $\beta = \left[m\sqrt{(2\tau - 1)\alpha U} \right] - 2(\tau - 1)$, where $\tau = \lfloor \tau_3 \rfloor$ or $\tau = \lceil \tau_3 \rceil$. The expected heuristic running time for each kangaroo is $\left((4/m)\sqrt{\alpha U/(2\tau - 1)} + \theta/\tau + O(1) \right) (1 + (\tau - 1)/\tau_3)\, T_G$.

Phase 4: Extracting R^S from h, $r = 1$

Algorithm (Algorithm 6.3.22; Algorithm 4.4 of [Stein, Williams, 1999])

Input: *A multiple, h_0 of R^S, a lower bound, l, of R^S.*
Output: R^S

1. *Set:* $h^* := 1$.
2. *Factor* $h_0 = \prod_{i=1}^{k} p_i^{a_i}$.
3. *For* $1 \leq i \leq k$*:*
   a. *If* $p_i < h_0/l$*, then:*
      i. *Find* $1 \leq e_i \leq a_i$ *minimal with* $D\left(2h_0/p_i^{e_i}\right) \neq 0$.
      ii. *Set* $h^* := p_i^{e_i - 1} h^*$.
4. *Output* h_0/h^*.

Complexity of Algorithm 6.3.1

"I like fast algorithms. They're kind of like sports cars for nerds." (Nate Wentzel)

Theorem ([Scheidler, Stein, 2007])

The complexity of Algorithm 6.3.1 is

$$O\left(q^{[(2g-1)/5]+\varepsilon(g)}\right)$$

ideal or infrastructure compositions, as $q \to \infty$, where

$$\varepsilon(g) = \begin{cases} 0 & \text{if } g \equiv 0, 3 \pmod{5}\ , \\ 1/4 & \text{if } g \equiv 1 \pmod{5}\ , \\ -1/4 & \text{if } g \equiv 2 \pmod{5}\ , \\ 1/2 & \text{if } g \equiv 4 \pmod{5}\ . \end{cases}$$

Comparison of the Running Times, Table 6.2

g	λ	H-W	*E-U*	H-W	*E-U*
1	0	$O\left(q^{1/4}\right)$	$O\left(q^{1/4}\right)$	$O\left(h^{0.25}\right)$	$O\left(h^{0.25}\right)$
2	0	$O\left(q^{3/4}\right)$	$O\left(q^{3/4}\right)$	$O\left(h^{0.375}\right)$	$O\left(h^{0.375}\right)$
3	1	$O\left(q^{5/4}\right)$	$O\left(q^{4/4}\right)$	$O\left(h^{0.417}\right)$	$O\left(h^{0.333}\right)$
4	1	$O\left(q^{7/4}\right)$	$O\left(q^{6/4}\right)$	$O\left(h^{0.438}\right)$	$O\left(h^{0.375}\right)$
5	2	$O\left(q^{9/4}\right)$	$O\left(q^{8/4}\right)$	$O\left(h^{0.45}\right)$	$O\left(h^{0.4}\right)$
6	2	$O\left(q^{11/4}\right)$	$O\left(q^{9/4}\right)$	$O\left(h^{0.458}\right)$	$O\left(h^{0.375}\right)$
7	2	$O\left(q^{13/4}\right)$	$O\left(q^{11/4}\right)$	$O\left(h^{0.464}\right)$	$O\left(h^{0.393}\right)$

- H-W: Hasse-Weil interval: $\left(\left(\sqrt{q}-1\right)^{2g},\ \left(\sqrt{q}+1\right)^{2g}\right)$
- *E-U*: uses the new interval $(E-U,\ E+U)$

Unit Rank 0 Results, Genus 3

The largest example required 27.2 hours using 18 kangaroos: 20.4 days of total machine time.

$$\begin{aligned} C_4 : Y^3 = x^4 &+ 512964174x^3 + 604076970x^2 \\ &+ 208417608x + 702771176 \end{aligned}$$

For the function field $\mathbb{F}_{10^9+9}(C_4)$:

$$\begin{aligned} h &= 1000020285132998304595632979 \\ &= 13 \cdot 19 \cdot 73 \cdot 114859 \cdot 482863041248304151 \end{aligned}$$

2880612442 jumps; $|h - E|/U = 0.0241890$

Unit Rank 0 Results, Genus 4

The largest example required 3.62 days using 20 kangaroos: 72.4 days of total machine time.

$$C_8 : Y^3 = x^5 + 537882x^4 + 755468x^3 + 137780x^2 + 366795x + 268815$$

For the function field $\mathbb{F}_{10^6+3}(C_8)$:

$$h = 1001264259802134080148796 = 2^2 \cdot 4549 \cdot 55026613530563534851$$

4872971415 jumps; $|h - E|/U = 0.3835040$

Unit Rank 1 Results, Genus 3

The largest example required 3.46 days using 20 kangaroos: 69.2 days of total machine time.

$$C_{14} : Y^3 = x^6 + 852737742x^5 + 113051170x^4 + 250054066x^3 + 513859851x^2$$

For the function field $\mathbb{F}_{10^9+7}(C_{14})$:

$$\begin{aligned} h = h_x R^S &= 12 \cdot 833333350639834005118671361 \\ &= 2^{10} \cdot 3^2 \cdot 7 \cdot 11 \cdot 109^2 \cdot 167 \cdot 710227281795313 \end{aligned}$$

3136227037 baby steps, 1568085553 giant steps;
$|h - E|/U = 0.0580483$

Unit Rank 1 Results, Genus 4

The largest example required 4.91 days using 18 kangaroos: 88.4 days of total machine time.

$$\begin{aligned} C_{18} : Y^3 = &\left(x^3 + 918037x^2 + 460902x + 923544\right) \\ &\cdot \left(x^3 + 891576x^2 + 694204x + 79732\right)^2 \end{aligned}$$

For the function field $\mathbb{F}_{10^6+37}(C_{18})$:

$$\begin{aligned} h = h_x R^S &= 9 \cdot 11112779170481599571357 7 \\ &= 3^5 \cdot 25603 \cdot 160756322978377817 \end{aligned}$$

3127164698 baby steps, 1042434250 giant steps;
$|h - E|/U = 0.4230388$

Projected Running Times to compute h, $r = 0$

q	g	Phase 1	Phase 3	Exp. time	Exp. Jumps
$10^{10} + 33$	3	$7.92\,d$	$142.\,d$	$150.\,d$	$2.086 \cdot 10^{10}$
$10^{11} + 3$	3	$83.8\,d$	$3.90\,y$	$4.13\,y$	$2.086 \cdot 10^{11}$
$10^{12} + 39$	3	$2.43\,y$	$39.0\,y$	$41.4\,y$	$2.086 \cdot 10^{12}$
$10^{7} + 141$	4	$9.21\,m$	$951.\,d$	$951.\,d$	$6.398 \cdot 10^{10}$
$10^{8} + 39$	4	$1.69\,h$	$82.4\,y$	$82.4\,y$	$2.023 \cdot 10^{12}$
$10^{9} + 9$	4	$17.9\,h$	$2604\,y$	$2604\,y$	$6.398 \cdot 10^{13}$

- Program uses C++ with NTL
- Sun workstation, AMD Opteron 148 2.2 GHz processor, 1 GB RAM

Projected Running Times to compute R^S, $r = 1$

q	g	τ	Exp. Time	Exp. Jumps	$\lg\theta$	Exp. Traps
$10^{10}+19$	3	3	$714.\,d$	$4.846 \cdot 10^{10}$	24	2888
$10^{11}+19$	3	3	$19.6\,y$	$4.846 \cdot 10^{11}$	26	7221
$10^{12}+61$	3	3	$196.\,y$	$4.846 \cdot 10^{12}$	28	18053
$10^{7}+19$	4	4	$9.76\,y$	$1.675 \cdot 10^{11}$	24	9984
$10^{8}+7$	4	4	$309.\,y$	$5.296 \cdot 10^{12}$	26	88662
$10^{9}+7$	4	4	$9762\,y$	$1.675 \cdot 10^{14}$	28	623986

- Times for Phases 1, 2, and 4 are negligible compared with the expected running times.

Summary of Main Results

- Characterization of unique divisor class representatives
- Divisor-theoretic description of $\mathcal{R}_{\mathbf{C}}$; correspondence with ideal-theoretic constructions
- Improved bounds on baby steps, reduction, elements of $\mathcal{R}_{\mathbf{C}}$, and $|\mathcal{R}_{\mathbf{C}}|$
- Complete description of ideal multiplication and inversion for $\mathrm{char}(K) \neq 3$
- Ideal reduction in $Cl(\mathcal{O})$ for $\mathrm{sig}(K) = (3, 1)$
- Reduction and giant steps in $\mathcal{R}$ for $\mathrm{char}(K) \geq 5$ and $r = 2$
- Improvement to the Kangaroo method in $\mathcal{R}$
- Methods to extract R^S from h for $r = 1$
- Computation of 28-digit divisor class numbers, $g = 3$
- Computation of 25-digit divisor class numbers, $g = 4$

Future Work

- Extend Baby Step-Giant Step and Kangaroo methods to $r = 2$
- Implement Index Calculus methods [Thériault, 2003; Diem, 2006; Diem and Thomé, 2008]
- Develop faster arithmetic [Flon and Oyono, 2004; Khuri-Makdisi, 2004, 2007; Galbraith, Harrison, and Mireles, 2008]
- Speed up Pollard's Rho Method via baby steps in $\mathcal{R}$.
- Study periods of $\mathcal{R}$ for $r = 2$
- Study infrastructures of higher degree function fields
- Arithmetic of general cubic function fields
- Infrastructures of K with $\mathrm{sig}(K) = (1, 1; 2, 1)$
- Characteristic 2 and 3

Acknowledgments

Thank you!

- Advisor: Prof. Scheidler
- Committee: Prof. Duursma, Prof. McCullough, Prof. Ullom, Prof. Zaharescu
- Assistance: CISaC (Calgary) and Prof. Stein (Oldenburg)
- Friends and colleagues in attendance
- Mom R. and Dad R.
- Mom and Dad
- Bethany