Shorter Compact Representations on Hyperelliptic Curves

Renate Scheidler

UNIVERSITY OF CALGARY

West Coast Number Theory Conference

December 16, 2013

Shorter Compact Representations on Hyperelliptic Curves

Renate Scheidler

UNIVERSITY OF CALGARY

West Coast Number Theory Conference

December 16, 2013

Work in Progress

Differences to Previous Talk

Differences to Previous Talk

In a nutshell, replace

- $\mathbb{Z}$ by $\mathbb{F}_q[x]$ (i.e. rational integers by polynomials)
- $\mathbb{Q}$ by $\mathbb{F}_q(x)$ (i.e. rational numbers by rational functions)
- log by deg

where $\mathbb{F}_q$ is a finite field.

Differences to Previous Talk

In a nutshell, replace

- $\mathbb{Z}$ by $\mathbb{F}_q[x]$ (i.e. rational integers by polynomials)
- $\mathbb{Q}$ by $\mathbb{F}_q(x)$ (i.e. rational numbers by rational functions)
- $\log$ by $\deg$

where $\mathbb{F}_q$ is a finite field.

Assume q is odd and let $\Delta(x) \in \mathbb{F}_q[x]$ be monic of even degree:

$$\Delta(x) = x^{2m} + a_{2m-1}x^{2m-1} + \cdots + a_0 \qquad (a_i \in \mathbb{F}_q)$$
$$\implies \sqrt{\Delta(x)} = \pm(x^m + b_{m-1}x^{m-1} + \cdots + b_0 + b_{-1}x^{-1} + b_{-2}x^{-2} + \cdots)$$

with $b_i \in \mathbb{F}_q$.

In a nutshell, replace

- $\mathbb{Z}$ by $\mathbb{F}_q[x]$ (i.e. rational integers by polynomials)
- $\mathbb{Q}$ by $\mathbb{F}_q(x)$ (i.e. rational numbers by rational functions)
- log by deg

where $\mathbb{F}_q$ is a finite field.

Assume q is odd and let $\Delta(x) \in \mathbb{F}_q[x]$ be monic of even degree:

$$\Delta(x) = x^{2m} + a_{2m-1}x^{2m-1} + \cdots + a_0 \qquad (a_i \in \mathbb{F}_q)$$
$$\Longrightarrow \sqrt{\Delta(x)} = \pm(x^m + b_{m-1}x^{m-1} + \cdots + b_0 + b_{-1}x^{-1} + b_{-2}x^{-2} + \cdots)$$

with $b_i \in \mathbb{F}_q$. This defines $\deg(\sqrt{\Delta}) = m$ and $|\sqrt{\Delta}| = q^m$.

Differences to Previous Talk

In a nutshell, replace

- $\mathbb{Z}$ by $\mathbb{F}_q[x]$ (i.e. rational integers by polynomials)
- $\mathbb{Q}$ by $\mathbb{F}_q(x)$ (i.e. rational numbers by rational functions)
- log by deg

where $\mathbb{F}_q$ is a finite field.

Assume q is odd and let $\Delta(x) \in \mathbb{F}_q[x]$ be monic of even degree:

$$\Delta(x) = x^{2m} + a_{2m-1}x^{2m-1} + \cdots + a_0 \qquad (a_i \in \mathbb{F}_q)$$
$$\Longrightarrow \sqrt{\Delta(x)} = \pm(x^m + b_{m-1}x^{m-1} + \cdots + b_0 + b_{-1}x^{-1} + b_{-2}x^{-2} + \cdots)$$

with $b_i \in \mathbb{F}_q$. This defines $\deg(\sqrt{\Delta}) = m$ and $|\sqrt{\Delta}| = q^m$.

Fixing a square root, it also defines $\deg(a + b\sqrt{\Delta})$ for $a, b \in \mathbb{F}_q(x)$.

Quadratic Function Fields and Hyperelliptic Curves

Let q be odd and $\Delta \in \mathbb{F}_q[x]$ is monic and square-free.

Quadratic function field: $K = \mathbb{F}_q(x)(\sqrt{\Delta}) = \{a + b\sqrt{\Delta} \mid a, b \in \mathbb{F}_q(x)\}$

Maximal order of K: $\mathcal{O} = \mathbb{F}_q[x][\sqrt{\Delta}] = \{a + b\sqrt{\Delta} \mid a, b \in \mathbb{F}_q[x]\}$

Quadratic Function Fields and Hyperelliptic Curves

Let q be odd and $\Delta \in \mathbb{F}_q[x]$ is monic and square-free.

Quadratic function field: $K = \mathbb{F}_q(x)(\sqrt{\Delta}) = \{a + b\sqrt{\Delta} \mid a, b \in \mathbb{F}_q(x)\}$
Maximal order of K**:** $\mathcal{O} = \mathbb{F}_q[x][\sqrt{\Delta}] = \{a + b\sqrt{\Delta} \mid a, b \in \mathbb{F}_q[x]\}$

$$K \text{ is } \begin{cases} \textbf{imaginary} & \text{if } \deg(\Delta) = 2g + 1 \\ \textbf{real} & \text{if } \deg(\Delta) = 2g + 2 \end{cases}$$

where g is the **genus** of the **hyperelliptic curve** $y^2 = \Delta(x)$.

Quadratic Function Fields and Hyperelliptic Curves

Let q be odd and $\Delta \in \mathbb{F}_q[x]$ is monic and square-free.

Quadratic function field: $K = \mathbb{F}_q(x)(\sqrt{\Delta}) = \{a + b\sqrt{\Delta} \mid a, b \in \mathbb{F}_q(x)\}$
Maximal order of K: $\mathcal{O} = \mathbb{F}_q[x][\sqrt{\Delta}] = \{a + b\sqrt{\Delta} \mid a, b \in \mathbb{F}_q[x]\}$

$$K \text{ is } \begin{cases} \textbf{imaginary} & \text{if } \deg(\Delta) = 2g+1 \\ \textbf{real} & \text{if } \deg(\Delta) = 2g+2 \end{cases}$$

where g is the **genus** of the **hyperelliptic curve** $y^2 = \Delta(x)$.

Note that degrees are defined on real quadratic function fields.

Quadratic Function Fields and Hyperelliptic Curves

Let q be odd and $\Delta \in \mathbb{F}_q[x]$ is monic and square-free.

Quadratic function field: $K = \mathbb{F}_q(x)(\sqrt{\Delta}) = \{a + b\sqrt{\Delta} \mid a, b \in \mathbb{F}_q(x)\}$

Maximal order of K: $\mathcal{O} = \mathbb{F}_q[x][\sqrt{\Delta}] = \{a + b\sqrt{\Delta} \mid a, b \in \mathbb{F}_q[x]\}$

$$K \text{ is } \begin{cases} \textbf{imaginary} & \text{if } \deg(\Delta) = 2g + 1 \\ \textbf{real} & \text{if } \deg(\Delta) = 2g + 2 \end{cases}$$

where g is the **genus** of the **hyperelliptic curve** $y^2 = \Delta(x)$.

Note that degrees are defined on real quadratic function fields.

Note: For q even, hyperelliptic curves have the form $y^2 + h(x)y = \Delta(x)$ with conditions on Δ and h. We disregard this case here.

Reduced Ideals

Let $K = \mathbb{F}_q(x, \sqrt{\Delta})$ and $\mathcal{O} = \mathbb{F}_q[x, \sqrt{\Delta}]$ with $\deg(\Delta) = 2g + 1$ or $2g + 2$

Reduced Ideals

Let $K = \mathbb{F}_q(x, \sqrt{\Delta})$ and $\mathcal{O} = \mathbb{F}_q[x, \sqrt{\Delta}]$ with $\deg(\Delta) = 2g+1$ or $2g+2$

Definition

A **reduced ideal** of $\mathcal{O}$ is an $\mathbb{F}_q[x]$-module of rank 2 with an $\mathbb{F}_q[x]$-basis

$$\{Q, P + \sqrt{\Delta}\}$$

such that

- $Q, P \in \mathbb{F}_q[x]$ with Q monic
- Q divides $P^2 - \Delta$
- $\deg(Q) \leq g$ (so $|Q| < |\sqrt{\Delta}|$)

Reduced Ideals

Let $K = \mathbb{F}_q(x, \sqrt{\Delta})$ and $\mathcal{O} = \mathbb{F}_q[x, \sqrt{\Delta}]$ with $\deg(\Delta) = 2g + 1$ or $2g + 2$

Definition

A **reduced ideal** of $\mathcal{O}$ is an $\mathbb{F}_q[x]$-module of rank 2 with an $\mathbb{F}_q[x]$-basis

$$\{Q, P + \sqrt{\Delta}\}$$

such that

- $Q, P \in \mathbb{F}_q[x]$ with Q monic
- Q divides $P^2 - \Delta$
- $\deg(Q) \leq g$ (so $|Q| < |\sqrt{\Delta}|$)

Here, Q is unique, P is unique modulo Q, and we write $\mathfrak{a} = (Q, P)$.

Reduced Ideals

Let $K = \mathbb{F}_q(x, \sqrt{\Delta})$ and $\mathcal{O} = \mathbb{F}_q[x, \sqrt{\Delta}]$ with $\deg(\Delta) = 2g + 1$ or $2g + 2$

Definition

A **reduced ideal** of $\mathcal{O}$ is an $\mathbb{F}_q[x]$-module of rank 2 with an $\mathbb{F}_q[x]$-basis

$$\{Q, P + \sqrt{\Delta}\}$$

such that

- $Q, P \in \mathbb{F}_q[x]$ with Q monic
- Q divides $P^2 - \Delta$
- $\deg(Q) \leq g$ (so $|Q| < |\sqrt{\Delta}|$)

Here, Q is unique, P is unique modulo Q, and we write $\mathfrak{a} = (Q, P)$.

Heuristically, with probability $1 - O(q^{-1})$: $\deg(Q) = g$.

Applications of Compact Representations

For Real Quadratic Function Fields: same as for number fields

Applications of Compact Representations

For Real Quadratic Function Fields: same as for number fields

In addition: **pairing computation** (real and imaginary fields):

- A reduced ideal ideal $\mathfrak{a} = (Q, P)$ corresponds to the affine part of a reduced divisor D with Mumford representation $\{Q, P\}$.

For Real Quadratic Function Fields: same as for number fields

In addition: **pairing computation** (real and imaginary fields):

- A reduced ideal ideal $\mathfrak{a} = (Q, P)$ corresponds to the affine part of a reduced divisor D with Mumford representation $\{Q, P\}$.
- Suppose $nD = \text{div}(\theta)$ for some $\theta \in \mathcal{O}$, so $\mathfrak{a}^n = (\theta)$.

Applications of Compact Representations

For Real Quadratic Function Fields: same as for number fields

In addition: **pairing computation** (real and imaginary fields):

- A reduced ideal ideal $\mathfrak{a} = (Q, P)$ corresponds to the affine part of a reduced divisor D with Mumford representation $\{Q, P\}$.
- Suppose $nD = \text{div}(\theta)$ for some $\theta \in \mathcal{O}$, so $\mathfrak{a}^n = (\theta)$.
- When computing pairings (for example, in hyperelliptic curve cryptography), one needs to evaluate the function θ at some other divisor.

Applications of Compact Representations

For Real Quadratic Function Fields: same as for number fields

In addition: **pairing computation** (real and imaginary fields):

- A reduced ideal ideal $\mathfrak{a} = (Q, P)$ corresponds to the affine part of a reduced divisor D with Mumford representation $\{Q, P\}$.
- Suppose $nD = \mathrm{div}(\theta)$ for some $\theta \in \mathcal{O}$, so $\mathfrak{a}^n = (\theta)$.
- When computing pairings (for example, in hyperelliptic curve cryptography), one needs to evaluate the function θ at some other divisor.
- Miller's algorithm does this on the fly (via relative generators)

Applications of Compact Representations

For Real Quadratic Function Fields: same as for number fields

In addition: **pairing computation** (real and imaginary fields):

- A reduced ideal ideal $\mathfrak{a} = (Q, P)$ corresponds to the affine part of a reduced divisor D with Mumford representation $\{Q, P\}$.
- Suppose $nD = \text{div}(\theta)$ for some $\theta \in \mathcal{O}$, so $\mathfrak{a}^n = (\theta)$.
- When computing pairings (for example, in hyperelliptic curve cryptography), one needs to evaluate the function θ at some other divisor.
- Miller's algorithm does this on the fly (via relative generators)
- If a compact representation of θ is pre-computed, then this evaluation could be done all at once.

Applications of Compact Representations

For Real Quadratic Function Fields: same as for number fields

In addition: **pairing computation** (real and imaginary fields):

- A reduced ideal ideal $\mathfrak{a} = (Q, P)$ corresponds to the affine part of a reduced divisor D with Mumford representation $\{Q, P\}$.
- Suppose $nD = \mathrm{div}(\theta)$ for some $\theta \in \mathcal{O}$, so $\mathfrak{a}^n = (\theta)$.
- When computing pairings (for example, in hyperelliptic curve cryptography), one needs to evaluate the function θ at some other divisor.
- Miller's algorithm does this on the fly (via relative generators)
- If a compact representation of θ is pre-computed, then this evaluation could be done all at once.

Is this faster than using Miller's method? Only an implementation will tell.

UNIVERSITY OF CALGARY

Definition

Fix a base $m \in \mathbb{Z}$ with $m \geq 2$, and a digit bound B_m. For $n \in \mathbb{N}$, an (m, B_m)-**expansion of** n is a representation

$$n = \sum_{i=0}^{\ell} b_{\ell-i} m^i \quad \text{with} \quad -B_m \leq b_i \leq B_m$$

UNIVERSITY OF CALGARY

Definition

Fix a base $m \in \mathbb{Z}$ with $m \geq 2$, and a digit bound B_m. For $n \in \mathbb{N}$, an (m, B_m)-**expansion of** n is a representation

$$n = \sum_{i=0}^{\ell} b_{\ell-i} m^i \quad \text{with} \quad -B_m \leq b_i \leq B_m$$

Examples:

Unsigned digits:	$0 \leq b_i \leq m-1,$	$B_m = m-1$
Signed digits, m odd:	$-(m-1)/2 \leq b_i \leq (m-1)/2,$	$B_m = (m-1)/2$
Signed digits, m even:	$-m/2 < b_i \leq m/2,$	$B_m = m/2$
Non-adjacent form:	$m = 2,\ -1 \leq b_i \leq 1,\ b_i b_{i+1} = 0,$	$B_m = 1$

Compact Representations in Imaginary Fields

Compact Representations in Imaginary Fields

Definition

Let $n \in \mathbb{N}$, $\theta \in \mathcal{O}$, and $\mathfrak{a} = (Q, P)$ a reduced $\mathcal{O}$-ideal with $(\theta) = \mathfrak{a}^n$.

Compact Representations in Imaginary Fields

Definition

Let $n \in \mathbb{N}$, $\theta \in \mathcal{O}$, and $\mathfrak{a} = (Q, P)$ a reduced $\mathcal{O}$-ideal with $(\theta) = \mathfrak{a}^n$.

Let ℓ be the length of a base (m, B_m)-expansion of n.

Compact Representations in Imaginary Fields

Definition

Let $n \in \mathbb{N}$, $\theta \in \mathcal{O}$, and $\mathfrak{a} = (Q, P)$ a reduced $\mathcal{O}$-ideal with $(\theta) = \mathfrak{a}^n$.

Let ℓ be the length of a base (m, B_m)-expansion of n.

An (m, B_m)-**compact representation** of θ

Compact Representations in Imaginary Fields

Definition

Let $n \in \mathbb{N}$, $\theta \in \mathcal{O}$, and $\mathfrak{a} = (Q, P)$ a reduced $\mathcal{O}$-ideal with $(\theta) = \mathfrak{a}^n$.

Let ℓ be the length of a base (m, B_m)-expansion of n.

An (m, B_m)-**compact representation** of θ is a $(2\ell + 1)$-tuple

$$(\lambda_0, \lambda_1, \ldots \lambda_\ell; L_1, L_2, \ldots L_\ell)$$

Compact Representations in Imaginary Fields

Definition

Let $n \in \mathbb{N}$, $\theta \in \mathcal{O}$, and $\mathfrak{a} = (Q, P)$ a reduced $\mathcal{O}$-ideal with $(\theta) = \mathfrak{a}^n$.

Let ℓ be the length of a base (m, B_m)-expansion of n.

An (m, B_m)-**compact representation** of θ is a $(2\ell + 1)$-tuple

$$(\lambda_0, \lambda_1, \ldots \lambda_\ell; L_1, L_2, \ldots L_\ell)$$

where

- $\lambda_i = U_i + V_i\sqrt{\Delta} \in \mathcal{O}$ with U_i monic,

Compact Representations in Imaginary Fields

Definition

Let $n \in \mathbb{N}$, $\theta \in \mathcal{O}$, and $\mathfrak{a} = (Q, P)$ a reduced $\mathcal{O}$-ideal with $(\theta) = \mathfrak{a}^n$.

Let ℓ be the length of a base (m, B_m)-expansion of n.

An (m, B_m)-**compact representation** of θ is a $(2\ell + 1)$-tuple

$$(\lambda_0, \lambda_1, \ldots \lambda_\ell; L_1, L_2, \ldots L_\ell)$$

where

- $\lambda_i = U_i + V_i\sqrt{\Delta} \in \mathcal{O}$ with U_i monic, $\deg(U_i) \leq \Big((m+1)g + B_m \deg(Q)\Big)/2$ and $\deg(V_i) \leq \Big((m-1)g + B_m \deg(Q) - 1\Big)/2$,

Compact Representations in Imaginary Fields

Definition

Let $n \in \mathbb{N}$, $\theta \in \mathcal{O}$, and $\mathfrak{a} = (Q, P)$ a reduced $\mathcal{O}$-ideal with $(\theta) = \mathfrak{a}^n$.

Let ℓ be the length of a base (m, B_m)-expansion of n.

An (m, B_m)-**compact representation** of θ is a $(2\ell + 1)$-tuple

$$(\lambda_0, \lambda_1, \ldots \lambda_\ell; L_1, L_2, \ldots L_\ell)$$

where

- $\lambda_i = U_i + V_i\sqrt{\Delta} \in \mathcal{O}$ with U_i monic,
  $\deg(U_i) \leq \Big((m+1)g + B_m \deg(Q)\Big)/2$ and
  $\deg(V_i) \leq \Big((m-1)g + B_m \deg(Q) - 1\Big)/2$,
- $L_i \in \mathbb{F}_q[x]$ monic with $\deg(L_i) \leq g$

Compact Representations in Imaginary Fields

Definition

Let $n \in \mathbb{N}$, $\theta \in \mathcal{O}$, and $\mathfrak{a} = (Q, P)$ a reduced $\mathcal{O}$-ideal with $(\theta) = \mathfrak{a}^n$.

Let ℓ be the length of a base (m, B_m)-expansion of n.

An (m, B_m)-**compact representation** of θ is a $(2\ell + 1)$-tuple

$$(\lambda_0, \lambda_1, \dots \lambda_\ell; L_1, L_2, \dots L_\ell)$$

where

- $\lambda_i = U_i + V_i\sqrt{\Delta} \in \mathcal{O}$ with U_i monic, $\deg(U_i) \leq \Big((m+1)g + B_m \deg(Q)\Big)/2$ and $\deg(V_i) \leq \Big((m-1)g + B_m \deg(Q) - 1\Big)/2$,
- $L_i \in \mathbb{F}_q[x]$ monic with $\deg(L_i) \leq g$, and

$$\theta = \prod_{i=0}^{\ell} \left(\frac{\lambda_i}{L_i^m}\right)^{m^{\ell-i}} \quad \text{with } L_0 \in \mathbb{F}_q^* .$$

Size of a Compact Representation

Size of a Compact Representation

$$\#\ \text{elements in } \mathbb{F}_q \quad = \quad (\ell+1)\Big((m+1)g + B_m \deg(Q)\Big) - g$$

Size of a Compact Representation

$$\begin{aligned}\#\text{ elements in } \mathbb{F}_q &= (\ell+1)\Big((m+1)g + B_m \deg(Q)\Big) - g \\ &= \ell\Big((m+1)g + B_m \deg(Q)\Big) + O(mg)\end{aligned}$$

Size of a Compact Representation

$$\begin{aligned}
\#\text{ elements in } \mathbb{F}_q &= (\ell+1)\Big((m+1)g + B_m \deg(Q)\Big) - g \\
&= \ell\Big((m+1)g + B_m \deg(Q)\Big) + O(mg) \\
&= \frac{\log(n)}{\log(m)}\Big((m+1)g + B_m \deg(Q)\Big) + O(mg)
\end{aligned}$$

Size of a Compact Representation

$$\begin{aligned}
\#\text{ elements in } \mathbb{F}_q &= (\ell+1)\Big((m+1)g + B_m \deg(Q)\Big) - g \\
&= \ell\Big((m+1)g + B_m \deg(Q)\Big) + O(mg) \\
&= \frac{\log(n)}{\log(m)}\Big((m+1)g + B_m \deg(Q)\Big) + O(mg)
\end{aligned}$$

To find the optimal m, minimize main term: solve an equation of the form

$$am\log(m) - am - b = 0$$

for m, where a, b are

- monic linear functions in g if $\deg(Q) = 1$
- constant if $\deg(Q) = g$

Size of a Compact Representation

$$\begin{aligned}
\#\text{ elements in } \mathbb{F}_q &= (\ell+1)\Big((m+1)g + B_m \deg(Q)\Big) - g \\
&= \ell\Big((m+1)g + B_m \deg(Q)\Big) + O(mg) \\
&= \frac{\log(n)}{\log(m)}\Big((m+1)g + B_m \deg(Q)\Big) + O(mg)
\end{aligned}$$

To find the optimal m, minimize main term: solve an equation of the form

$$am\log(m) - am - b = 0$$

for m, where a, b are

- monic linear functions in g if $\deg(Q) = 1$
- constant if $\deg(Q) = g$

Looks like $m = 3$ or $m = 4$ in all cases (to be confirmed by implementation).

Distances in real quadratic fields

The **distance** of a reduced principal ideal $\mathfrak{a}$ is $\delta(\mathfrak{a}) = \deg(\theta)$, where θ is the monic generator of $\mathfrak{a}$ of minimal non-negative degree.

Distances in real quadratic fields

The **distance** of a reduced principal ideal $\mathfrak{a}$ is $\delta(\mathfrak{a}) = \deg(\theta)$, where θ is the monic generator of $\mathfrak{a}$ of minimal non-negative degree.

Note that distances are integers, so no approximations are necessary!

Distances in real quadratic fields

The **distance** of a reduced principal ideal $\mathfrak{a}$ is $\delta(\mathfrak{a}) = \deg(\theta)$, where θ is the monic generator of $\mathfrak{a}$ of minimal non-negative degree.

Note that distances are integers, so no approximations are necessary!

For $n \in \mathbb{N}$, let $\mathfrak{a}[n]$ be the unique reduced principal ideal $\mathfrak{a}$ such that

$$\delta(\mathfrak{a}) \text{ maximal and } \delta(\mathfrak{a}) \leq n$$

Distances in real quadratic fields

The **distance** of a reduced principal ideal $\mathfrak{a}$ is $\delta(\mathfrak{a}) = \deg(\theta)$, where θ is the monic generator of $\mathfrak{a}$ of minimal non-negative degree.

Note that distances are integers, so no approximations are necessary!

For $n \in \mathbb{N}$, let $\mathfrak{a}[n]$ be the unique reduced principal ideal $\mathfrak{a}$ such that

$$\delta(\mathfrak{a}) \text{ maximal and } \delta(\mathfrak{a}) \leq n$$

Heuristically, with probability $1 - O(q^{-1})$:

- Distances of neighbouring reduced ideals are spaced 1 apart.

Distances in real quadratic fields

The **distance** of a reduced principal ideal $\mathfrak{a}$ is $\delta(\mathfrak{a}) = \deg(\theta)$, where θ is the monic generator of $\mathfrak{a}$ of minimal non-negative degree.

Note that distances are integers, so no approximations are necessary!

For $n \in \mathbb{N}$, let $\mathfrak{a}[n]$ be the unique reduced principal ideal $\mathfrak{a}$ such that

$$\delta(\mathfrak{a}) \text{ maximal and } \delta(\mathfrak{a}) \leq n$$

Heuristically, with probability $1 - O(q^{-1})$:

- Distances of neighbouring reduced ideals are spaced 1 apart.
- $\delta(\mathfrak{a}[n]) = n$ for almost all n.

Distances in real quadratic fields

The **distance** of a reduced principal ideal $\mathfrak{a}$ is $\delta(\mathfrak{a}) = \deg(\theta)$, where θ is the monic generator of $\mathfrak{a}$ of minimal non-negative degree.

Note that distances are integers, so no approximations are necessary!

For $n \in \mathbb{N}$, let $\mathfrak{a}[n]$ be the unique reduced principal ideal $\mathfrak{a}$ such that

$$\delta(\mathfrak{a}) \text{ maximal and } \delta(\mathfrak{a}) \leq n$$

Heuristically, with probability $1 - O(q^{-1})$:

- Distances of neighbouring reduced ideals are spaced 1 apart.
- $\delta(\mathfrak{a}[n]) = n$ for almost all n.
- The number of reduction steps required to obtain the first reduced ideal when starting at $\mathfrak{a}^m$ is $h_m = \lceil (m-1)g/2 \rceil$. So we are h_m "adjustment steps" short of distance $m\delta(\mathfrak{a})$.

Avoiding the Headwind

Let k be maximal with $n \geq h_m \dfrac{m^k - 1}{m - 1}$ (with "$>$" if $m = 2$ or $n = m^\ell + 1$)

Avoiding the Headwind

Let k be maximal with $n \geq h_m \dfrac{m^k - 1}{m - 1}$ (with ">" if $m = 2$ or $n = m^\ell + 1$)

Properties:

- $k \leq \ell \leq k + \log(3g/2)$ if $g \geq 2$, $k = \ell + 1$ if $g = 1$

Let k be maximal with $n \geq h_m \dfrac{m^k - 1}{m - 1}$ (with "$>$" if $m = 2$ or $n = m^\ell + 1$)

Properties:

- $k \leq \ell \leq k + \log(3g/2)$ if $g \geq 2$, $k = \ell + 1$ if $g = 1$
- If $N = n + h_m \dfrac{m^k - 1}{m - 1}$, then $n \leq N < mn$, so the (m, B_m)-representations of n and N have the same length ℓ

Let k be maximal with $n \geq h_m \dfrac{m^k - 1}{m - 1}$ (with ">" if $m = 2$ or $n = m^\ell + 1$)

Properties:

- $k \leq \ell \leq k + \log(3g/2)$ if $g \geq 2$, $\quad k = \ell + 1$ if $g = 1$
- If $N = n + h_m \dfrac{m^k - 1}{m - 1}$, then $n \leq N < mn$, so the (m, B_m)-representations of n and N have the same length ℓ

Set

$$s_{-1} = 0, \quad s_i = \begin{cases} ms_{i-1} + \tilde{b}_i & \text{for } 0 \leq i \leq \ell - k \\ ms_{i-1} + \tilde{b}_i - h_m & \text{for } \ell - k + 1 \leq i \leq \ell \end{cases}$$

where the $\tilde{b}_i$ are the (m, B_m)-digits of N.

Avoiding the Headwind

Let k be maximal with $n \geq h_m \dfrac{m^k - 1}{m - 1}$ (with ">" if $m = 2$ or $n = m^\ell + 1$)

Properties:

- $k \leq \ell \leq k + \log(3g/2)$ if $g \geq 2$, $k = \ell + 1$ if $g = 1$
- If $N = n + h_m \dfrac{m^k - 1}{m - 1}$, then $n \leq N < mn$, so the (m, B_m)-representations of n and N have the same length ℓ

Set

$$s_{-1} = 0, \quad s_i = \begin{cases} ms_{i-1} + \tilde{b}_i & \text{for } 0 \leq i \leq \ell - k \\ ms_{i-1} + \tilde{b}_i - h_m & \text{for } \ell - k + 1 \leq i \leq \ell \end{cases}$$

where the $\tilde{b}_i$ are the (m, B_m)-digits of N.

Then $s_\ell = n$ and hence we expect $\delta(\mathfrak{a}[n]) = n$.

Compact Representations in Real Fields

Definition

Let $n \in \mathbb{N}$ and $\theta \in \mathcal{O}$ with $(\theta) = \mathfrak{a}[n]$.

Definition

Let $n \in \mathbb{N}$ and $\theta \in \mathcal{O}$ with $(\theta) = \mathfrak{a}[n]$.

Let ℓ be the length of a base (m, B_m)-expansion of n and k as above.

UNIVERSITY OF CALGARY

Definition

Let $n \in \mathbb{N}$ and $\theta \in \mathcal{O}$ with $(\theta) = \mathfrak{a}[n]$.

Let ℓ be the length of a base (m, B_m)-expansion of n and k as above.

An (m, B_m)-**compact representation** of θ is a $(2\ell + 1)$-tuple

$$(\lambda_0, \lambda_1, \ldots \lambda_\ell; L_1, L_2, \ldots L_\ell)$$

Definition

Let $n \in \mathbb{N}$ and $\theta \in \mathcal{O}$ with $(\theta) = \mathfrak{a}[n]$.

Let ℓ be the length of a base (m, B_m)-expansion of n and k as above.

An (m, B_m)-**compact representation** of θ is a $(2\ell + 1)$-tuple

$$(\lambda_0, \lambda_1, \ldots \lambda_\ell; L_1, L_2, \ldots L_\ell)$$

where we expect

- $\lambda_i = U_i + V_i\sqrt{\Delta} \in \mathcal{O}$ with U_i monic,

UNIVERSITY OF CALGARY

Definition

Let $n \in \mathbb{N}$ and $\theta \in \mathcal{O}$ with $(\theta) = \mathfrak{a}[n]$.

Let ℓ be the length of a base (m, B_m)-expansion of n and k as above.

An (m, B_m)-**compact representation** of θ is a $(2\ell + 1)$-tuple

$$(\lambda_0, \lambda_1, \ldots \lambda_\ell; L_1, L_2, \ldots L_\ell)$$

where we expect

- $\lambda_i = U_i + V_i\sqrt{\Delta} \in \mathcal{O}$ with U_i monic,
  $\deg(U_i) \leq 2h_m + B_m + g$, $\deg(V_i) = 2h_m + B_m - 1$ for $0 \leq i \leq \ell - k$,
  $\deg(U_i) \leq h_m + B_m + g$, $\deg(V_i) = h_m + B_m - 1$ for $\ell - k + 1 \leq i \leq \ell$,

UNIVERSITY OF CALGARY

Definition

Let $n \in \mathbb{N}$ and $\theta \in \mathcal{O}$ with $(\theta) = \mathfrak{a}[n]$.

Let ℓ be the length of a base (m, B_m)-expansion of n and k as above.

An (m, B_m)-**compact representation** of θ is a $(2\ell + 1)$-tuple

$$(\lambda_0, \lambda_1, \ldots \lambda_\ell; L_1, L_2, \ldots L_\ell)$$

where we expect

- $\lambda_i = U_i + V_i\sqrt{\Delta} \in \mathcal{O}$ with U_i monic,
  $\deg(U_i) \le 2h_m + B_m + g$, $\deg(V_i) = 2h_m + B_m - 1$ for $0 \le i \le \ell - k$,
  $\deg(U_i) \le h_m + B_m + g$, $\deg(V_i) = h_m + B_m - 1$ for $\ell - k + 1 \le i \le \ell$,
- $L_i \in \mathbb{F}_q[x]$ monic with $\deg(L_i) \le g$

UNIVERSITY OF CALGARY

Definition

Let $n \in \mathbb{N}$ and $\theta \in \mathcal{O}$ with $(\theta) = \mathfrak{a}[n]$.

Let ℓ be the length of a base (m, B_m)-expansion of n and k as above.

An (m, B_m)-**compact representation** of θ is a $(2\ell + 1)$-tuple

$$(\lambda_0, \lambda_1, \ldots \lambda_\ell; L_1, L_2, \ldots L_\ell)$$

where we expect

- $\lambda_i = U_i + V_i\sqrt{\Delta} \in \mathcal{O}$ with U_i monic,
  $\deg(U_i) \leq 2h_m + B_m + g$, $\deg(V_i) = 2h_m + B_m - 1$ for $0 \leq i \leq \ell - k$,
  $\deg(U_i) \leq h_m + B_m + g$, $\deg(V_i) = h_m + B_m - 1$ for $\ell - k + 1 \leq i \leq \ell$,
- $L_i \in \mathbb{F}_q[x]$ monic with $\deg(L_i) \leq g$, and

$$\theta = \prod_{i=0}^{\ell} \left(\frac{\lambda_i}{L_i^m}\right)^{m^{\ell-i}} \quad \text{with } L_0 \in \mathbb{F}_q^* .$$

Size of a Compact Representation

Size of a Compact Representation

$$\#\text{ elts in } \mathbb{F}_q = (\ell - k + 1)(4h_m + 2B_m + g) + k(2h_m + 2B_m + g)$$

Size of a Compact Representation

$$\begin{aligned}\#\text{ elts in }\mathbb{F}_q &= (\ell - k + 1)(4h_m + 2B_m + g) + k(2h_m + 2B_m + g)\\ &= \ell\Big((m+1)g + 2B_m + \epsilon\Big) + O(mg\log(g))\end{aligned}$$

Size of a Compact Representation

$$\begin{aligned}
\#\text{ elts in } \mathbb{F}_q &= (\ell - k + 1)(4h_m + 2B_m + g) + k(2h_m + 2B_m + g) \\
&= \ell\Big((m+1)g + 2B_m + \epsilon\Big) + O(mg\log(g)) \\
&= \frac{\log(n)}{\log(m)}\Big((m+1)g + 2B_m + \epsilon\Big) + O(mg\log(g))
\end{aligned}$$

for m, where $\epsilon = 0$ is the parity of $(m+1)g$ (0 if even, 1 if odd).

Size of a Compact Representation

$$\begin{aligned}\#\text{ elts in } \mathbb{F}_q &= (\ell - k + 1)(4h_m + 2B_m + g) + k(2h_m + 2B_m + g) \\ &= \ell\Big((m+1)g + 2B_m + \epsilon\Big) + O(mg\log(g)) \\ &= \frac{\log(n)}{\log(m)}\Big((m+1)g + 2B_m + \epsilon\Big) + O(mg\log(g))\end{aligned}$$

for m, where $\epsilon = 0$ is the parity of $(m+1)g$ (0 if even, 1 if odd).

To find the optimal m, minimize main term: solve an equation of the form

$$am\log(m) - am - b = 0$$

where a, b are monic linear functions in g.

$$\begin{aligned}
\#\text{ elts in } \mathbb{F}_q &= (\ell - k + 1)(4h_m + 2B_m + g) + k(2h_m + 2B_m + g) \\
&= \ell\Big((m+1)g + 2B_m + \epsilon\Big) + O(mg\log(g)) \\
&= \frac{\log(n)}{\log(m)}\Big((m+1)g + 2B_m + \epsilon\Big) + O(mg\log(g))
\end{aligned}$$

for m, where $\epsilon = 0$ is the parity of $(m+1)g$ (0 if even, 1 if odd).

To find the optimal m, minimize main term: solve an equation of the form

$$am\log(m) - am - b = 0$$

where a, b are monic linear functions in g.

Expect again that $m = 3$ or $m = 4$ (to be confirmed by implementation).

That's All, Folks!

∗ ∗ ∗ **Questions?** ∗ ∗ ∗