Optimality of the Width-w Non-adjacent Form - A Diophantine inequality

Volker Ziegler

Institute for Analysis and Computational Number Theory
Graz University of Technology

Uniform Distribution Theory
25th June- 29th June 2012
Smolenice

Frobenius and add

Question

Given an Elliptic curve E defined over a finite field $\mathbb{F}_q$, a point P on $E(\mathbb{F}_{q^l})$ and an integer n. How can we compute nP efficiently?

Frobenius and add

Question

Given an Elliptic curve E defined over a finite field $\mathbb{F}_q$, a point P on $E(\mathbb{F}_{q^l})$ and an integer n. How can we compute nP efficiently?

Let ϕ be the Frobenius endomorphism $\phi((x, y)) = (x^q, y^q)$ then ϕ fulfills

$$\phi^2 - p\phi + q = 0.$$

Therefore we identify ϕ with an quadratic algebraic integer τ which fulfills the same equation.

The fastest way to compute qP for some $P \in E(\mathbb{F}_{q^l})$ is to compute

$$qP = p\phi(P) - \phi^2(P).$$

The fastest way to compute qP for some $P \in E(\mathbb{F}_{q^l})$ is to compute

$$qP = p\phi(P) - \phi^2(P).$$

Now, let us represent the integer n as $n = \sum_{j=0}^{\ell} \eta_j \tau^j$ for η_j from a suitable digit set $\mathcal{D}$, then

$$nP = \sum_{j=0}^{\ell} \eta_j \phi^j(P),$$

where the ηP for $\eta \in \mathcal{D}$ are precomputed.

w-NAF

Consider an expansion $n = \sum_{j=0}^{\ell} \eta_j \tau^j$ as a sequence $(\eta_j) \in \mathcal{D}^{\mathbb{N}_0}$ with $\eta_j \in \mathcal{D}$. If each block $(\eta_j, \ldots, \eta_{j+w})$ contains at most one non-zero digit, we call this expansion an width-w non adjacent form (w-NAF for short).

w-NAF

Consider an expansion $n = \sum_{j=0}^{\ell} \eta_j \tau^j$ as a sequence $(\eta_j) \in \mathcal{D}^{\mathbb{N}_0}$ with $\eta_j \in \mathcal{D}$. If each block $(\eta_j, \ldots, \eta_{j+w})$ contains at most one non-zero digit, we call this expansion an width-w non adjacent form (w-NAF for short).
Let $\eta \in \mathcal{D}^{\mathbb{N}_0}$ and let $|\eta|$ be the number of non-zero digits. We call a w-NAF η optimal, if for any expansion ξ representing the same integer as η we have $|\eta| \leq |\xi|$.

w-NAF

Consider an expansion $n = \sum_{j=0}^{\ell} \eta_j \tau^j$ as a sequence $(\eta_j) \in \mathcal{D}^{\mathbb{N}_0}$ with $\eta_j \in \mathcal{D}$. If each block $(\eta_j, \dots, \eta_{j+w})$ contains at most one non-zero digit, we call this expansion an width-w non adjacent form (w-NAF for short).

Let $\eta \in \mathcal{D}^{\mathbb{N}_0}$ and let $|\eta|$ be the number of non-zero digits. We call a w-NAF η optimal, if for any expansion ξ representing the same integer as η we have $|\eta| \leq |\xi|$.

Question

For which basis τ and digit sets $\mathcal{D}$ are w-NAF expansions optimal?

Examples

- For base 2 and digit set $\{-1, 0, 1\}$ the 2-NAF are optimal (Reitwiesner 1960).

Examples

- For base 2 and digit set $\{-1, 0, 1\}$ the 2-NAF are optimal (Reitwiesner 1960).
- For base 2 and digit set consisting of 0 and all odd numbers with absolute value $< 2^{w-1}$ the w-NAF are optimal (Muir, Stinson 2006).

Examples

- For base 2 and digit set $\{-1, 0, 1\}$ the 2-NAF are optimal (Reitwiesner 1960).
- For base 2 and digit set consisting of 0 and all odd numbers with absolute value $< 2^{w-1}$ the w-NAF are optimal (Muir, Stinson 2006).
- For base $b \geq 2$ and digit set consisting of 0 and all integers with absolute value $< \frac{1}{2}b^w$ and not divisible by b the w-NAF expansion is optimal (Heuberger, Krenn 2011).

Voronoi cells

Let $\tau \in \mathbb{C}$ be a solution to $x^2 - px + q = 0$, with $p, q \in \mathbb{Z}$ such that $q - p^2/4 > 0$. We set

$$V = \{z \in \mathbb{C} : \forall y \in \mathbb{Z}[\tau]\ |z| \leq |z - y|\}$$

and call it Voronoi cell.

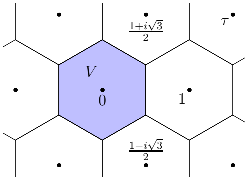

Figure: Voronoi cell with $\tau = (3 + \sqrt{-3})/2$.

Digit sets

Let w be an integer with $w \geq 2$. Then we choose the Digit set $\mathcal{D} \subset \mathbb{Z}[\tau]$ that consists of 0 and exactly one representative $\in \tau^w V$ of each residue class of $\mathbb{Z}[\tau]$ modulo τ^w which is not divisible by τ. This digit set is called minimal norm representatives digit set.

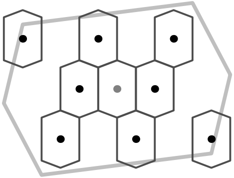

Figure: Digit set for $\tau = (1 + \sqrt{-13})/2$ and $w = 2$.

Existence and Uniqueness

Theorem (Heuberger, Krenn 2011)

The w-NAF exists and are unique for base τ with the minimal norm representatives digit set modulo τ^w.

Existence and Uniqueness

Theorem (Heuberger, Krenn 2011)

The w-NAF exists and are unique for base τ with the minimal norm representatives digit set modulo τ^w.

Let τ be a root of $x^2 - px + q = 0$. Then the w-NAFs are optimal if

- $w \geq 4$ and $|p| \geq 3$,

Existence and Uniqueness

Theorem (Heuberger, Krenn 2011)

The w-NAF exists and are unique for base τ with the minimal norm representatives digit set modulo τ^w.

Let τ be a root of $x^2 - px + q = 0$. Then the w-NAFs are optimal if

- $w \geq 4$ and $|p| \geq 3$,
- $w = 3$ and $|p| \geq 5$,

Existence and Uniqueness

Theorem (Heuberger, Krenn 2011)

The w-NAF exists and are unique for base τ with the minimal norm representatives digit set modulo τ^w.

Let τ be a root of $x^2 - px + q = 0$. Then the w-NAFs are optimal if

- $w \geq 4$ and $|p| \geq 3$,
- $w = 3$ and $|p| \geq 5$,
- $w = 3$ and $|p| = 4$ and $5 \leq q \leq 9$,
- $\ldots$

Question

What is with p small, in particular $p = \pm 1$.

The general idea

Suppose we have an expansion of the form $\alpha = a + \tau^{w-1} b$, such that b lies near the border of the expanded Voronoi cell $\tau^w V$.

The general idea

Suppose we have an expansion of the form $\alpha = a + \tau^{w-1} b$, such that b lies near the border of the expanded Voronoi cell $\tau^w V$.
We take a new $a' = a + d\tau^{w-1} \in \tau^w V$ such that $\alpha = a' + (b+d)\tau^{w-1}$ and $\tau | b + d$, i.e. we have

$$\alpha = a' + \frac{\overbrace{b+d}^{:=b'}}{\tau} \tau^w .$$

The general idea

Suppose we have an expansion of the form $\alpha = a + \tau^{w-1} b$, such that b lies near the border of the expanded Voronoi cell $\tau^w V$.
We take a new $a' = a + d\tau^{w-1} \in \tau^w V$ such that $\alpha = a' + (b+d)\tau^{w-1}$ and $\tau | b + d$, i.e. we have

$$\alpha = a' + \frac{\overbrace{b+d}^{:=b'}}{\tau}\tau^w.$$

If $b' \notin \tau^w V$, then b' has weight at least two and because w-NAF expansions exist and are unique the w-NAF of α would have weight ≥ 3 and is therefore not optimal.

Digit set

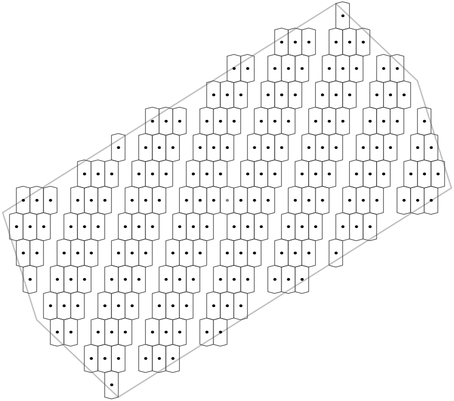

Figure: Digit set in $\tau^w V$.

The corridors

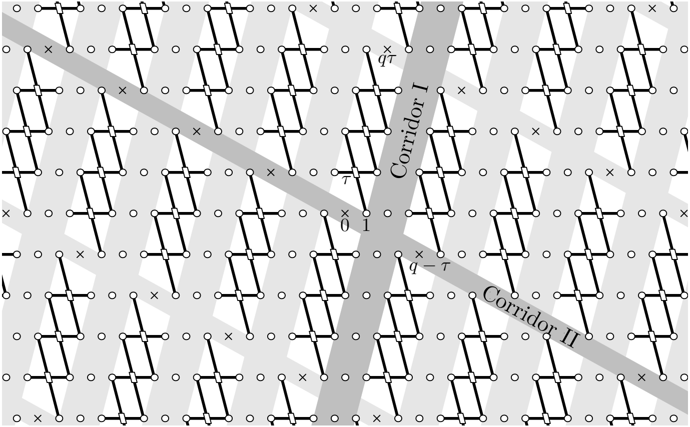

Figure: Corridors.

Some notations

Let us fix the following notation:

$$\tau^2 - p\tau + q = 0 \qquad \tau = \frac{p}{2} + i\sqrt{q - \frac{1}{4}}$$

$$R = -\frac{1}{2} + \frac{i}{2\sqrt{4q-1}} \qquad S = -\frac{1}{2} - \frac{i}{2\sqrt{4q-1}}$$

$$T = i\frac{2q-1}{\sqrt{4q-1}}$$

$$\sigma_I = 2\sqrt{q - \frac{1}{4}} + \sqrt{q} \qquad \sigma_{II} = |q + 1 - 2\tau| + \sqrt{q}$$

$$d_I = \frac{\tau}{\sqrt{q}} \qquad d_{II} = p - \frac{\tau}{q}$$

$$W_I = (q-2)\sqrt{1 - \frac{1}{4q}} \qquad W_{II} = \frac{\sqrt{4q-1}}{q}$$

Relation to a Diophantine inequality

Theorem (Krenn, Z. 2012)

If w and q do not satisfy the inequality

$$\left|\mathrm{Im}\left(\tau^{w} E d_c^{-1}\right)\right| < W_c \left(1 - 2\frac{\sigma_c}{|\tau|^{w}|E|}\right)^{-1},$$

with $E \in \{R, S, T\}$ and $c \in \{I, II\}$. Then we can construct a counter example of the kind described above

Relation to a Diophantine inequality

Theorem (Krenn, Z. 2012)

If w and q do not satisfy the inequality

$$\left|\operatorname{Im}\left(\tau^{w} E d_c^{-1}\right)\right| < W_c \left(1 - 2\frac{\sigma_c}{|\tau|^{w}|E|}\right)^{-1},$$

with $E \in \{R, S, T\}$ and $c \in \{I, II\}$. Then we can construct a counter example of the kind described above

Conjecture (Krenn, Z. 2012)

The inequality has no solution if $w \geq 12$ and $q \geq 2$.

The inequality

Considering the original inequality and dividing it through $\bar{\tau}^w \overline{Ed_c^{-1}}/2$ we obtain

$$\left| \frac{\tau^w Ed_c^{-1}}{\overline{\bar{\tau}^w \overline{Ed_c^{-1}}}} - 1 \right| < \frac{8(2+\sqrt{2})q}{q^{w/2}} < \frac{28q}{q^{w/2}}.$$

The inequality

Considering the original inequality and dividing it through $\bar\tau^w\overline{Ed_c^{-1}}/2$ we obtain

$$\left|\frac{\tau^w E d_c^{-1}}{\bar\tau^w\overline{Ed_c^{-1}}}-1\right| < \frac{8(2+\sqrt{2})q}{q^{w/2}} < \frac{28q}{q^{w/2}}.$$

Note that

$$\begin{aligned} R &= \tau\frac{i}{\overline{\sqrt{4q-1}}}, & S &= \bar\tau\frac{i}{\overline{\sqrt{4q-1}}} & &\text{if } p = 1,\\ R &= \bar\tau\frac{-i}{\overline{\sqrt{4q-1}}}, & S &= \tau\frac{-i}{\overline{\sqrt{4q-1}}} & &\text{if } p = -1, \end{aligned}$$

and

$$\frac{T}{\bar T} = 1, \qquad \frac{d_I}{\bar d_I} = \frac{\tau}{\bar\tau}, \qquad \frac{d_{II}}{\bar d_{II}} = \frac{\tau^2}{\bar\tau^2}.$$

Linear forms in logarithms

Therefore we have to consider the following form in two logarithms:

$$\left|(w+l)\log\frac{\tau}{\overline{\tau}} - k\log(-1)\right| < \frac{42q}{q^{w/2}}$$

where $|l| \leq 3$.

Linear forms in logarithms

Therefore we have to consider the following form in two logarithms:

$$\left|(w+l)\log\frac{\tau}{\bar{\tau}} - k\log(-1)\right| < \frac{42q}{q^{w/2}}$$

where $|l| \leq 3$.
We can compute asymptotic expansions of the logarithms and obtain

$$\frac{1}{i}\log\frac{\tau}{\bar{\tau}} = \pi \pm \frac{1}{\sqrt{q}} + \frac{1}{24q^{3/2}} + O\left(\frac{1}{q^{5/2}}\right),$$

where the "$+$" sign holds if and only if $p = 1$.

Bounds for q and w

Therefore the inequalities for the linear forms in logarithms yield

$$\left|(w+l-k)\pi + \frac{\pm(w+l)}{\sqrt{q}} + O\left(\frac{w+l}{q^{3/2}}\right)\right| < \frac{42q}{q^{w/2}}$$

Bounds for q and w

Therefore the inequalities for the linear forms in logarithms yield

$$\left|(w+l-k)\pi + \frac{\pm(w+l)}{\sqrt{q}} + O\left(\frac{w+l}{q^{3/2}}\right)\right| < \frac{42q}{q^{w/2}}$$

Therefore we have $q \lesssim (w/\pi)^2$. Using lower bounds for linear forms in two logarithms due to Laurent, et.al. we get an absolute upper bound for w provided q is not too small. In particular we obtain $w \leq 241747$ and therefore $q > 5.926 \cdot 10^9$.

Completing the proof of the conjecture

Notet that we also have

$$\left|\frac{k}{w+l}-\frac{\log\frac{\tau}{\bar{\tau}}}{\pi}\right|<\frac{42q}{(w+l)\pi q^{w/2}}$$

i.e. that implies $k/(w+l)$ is a continued fraction to $\delta=\frac{\log\frac{\tau}{\bar{\tau}}}{\pi}$ and we can easily check for each q (large enough) whether a solution exists.

Completing the proof of the conjecture

Notet that we also have

$$\left|\frac{k}{w+l} - \frac{\log\frac{\tau}{\overline{\tau}}}{\pi}\right| < \frac{42q}{(w+l)\pi q^{w/2}}$$

i.e. that implies $k/(w+l)$ is a continued fraction to $\delta = \frac{\log\frac{\tau}{\overline{\tau}}}{\pi}$ and we can easily check for each q (large enough) whether a solution exists.This is work in progress.