Applications of Digital Expansions in the Efficient Implementation of Cryptosystems

Clemens Heuberger

Graz University of Technology, Austria

Supported by the Austrian Science Foundation FWF, project S9606, that is part of the Austrian National Research Network "Analytic Combinatorics and Probabilistic Number Theory."

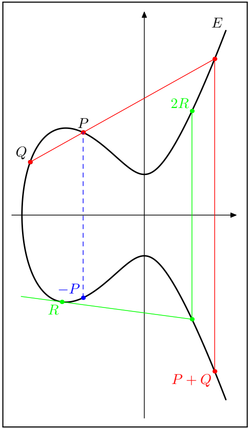
Luminy, March 25th, 2009

Outline

Elliptic curve cryptography

Elliptic Curve $E : y^2 = x^3 + ax^2 + bx + c$
For $P \in E$ and $n \in \mathbb{Z}$, nP can be calculated easily.
No efficient algorithm to calculate n from P and nP?
Fast calculation of nP desirable!

Methods also apply to Abelian groups (e.g., the Jacobian of a hyperelliptic curve) where subtracting a point is as cheap as addition.



Double-and-Add Algorithm

Calculating $27P$ via a doubling and adding scheme using the standard binary expansion of 27:

$$\begin{aligned} 27 &= (11011)_2, \\ 27P &= 2(2(2(2(P) + P) + 0) + P) + P. \end{aligned}$$

Number of additions $\sim$ Hamming weight of the binary expansion (Number of nonzero digits)
Number of doublings $\sim$ length of the expansion

Double, Add, and Subtract Algorithm

Subtraction is as cheap as addition!

$$27 = (100\bar{1}0\bar{1})_2,$$
$$27P = 2(2(2(2(2(P) + 0) + 0) - P) + 0) - P.$$

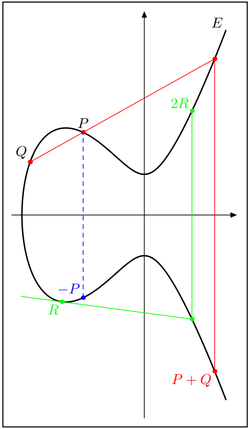
$(\bar{1} := -1)$

$\Longrightarrow$ Use of signed digit expansions

Number of additions/subtractions $\sim$ Hamming weight of the binary expansion

Number of multiplications $\sim$ length of the expansion

There are (infinitely) many signed binary expansions of an integer (Redundancy) $\Longrightarrow$ find expansion of minimal Hamming weight.



Deriving a Low-Weight Representation

Take an integer n.

- If n is even, we have to take 0 as least significant digit and continue with $n/2$.
- If $n \equiv 1 \pmod 4$, we take 1 as least significant digit and continue with $(n-1)/2$. This is even and guarantees a zero in the next step.
- If $n \equiv 3 \equiv -1 \pmod 4$, we take -1 as least significant digit and continue with $(n+1)/2$. This is even and guarantees a zero in the next step.

This procedure yields a zero after every non-zero, which should yield a low weight expansion. There are no adjacent non-zeros.

Non-Adjacent Form

Theorem (Reitwiesner 1960)

Let $n \in \mathbb{Z}$, then there is exactly one signed binary expansion $\varepsilon \in \{-1,0,1\}^{\mathbb{N}_0}$ of n such that

$$n = \sum_{j\geq 0} \varepsilon_j 2^j, \qquad (\varepsilon \text{ is a binary expansion of } n),$$

$$\varepsilon_j \varepsilon_{j+1} = 0 \qquad \text{for all } j \geq 0.$$

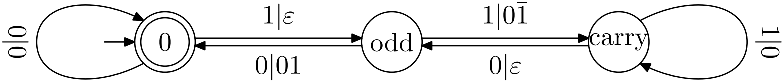
It is called the Non-Adjacent Form (NAF) of n.
It minimises the Hamming weight amongst all signed binary expansions with digits $\{0, \pm 1\}$ of n.

Non-Adjacent Form: Applications

- Efficient arithmetic operations (Reitwiesner 1960)
- Coding Theory
- Jump interpolation search trees (Güntzer and Paul 1987)
- Exponentiation (Jedwab and Mitchell 1989)
- Elliptic Curve Cryptography (Morain and Olivos 1990)

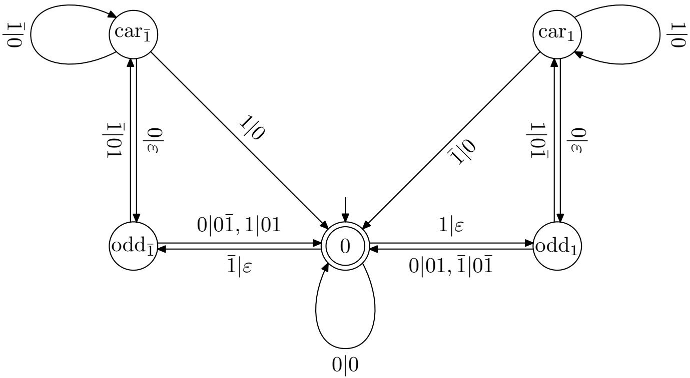
Transducer Automaton Unsigned → NAF

Conversion of the unsigned binary expansion in nonadjacent form from right to left.



Transducer Automaton Any Signed Expansion $\longrightarrow$ NAF

Conversion of any signed binary expansion in nonadjacent form from right to left.



There is no cycle of increasing weight $\Rightarrow$ NAF is optimal.

Analysis of the NAF — Known Results

Theorem

$$\mathbb{E}(H_\ell) = \frac{1}{3}\ell + \frac{2}{9} + O(2^{-\ell}),$$

$$\mathbb{V}(H_\ell) = \frac{2}{27}\ell + \frac{8}{81} + O(\ell 2^{-\ell}),$$

$$\lim_{\ell\to\infty} \mathbb{P}\left(H_\ell \le \frac{\ell}{3} + h\sqrt{\frac{2\ell}{27}}\right) = \frac{1}{\sqrt{2\pi}}\int_0^h e^{-t^2/2}\,dt,$$

where H_ℓ is the Hamming weight of a random NAF of length $\le \ell$ (all NAFs of length $\le \ell$ are considered to be equally likely).

Subblock Occurrences without Restricting to Full Blocks

Let $\mathbf{b} = (b_{r-1}, \ldots, b_0) \neq \mathbf{0}$ be an admissible block, $(\ldots \varepsilon_2(n)\varepsilon_1(n)\varepsilon_0(n))$ the NAF of n.
We consider

$$S_{\mathbf{b}}(N) := \sum_{n<N} \sum_{k=0}^{\infty} [(\varepsilon_{k+r-1}(n), \ldots, \varepsilon_k(n)) = \mathbf{b}],$$

i.e. the number of occurrences of the block **b** in the NAFs of the positive integers less than N.

Subblock Occurrences

Theorem (Grabner-H.-Prodinger 2003)

If $b_{r-1} = 0$, then $S_{\mathbf{b}}(N) =$

$$\frac{Q(b_0)}{3 \cdot 2^r} N \log_2 N + N h_0(\mathbf{b}) + N H_{\mathbf{b}}(\log_2 N) + o(N),$$

where

$$\begin{aligned} Q(\eta) &= 2 + 2\,[\eta = 0] \\ H_{\mathbf{b}}(x) &= \sum_{k \in \mathbb{Z} \setminus \{0\}} h_k(\mathbf{b}) e^{2k\pi i x} \end{aligned}$$

for explicitly known constants $h_k(\mathbf{b})$, $k \in \mathbb{Z}$.
$H_{\mathbf{b}}(x)$ is a 1-periodic continuous function.

NAF: Counting Subblocks — Explicit constants

$$h_k(\mathbf{b}) = \frac{\zeta\left(\frac{2k\pi i}{\log 2}, \alpha_{\min}(\mathbf{b})\right) - \zeta\left(\frac{2k\pi i}{\log 2}, \alpha_{\max}(\mathbf{b})\right)}{2k\pi i(1 + \frac{2k\pi i}{\log 2})} \text{ for } k \neq 0,$$

$$h_0(\mathbf{b}) = \log_2 \Gamma(\alpha_{\min}(\mathbf{b})) - \log_2 \Gamma(\alpha_{\max}(\mathbf{b})) - \frac{Q(b_0)}{3 \cdot 2^r}\left(r + \frac{1}{6} + \frac{1}{\log 2}\right) + \frac{1}{3 \cdot 2^{r-1}},$$

$$\alpha_{\min}(\mathbf{b}) = [\text{value}(\mathbf{b}) < 0] + 2^{-r}\text{value}(\mathbf{b}) - \frac{1 + [b_0 \text{ even}]}{3 \cdot 2^r}$$

$$\alpha_{\max}(\mathbf{b}) = [\text{value}(\mathbf{b}) < 0] + 2^{-r}\text{value}(\mathbf{b}) + \frac{1 + [b_0 \text{ even}]}{3 \cdot 2^r}$$

$\zeta(s, x)$ denotes the Hurwitz ζ-function.
The case $r = 1$ is contained in Thuswaldner (1999).

Further Results

- Dynamical Aspects (Dajani-Kraaikamp-Liardet 2006)
- Analysis of von Neumann addition (H.-Prodinger 2003)
- Number of optimal expansions (Grabner-H. 2006)
- Alternative digit sets (Muir-Stinson 2004, 2005; Avoine-Monnerat-Peyrin 2004; H.-Prodinger 2006)
- ...

Right-to-Left vs. Left-to-Right

Left-To-Right scalar multiplication:

$$\begin{aligned} 27 &= (11011)_2, \\ 27P &= 2(2(2(2(P) + P) + 0) + P) + P. \end{aligned}$$

Right-To-Left scalar multiplication:

$$27P = 2^4 P + (2^3 P + (2^2 0 + (2^1 P + 2^0 P))),$$

where $2^k P = 2(2^{k-1} P)$.
In our case (addition of $\pm P$), both methods are available.
Joye and Yen 2000 give an algorithm for computing a $\{0, 1, -1\}$-expansion of minimal weight (i.e., weight is equal to that of the NAF) from left to right.

1. Introduction
2. Windows and Precomputation
   - Sliding Windows
   - w-NAF
   - Fractional Windows
   - Double Base
3. Linear Combinations and Joint Expansions
4. Endomorphisms and Complex Bases

Windows and Higher Bases

Let

$$n = (\boxed{10\bar{1}}\,\boxed{001}\,\boxed{0\bar{1}0}\,\boxed{010}\,\boxed{101})_2.$$

Take "windows" of length w. Gives expansion to the base of 2^w with many digits $d \in \{0\} \cup \mathcal{D}$.
Precompute dP for $d \in \mathcal{D}$ (with $d > 0$).
Left-to-right scalar multiplication:

$$nP = 2^3(2^3(2^3(2^3(\boxed{10\bar{1}}\,P) + \boxed{001}\,P) - \boxed{010}\,P) + \boxed{010}\,P) + \boxed{101}\,P.$$

Right-to-left scalar multiplication in general not efficient: One would have to compute $2^{kw}dP$ for all $d \in \mathcal{D}$ with $d > 0$.

Sliding Windows

Let

$$z = (\boxed{10\bar{1}}00\boxed{10\bar{1}}\boxed{001}0\boxed{101})_2.$$

Sliding windows of length $w = 3$.
Can be seen as an expansion with digits

$$\left\{0, \pm 1, \pm 3, \ldots, \pm \frac{4 \cdot 2^n - (-1)^n}{3}\right\}.$$

Apart from 0, only odd digits are used.
Expected Hamming weight (Grabner-H.-Prodinger-Thuswaldner 2005):

$$\frac{1}{w + (4 - 4(-2)^{-w})/3}\ell + O(1)$$

w-NAF

If one does not start with the NAF and forms windows out of it, but directly creates a suitable expansion, another approach is possible (cf. Cohen 2005):
We set $\mathcal{D} = \{\pm 1, \pm 3, \ldots, \pm(2^{w-1} - 1)\}$. Then every $n \in \mathbb{Z}$ admits a unique expansion

$$n = \sum_{j=0}^{\ell} d_j 2^j \qquad d_j \in \{0\} \cup \mathcal{D}$$

with the w-NAF condition:

$$\text{If } d_j \neq 0, \text{ then } d_{j+1} = d_{j+2} = \cdots = d_{j+w-1} = 0.$$

Expected Hamming weight of a w-NAF of length ℓ:

$$\frac{1}{w+1}\ell - \frac{(w-1)(w+2)}{2(w+1)^2} + o(1).$$

Fractional Windows

- Möller 2003, 2005: In restricted memory environments (e.g., smartcards), the required stored data for sliding width w windows or w-NAF may not fit with the available storage area. Use *fractional windows:* odd digits from $-m, \ldots, m$.
- Phillips and Burgess (2004) suggest odd digits from the set $\mathcal{D}_{\ell,u} = \{\ell, \ldots, u\}$ with $\ell \leq 0$ and $u \geq 1$.
  Common generalisation of all representations presented so far, including unsigned expansions.

Computing Fractional Windows Expansions

Choose w maximally such that $\mathcal{D}$ contains at least one representative of every odd residue class modulo 2^{w-1}. Some residue classes modulo 2^{w-1} will have two representatives.

- If n is even, the last digit is 0 and we continue with $n/2$.
- If $n \equiv d \in \mathcal{D}_{\ell,u} \pmod{2^{w-1}}$ such that d is the unique representative of its residue class modulo 2^{w-1}, the last digit is d, then we have $w-2$ zeros and we continue with $(n-d)/2^{w-1}$.
- If $n \equiv d_1 \equiv d_2 \in \mathcal{D}_{\ell,u} \pmod{2^{w-1}}$ for distinct d_1 and d_2, then for $n \equiv d_j \pmod{2^w}$ for one $j \in \{1,2\}$. The last digit is d_j, then we have $w-1$ zeros, and we continue with $(n-d)/2^w$.

This construction minimises the Hamming weight over all expansions with digits from $\mathcal{D}_{\ell,u}$ (Phillips and Burgess).

Analysis

Let W_n be a random expansion of length n, constructed according to the above algorithm. Then

$$\mathbb{E}(W_n) = \frac{1}{w-1+\lambda}n+O(1) \quad \text{and} \quad \mathrm{Var}(W_n) = \frac{(3-\lambda)\lambda}{(w-1+\lambda)^3}n+O(1),$$

where

$$\lambda = \frac{u-\ell+2}{2^{w-1}}.$$

Furthermore, the random variable W_n satisfies the central limit law

$$\lim_{n\to\infty} \Pr\left(W_n \le \mathbb{E}(W_n) + x\sqrt{\mathrm{Var}(W_n)}\right) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-\frac{t^2}{2}}\,dt.$$

Left-To-Right

- w-NAF: Muir-Stinson 2005; Avanzi 2005; Okeya-Schmidt-Samoa-Spahn-Takagi 2004; Khabbazian-Gulliver-Bhargava 2005; H.-Katti-Prodinger-Ruan 2005.
- $\{-m, \ldots, m\}$: Möller 2004
- $\mathcal{D}_{\ell,u} = \{\ell, \ldots, u\}$: H.-Muir 2009.

In all these cases, an expansion of minimal weight with the same digit set is constructed (but not satisfying the respective syntactical conditions), it can be calculated from left to right.

Left-To-Right by Approximation

Consider the digit set $\mathcal{D}_{\ell,u} = \{\ell, \dots, u\}$.

Idea: Approximate given integer n by the "closest" weight-one integer c_1. Continue the process with $n - c_1$.

The notion of "closest" has to take into account the lack of symmetry of the digit set: If $c_1 < n < c_2$ and c_1 and c_2 are successive weight-one integers, then c_1 is "closest" to n if and only if

$$n - c_1 < \frac{u}{u + |\ell|}(c_2 - c_1).$$

In general, this decision cannot be made by an automaton reading the standard binary expansion from left to right.

Luckily, some "tolerance" can be allowed: Always choosing the "almost closest" (closest up to a fixed error, depending on ℓ and u) yields a minimal weight expansion, computable by a transducer automaton from the standard binary expansion (for fixed ℓ and u).

Double Base

- Dimitrov-Jullien-Miller 1998:

$$n = \sum_{i=0}^{h-1} c_i 2^{a_i} 3^{b_i} \qquad \text{with } c_i \in \{\pm 1\}$$

  and sequences a_i and b_i. Fewer additions ($O(\log(n)/\log\log n)$), but precomputation is more expensive.
- Dimitrov-Imbert-Mishra 2005: Impose additional condition $a_0 \le a_1 \le \cdots \le a_{h-1}$ and $b_0 \le b_1 \le \cdots \le b_{h-1}$. More additions, but successive computation of $2^{a_i} 3^{b_i}$ feasible.
- Doche and Imbert 2006: Allow larger digit set.

Joint expansions

Let $n_1, n_2 \in \mathbb{Z}$ and consider a signed binary joint expansion $\boldsymbol{\varepsilon} = (\varepsilon_j^{(i)})_{\substack{i=1,2\\ j\ge 0}} \in \{-1,0,1\}^{\{1,2\}\times\mathbb{N}_0}$ of n_1 and n_2, i.e.,

$$n_i = \sum_{j\ge 0} \varepsilon_j^{(i)} 2^j.$$

(The ith row is an expansion of n_i.)

Example: Compute 30P+21Q on Curve.

Precompute $P+Q, P-Q$.

$$30 = (1000\bar{1}0)_2, \qquad \bar{1} := -1$$

$$21 = (10\bar{1}0\bar{1}\bar{1})_2,$$

$$30P + 21Q = 2(2(2(2(2(P+Q)+0)-Q)+0)-(P+Q))-Q.$$

Joint Hamming weight: number of nonzero columns (corresponds to the number of additions).

Simple Joint Sparse Form

We define

$$A_j(\varepsilon) = \{i \in \{1, 2\} : \varepsilon_j^{(i)} \neq 0\}.$$

(Positions of nonzero digits in "column" j.)

Theorem (Grabner-H.-Prodinger 2004)

There is a unique simple joint sparse form of (n_1, n_2) such that

$$A_{j+1}(\varepsilon) \supsetneq A_j(\varepsilon) \text{ or } A_{j+1}(\varepsilon) = \emptyset$$

for all $j \geq 0$.
The simple joint sparse form minimises the joint Hamming weight over all joint expansions of n_1, n_2.

Simple Joint Sparse Form

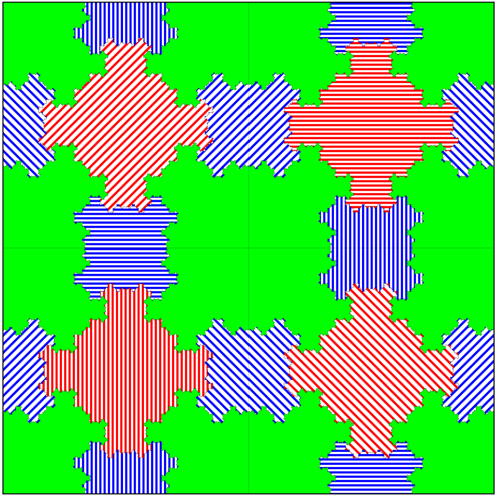
$$A_{j+1}(\varepsilon) \supsetneq A_j(\varepsilon) \text{ or } A_{j+1}(\varepsilon) = \emptyset$$

Regular expression (main term only; all sign combinations are allowed):

$$(\cdots)\cdot\left(\begin{matrix}0\\0\end{matrix} + \begin{matrix}0 & \pm1\\0 & 0\end{matrix} + \begin{matrix}0 & 0\\0 & \pm1\end{matrix} + \begin{matrix}0 & \pm1\\0 & \pm1\end{matrix} + \begin{matrix}0 & \pm1 & \pm1\\0 & \pm1 & 0\end{matrix} + \begin{matrix}0 & \pm1 & 0\\0 & \pm1 & \pm1\end{matrix}\right)^*$$

Similar Joint Sparse Form: Solinas 2001.

Simple Joint Sparse Form: Characteristic Sets



Digit (x_k, y_k) of SJSF of (m, n) given by set containing $(\{m/2^{k+2}\}, \{n/2^{k+2}\})$

Colour	x_k	y_k
green	0	0
blue, diagonal stripes (/)	0	1
blue, diagonal stripes (\)	0	-1
blue, vertical stripes	1	0
blue, horizontal stripes	-1	0
red, vertical stripes	1	1
red, diagonal stripes (/)	1	-1
red, diagonal stripes (\)	-1	1
red, horizontal stripes	-1	-1

Analysis

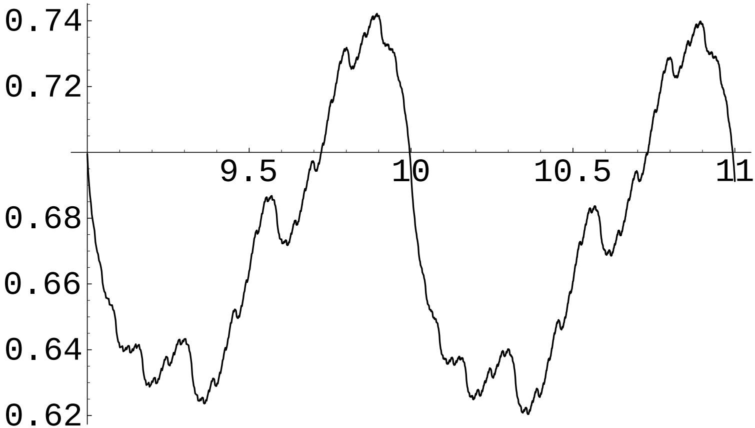
Theorem (Grabner-H.-Prodinger 2004)

The Hamming weight of the Joint Sparse Form of two positive integers satisfies the following asymptotic formula

$$S(N) = \sum_{m,n<N} h(m,n) = \frac{N^2}{2}\log_2 N + N^2\Phi(\log_2 N) + O(N^\alpha),$$

where Φ *is a continuous periodic function of period* 1 *and* $\alpha = 1.2107605332885233950\ldots$.

Analysis



Plot of $S(N)/N^2 - \frac{1}{2}\log_2 N$ over $\log_2 N$ for $N = 512, \ldots, 2048$.

Larger Digit Set

Take the digit set

$$D_{\ell,u} := \{j \in \mathbb{Z} : \ell \le j \le u\}, \text{ where } \ell \le 0 \le 1 \le u.$$

Note that we now allow even digits, too.
Choose w such that

$$2^{w-1} < \#D_{\ell,u} = u - \ell + 1 \le 2^w.$$

Then, for every residue class modulo 2^{w-1}, the set $D_{\ell,u}$ contains one or two representatives.
Task: Given an integer vector $\mathbf{n} \in \mathbb{Z}^d$, find a binary $D_{\ell,u}$-expansion of $\mathbf{n}$ minimising the joint Hamming weight!

Colexicographically Minimal Expansions

Consider the binary $D_{-3,5}$-expansions

$$\begin{pmatrix}1\\5\end{pmatrix} = \begin{pmatrix}0001\\0005\end{pmatrix}_2 = \begin{pmatrix}0001\\100\bar{3}\end{pmatrix}_2.$$

Attach the 0-1-word where 0 stands for a zero column and 1 for column containing a nonzero entry:

$$0001 \quad 1001.$$

The first word is called colexicographically smaller than the second one (the words are compared lexicographically from right to left).

Colexicographically Minimal vs. Minimal Joint Hamming Weight

Questions:

- Do colexicographically minimal expansions minimise the joint Hamming weight over all $D_{\ell,u}$-expansions?
- How to find colexicographically minimal expansions?

Both the NAF and the Simple Joint Sparse Form are $D_{-1,1}$-colexicographically minimal expansions.

Computing Colexicographically Minimal Expansions

Consider $D_{-1,3}$ and $\mathbf{n} = (12, -10)$

- Since both numbers are even, we have to write a zero-column and continue with $(6, -5)$.
- One of the numbers is odd, so we have to write a nonzero-column now. Column 2 will be a zero column iff we choose digits congruent to the numbers modulo 4.
  One choice for first digit: $6 \equiv 2 \pmod 4$. (Number for column 3 will be 1).
  Two choices for the second digit: $-5 \equiv -1 \pmod 4$ (Number for column 3 will be -1) or $-5 \equiv 3 \pmod 4$ (Number for column 3 will be -2).
  We therefore cannot avoid a nonzero column 3. We only have one representative $\equiv -2 \pmod 4$, thus choosing digit vector $\binom{2}{-1}$ leads to more flexibility in the next step.

Computing Colexicogr. Minimal Expansions (Cont.)

- Result:

$$\begin{pmatrix} 12 \\ -10 \end{pmatrix} = \begin{pmatrix} 1020 \\ \bar{1}0\bar{1}0 \end{pmatrix}_2$$

This leads to an online algorithm for computing a colexicographically minimal expansion. Can be realized by a transducer automaton (for fixed ℓ, u).

Uniqueness?

$D_{-3,5}$:

$$\begin{pmatrix}1\\5\\9\end{pmatrix} = \begin{pmatrix}0001\\0005\\1001\end{pmatrix}_2 = \begin{pmatrix}0001\\100\bar{3}\\1001\end{pmatrix}$$

Both are colexicographically minimal. Not unique.

What about the Joint Hamming Weight

Among all optimal expansions (with respect to the joint Hamming weight), take one which is colexicographically minimal.
Repeat the above argument to see that it has essentially the same shape as a colexicographically minimal expansion.

Theorem (H., Muir 2007)

Let ℓ, u be given. There is an online algorithm for computing a colexicographically minimal expansion.
Every colexicographically minimal expansion minimises the joint Hamming weight among all $D_{\ell,u}$-expansions of the given integer vector.

Digit set $\{0, 1, 3\}$

Consider binary expansions with digits $\{0, 1, 3\}$.

$$\begin{pmatrix}5\\9\end{pmatrix} = \begin{pmatrix}0101\\1001\end{pmatrix}_2 = \begin{pmatrix}0013\\0033\end{pmatrix}_2$$

The second expression has lower joint Hamming weight, but is colexicographically greater.

The precise structure of $D_{\ell,u}$ cannot be arbitrarily relaxed.

Left-To-Right Joint Expansion

An algorithm for computing a joint expansion with digits $\{0, 1, -1\}$ of minimal weight fromleft to right is available: H.-Katti-Prodinger-Ruan 2005.

Uses intermediate expansion with the property that nonzero digits alternate in sign (cancels carries).

Then lexicographically minimal expansions (from left to right) have minimal joint weight.

Frobenius Endomorphism

Let $a \in \{0, 1\}$. We consider the Koblitz Curve

$$E_a : y^2 + xy = x^3 + ax^2 + 1,$$

over some finite field $\mathbb{F}_{2^m}$ of characteristic 2. These are the only non-supersingular curves defined over $\mathbb{F}_2$.
Consider the Frobenius automorphism $\tau : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}; x \mapsto x^2$ and extend it to an endomorphism of $E_a(\mathbb{F}_{2^m})$.
For all $P \in E_a(\mathbb{F}_{2^m})$, we have

$$\tau(\tau(P)) + 2P = \mu\tau(P), \text{ where } \mu = (-1)^{1-a}.$$

In the endomorphism ring of E_a, this yields the equation

$$\tau^2 + 2 = \mu\tau.$$

The endomorphism τ can be identified with $\frac{\mu+\sqrt{-7}}{2}$.

τ-Expansions and Scalar Multiplication

Assume that a digit expansion of n to the base of τ is known, e.g., $n = \sum_{j=0}^{\ell-1} c_j \tau^j$ ($c_j \in \{0, 1\}$, $c_{\ell-1} \neq 0$). Then

$$(c_{\ell-1}\tau^{\ell-1} + c_{\ell-2}\tau^{\ell-2} + c_{\ell-3}\tau^{\ell-3} + \cdots + c_1\tau + c_0)P = \tau(\tau(\tau(\tau(\tau(c_{\ell-1}P) + c_{\ell-2}P) + c_{\ell-3}P)\cdots) + c_1P) + c_0P$$

(Horner's scheme; Frobenius-and-Add-Algorithm). This is a generalisation of the binary Double-and-Add-Algorithm, but an application of the Frobenius endomorphism is much faster than doubling.

- Number of (fast) Frobenius applications: length of the expansion.
- Number of Additions/Subtractions: Hamming weight (number of nonzero digits) of the expansion (minus one).

τ-Expansions

Does every $n \in \mathbb{Z}$ admit a base-τ-expansion $n = \sum_{j=0}^{\ell-1} c_j \tau^j$ ($c_j \in \{0, 1\}$, $c_{\ell-1} \neq 0$)? Yes.

Theorem (Kátai and Kovács 1981)

τ is a base of a canonical number system in $\mathbb{Z}[\tau]$, i.e., every $z \in \mathbb{Z}[\tau]$ can be represented by a unique τ-expansion

$$n = \sum_{j=0}^{\ell-1} c_j \tau^j, \qquad c_j \in \{0, 1\}, c_{\ell-1} \neq 0.$$

Introducing Redundancy

Increase the digit set $\mathcal{D}$ $\Rightarrow$ Introduce Redundancy in the digital expansion $\Rightarrow$ Decrease Hamming weight at the cost of precomputations.

Problem

Choose the τ-expansion of n with digits from $\{0\} \cup \mathcal{D}$ of minimum weight.

Simplest case: digit set $\mathcal{D} = \{\pm 1\}$ (here, no precomputation is necessary as $(-1) \cdot P = -P$ is free).

Example

$10 = -1 \cdot \tau^8 + 0 \cdot \tau^7 - 1 \cdot \tau^6 + 0 \cdot \tau^5 - 1 \cdot \tau^4 + 0 \cdot \tau^3 + 0 \cdot \tau^2 + 1 \cdot \tau + 0 \cdot \tau^0$ $(\mu = -1)$.

τ-NAF

Theorem (Solinas 1997, 2000)

For each $z \in \mathbb{Z}[\tau]$, there is a unique word $c_{\ell-1} \ldots c_0 \in \{0, \pm 1\}^*$ with $c_{\ell-1} \neq 0$ such that

$$z = \operatorname{value}_\tau(c_{\ell-1} \ldots c_0) := \sum_{j \geq 0} c_j \tau^j, \quad (c_{\ell-1} \ldots c_0 \text{ is a } \tau\text{-expansion of } z),$$

$$c_j c_{j+1} = 0 \qquad \text{for all } j \geq 0.$$

"τ-Non-Adjacent-Form (τ-NAF)".

Theorem (Gordon 1998)

The τ-NAF minimises the Hamming weight over all $\{0, \pm 1\}$-τ-expansions of n.

Computation of the τ-NAF

$$10 \equiv 0 \pmod{\tau} \qquad \frac{10}{\tau} = -5 - \tau$$

$$-5 - 5\tau \equiv 1 \pmod{\tau^2} \qquad \frac{(-5-\tau)-1}{\tau} = -2 + 3\tau$$

$$-2 + 3\tau \equiv 0 \pmod{\tau} \qquad \frac{-2+3\tau}{\tau} = 4 + \tau$$

$$4 + \tau \equiv 0 \pmod{\tau} \qquad \frac{4+\tau}{\tau} = -1 - 2\tau$$

$$-1 - 2\tau \equiv -1 \pmod{\tau^2} \qquad \frac{(-1-2\tau)+1}{\tau} = -2$$

$$-2 \equiv 0 \pmod{\tau} \qquad \frac{-2}{\tau} = 1 + \tau$$

$$1 + \tau \equiv -1 \pmod{\tau} \qquad \frac{(1+\tau)+1}{\tau} = -\tau$$

$$-\tau \equiv 0 \pmod{\tau} \qquad \frac{-\tau}{\tau} = -1$$

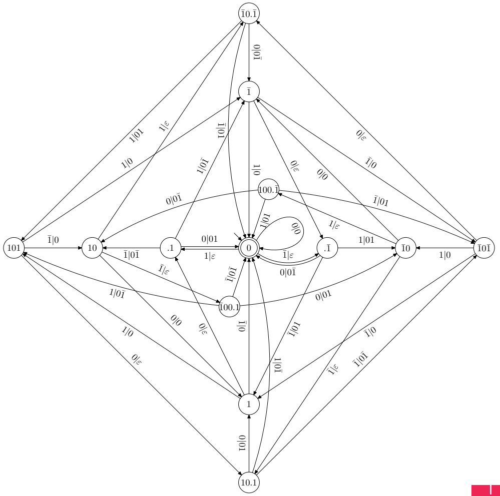
$$-1 \equiv -1 \pmod{\tau} \qquad \frac{(-1)+1}{\tau} = 0$$

$$10 = 0 + 1\tau + 0\tau^2 + 0\tau^3 + (-1)\tau^4 + 0\tau^5 + (-1)\tau^6 + 0\tau^7 + (-1)\tau^8$$

Computing the τ-NAF from any Expansion

$10 =$	0	0	1	-1	1	-1	-1	-1	0	(original)
$0 =$	-1	0	-2	1	-2	1	1	2	0	(carries)
$0 =$										(MinPoly)
$10 =$	-1	0	-1	0	-1	0	0	1	0	(result)

Transducer for computing the τ-NAF



Transducer to compute the τ-NAF from any signed τ-expansion from right to left, where $\mu = -1$.

$\mathcal{D}$-w-NAF

Choose $\mathcal{D} \subset \mathbb{Z}[\tau]$ such that $\mathcal{D}$ is a reduced residue system modulo τ^w and such that every $z \in \mathbb{Z}[\tau]$ admits a $\mathcal{D}$-w-NAF, i.e., an expansion

$$z = \sum_{j \geq 0} c_j \tau^j, \qquad c_j \in \{0\} \cup \mathcal{D}$$

with

$$c_j \neq 0 \text{ implies } c_{j+w-1} = \cdots = c_{j+1} = 0.$$

(every block of w digits contains at most one non-zero).
Such a $\mathcal{D}$ is called a w-Non-Adjacent-Digit-Set (w-NADS).
Computation of a w-NAF is analogous to that of the τ-NAF.
Termination!

Examples for w-NADS

$w = 1 \quad \mathcal{D} = \{1\}$ Canonical Number System,

$w = 2 \quad \mathcal{D} = \{\pm 1\}$ τ-NAF,

$w = 3 \quad \mathcal{D} = \{\pm 1, \pm(\tau^2 + 1)\}$,

$\vdots$

Representatives of Minimal Norm

Solinas (1997, 2000): For each residue class modulo τ^w coprime to τ, choose the representative of minimal norm (MNR(w)). This digit set is uniquely determined.

Theorem (Solinas 1997, 2000)

MNR(w) *is a w-Non-Adjacent-Digit-Set.*

Theorem (Blake-Kumar Murty-Xu 2005)

A symmetric (i.e., $d \in \mathcal{D} \implies -d \in \mathcal{D}$*) digit set* $\mathcal{D}$ *with* $1 \in \mathcal{D}$ *such that* $|d| < 2^{w/2}$ *for* $d \in \mathcal{D}$ *is a w-Non-Adjacent-Digit-Set.*

Short τ-NAF representatives

$$\mathrm{SNR}(w) = \{\,0\,\} \cup \Big\{\mathrm{value}(c_{w-1}\ldots c_0) : c_{w-1}\ldots c_0 \text{ is a } \tau\text{-NAF} \text{ with } c_0 \neq 0 \text{ and } c_{w-1} \in \{0, c_0\}\Big\}$$

Theorem (Avanzi, CH, Prodinger 2009+)

SNR(w) *is a w-NADS.*

Main Advantage:

- Easy Computation

Point Halving ($w = 3$)

For $w = 3$, the digit set of minimal norm representatives (and the only symmetric digit set of short τ-NAF representatives) is

$$\mathcal{D} = \{\pm 1, \pm\bar{\tau}\},$$

where $\bar{\tau} = \mu - \tau = -\mu(\tau^2 + 1)$ denotes the complex conjugate of τ. Note that we have $\tau\bar{\tau} = 2$.
We want to compute $zP = (\bar{\tau}z)(\tau(1/2P))$.
Set $Q := \tau(1/2P)$ (which can be computed easily from P).
Thus $P = \bar{\tau}Q$.

Theorem (Avanzi, H., Prodinger 2006)

zP can be computed by forming the $\{\pm 1, \pm\bar{\tau}\}$-3-NAF of $\bar{\tau}z$ and applying it to $Q = \tau(1/2P)$. The only precomputation is one point halving and one Frobenius application.

Optimality ($w = 3$)

Theorem (Avanzi, H., Prodinger 2006)

The $\{\pm 1, \pm\bar{\tau}\}$-3-NAF of a $z \in \mathbb{Z}[\tau]$ has minimal Hamming weight amongst all τ-expansions of z with digits $\{0, \pm 1, \pm\bar{\tau}\}$.

The proof uses 15 non deteriorating transformation rules or a transducer with 153 states.

Point Halving, General w

- Digit set: $\mathcal{D} = \{\pm\bar{\tau}^k : 0 \leq k < 2^{w-2}\}$.
- $\mathcal{D}$ is always a reduced residue system modulo τ^w.
- For $w \leq 6$, $\mathcal{D}$ is proven to be a w-NADS.
- For $w \in \{7, 8, 9, 10, 11, 12\}$, the set $\mathcal{D}$ is not a w-NADS.
- For a number with m digits, choose $w \approx \log_2 m - \log_2 \log_2 m$ for the first $\approx m(1 - \frac{1}{\log_2 m})$ digits and choose $w = 6$ for the remaining $\approx m/\log_2 m$ digits.
- Expected number of expensive curve operations: $O(m/\log m)$.
- Only point halvings are used in precomputations, no addition.

Avoiding Stored Precomputations

We want to compute zP. Fix w and $\mathcal{D} = \{\pm\bar{\tau}^k : 0 \le k < 2^{w-2}\}$.
Assume that normal bases are used, i.e., Frobenius applications are for free.
Write $y = \bar{\tau}^{2^{w-1}-1} z$ and consider its $\mathcal{D}$-w-NAF $y = \sum_{j\ge 0} \varepsilon_j \tau^j$.
Each nonzero digit ε_j can be written as $\varepsilon_j = s_j \bar{\tau}^{k_j}$ for suitable k_j and signs $s_j \in \{\pm 1\}$.
For each k, we collect the contribution of digits $\pm\bar{\tau}^k$ in $y^{(k)}$,

$$y^{(k)} = \sum_{\substack{j \\ \varepsilon_j = \pm\bar{\tau}^k}} s_j \tau^j,$$

which results in the decomposition

$$y = \sum_{k=0}^{2^{w-2}-1} y^{(k)} \bar{\tau}^k.$$

Avoiding Stored Precomputations (2)

So far, we have

$$y^{(k)} = \sum_{\substack{j \\ \varepsilon_j = \pm\bar{\tau}^k}} s_j \tau^j, \qquad y = \sum_{k=0}^{2^{w-2}-1} y^{(k)} \bar{\tau}^k.$$

We get

$$zP = \bar{\tau}^{-(2^{w-2}-1)} yP = \sum_{m=0}^{2^{w-2}-1} \left(\frac{\tau}{2}\right)^{2^{w-2}-1-m} y^{(m)} P.$$

This is evaluated by a Horner scheme in $\tau/2$, whose inner loop consists of the computation of $y^{(m)}P$ by a Horner scheme in τ, i.e., by a Frobenius-and-Add loop.

Algorithm for Normal Bases and Point Halving

INPUT: A Koblitz curve E_a, a point P of odd order on it, and a scalar z.
OUTPUT: zP

1. $y \leftarrow \bar{\tau}^{2^{w-2}-1} z$
   Write $y = \sum_{j=0}^{\ell} \varepsilon_j \tau^j$ where $\varepsilon_j \in \mathcal{D} := \{0\} \cup \pm\{\bar{\tau}^k : 0 \leq k < 2^{w-2}\}$
   Write $\varepsilon_j = s_j \bar{\tau}^{k_j}$ with $s_j \in \{0, \pm 1\}$
2. $\ell_k \leftarrow \max\left(\{-1\} \cup \{j : \varepsilon_j = \pm\bar{\tau}^k \text{ for some } k\}\right)$
3. $X \leftarrow 0$
4. **for** $k = 0$ **to** $2^{w-2} - 1$ **do**
5.   **if** $k > 0$ **then** $X \leftarrow \tau^{m-\ell_k} X$, $X \leftarrow \frac{1}{2} X$
6.   **for** $j = \ell_k$ **to** 0 **do**
7. $X \leftarrow \tau X$
8.   **if** $\varepsilon_j = \pm\bar{\tau}^k$ **then** $X \leftarrow X + s_j P$
9. **return** X

Example for Non-Optimality

Let $\mu = -1$, $w = 4$, $\mathcal{D} = \mathsf{MNR}(4) = \{0, \pm 1, \pm 1 \pm \tau, \pm(3 + \tau)\}$ (all signs are independent). Then

$$\text{value}(1000(-1-\tau)000(1-\tau)) = -9 = \text{value}((-3-\tau)00(-1)).$$

The $\mathcal{D}$-w-NAF has Hamming weight 3, the other expansion has Hamming weight 2 and is even shorter.
$\Rightarrow$ the MNR(4)-4-NAF is not optimal!

Chaotic Behaviour

Theorem (CH 2009+)

Consider $\mu = -1$, $w = 4$,
$\mathcal{D} = \mathrm{MNR}(4) = \{0, \pm 1, \pm 1 \pm \tau, \pm(3+\tau)\}$, *and*

$$z_\ell := \mathrm{value}\Big(0000(-1-\tau)\big(000(3+\tau)\big)^{(\ell)}0000(1+\tau)000(-1)\Big),$$

$$z'_\ell := \mathrm{value}\Big(1000(-1-\tau)\big(000(3+\tau)\big)^{(\ell)}0000(1+\tau)000(-1)\Big),$$

Here, $\big(000(3+\tau)\big)^{(\ell)}$ *means repetition of the block.*

$z_\ell \equiv z'_\ell \pmod{\tau^{4\ell+13}}$.

All optimal expansions of z_ℓ *start with* -1.

All optimal expansions of z'_ℓ *start with* $(1-\tau)$.

It is impossible to compute optimal expansions by a finite state transducer, it may be necessary to read the whole expansion.

"Chaotic behaviour"

Chaotic Behaviour

Known for . . .

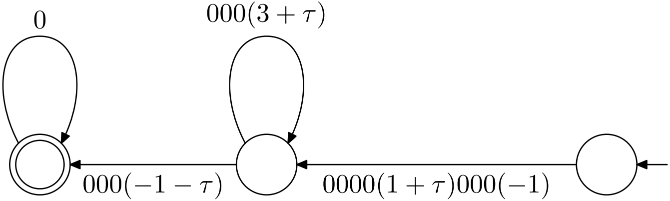
- $\mu = \pm 1$, $\tau^2 - \mu\tau + 2 = 0$, $\mathcal{D} \in \{$MNR(4), SNR(4), MNR(5), SNR(5), MNR(6), SNR(6), P$\bar{\tau}$(4), P$\bar{\tau}$(5)$\}$ (CH 2009+),
- $\mu = \pm 1$, $\tau^2 - \mu\tau + 2 = 0$, Joint expansions, $\mathcal{D} = \{0, \pm 1\}$ (CH 2009+)
- Base $\beta = -a \pm \sqrt{-1}$, $a \in \mathbb{Z}$, $a > 0$, $\mathcal{D} = \mathbb{Z}$. (Cost function: Sum of absolute values of the digits) (CH 2002)

Determining all Expansions of z_ℓ (1)

Consider $w = 4$, $\mu = -1$, $\mathcal{D} = \mathrm{MNR}(4)$ and

$$z_\ell := \mathrm{value}\Big(000(-1-\tau)\big(000(3+\tau)\big)^{(\ell)}0000(1+\tau)000(-1)\Big).$$

- z_ℓ is given by its 4-NAF.
- The language of the 4-NAFs of all z_ℓ, $\ell \geq 0$, is the language accepted by the finite state automaton $\mathcal{A}_R$.



Determining all Expansions of z_ℓ (2)

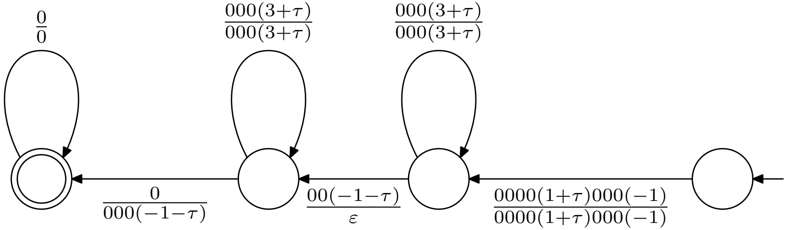
- There is a transducer automaton $\mathcal{A}_C$ converting arbitrary MNR(4)-expansions to the 4-NAF.
- It has 575 states. $\Rightarrow$ No Picture! 
- Concatenating this conversion transducer $\mathcal{A}_C$ with the recognition automaton $\mathcal{A}_R$ yields a huge automaton $\mathcal{A}_H$ recognising all expansions of some z_ℓ ($\ell \geq 0$) (the output of $\mathcal{A}_C$ is the input of $\mathcal{A}_R$).
- 2003 states, simplifying (pruning states from which the terminal state is not reachable) 608 states.
- Input Labels of $\mathcal{A}_H$: Input Labels of $\mathcal{A}_C$, i.e., arbitrary expansion of z_ℓ.
- Output Labels of $\mathcal{A}_H$: Output Labels of $\mathcal{A}_C$ = Labels of $\mathcal{A}_R$, i.e., 4-NAF of z_ℓ.

Determining Optimal Expansions of z_ℓ

- Assign weights to the transitions of $\mathcal{A}_H$: Hamming weight of the input expansion minus Hamming weight of the output expansion (4-NAF).
- Weight of a successful path (input label: expansion of some z_ℓ): Hamming weight of the input expansion minus Hamming weight of the 4-NAF = Deterioration of the arbitrary expansion compared to the 4-NAF.
- Optimal Expansion = Minimal Deterioration = Shortest Path.
- Shortest Path Computation (Bellman-Ford-Algorithm) (special structure of the digraph: several layers $\Rightarrow$ efficient)
- No Negative Cost Cycle, length of shortest path: 0 (4-NAF of z_ℓ is optimal, but there are other optimal expansions, too).
- Remove transitions not contained in any shortest path (using vertex potentials).

Determining Optimal Expansions of z_ℓ (2)

- Resulting transducer:

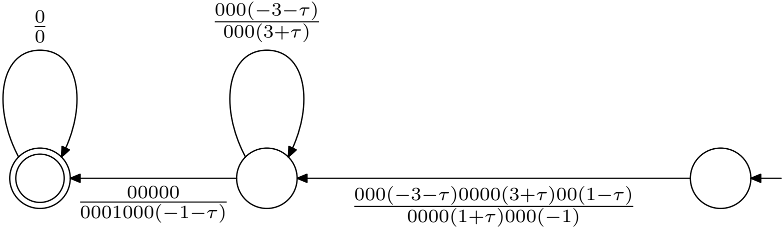


- All optimal expansions of all z_ℓ start with -1.

Optimal Expansions of z'_ℓ

$$z'_\ell := \mathsf{value}\Big(1000(-1-\tau)\big(000(3+\tau)\big)^{(\ell)}0000(1+\tau)000(-1)\Big).$$

- ...
- No Negative Cost Cycle, length of shortest path: -1 (4-NAF is optimal up to one).
- Resulting transducer:



- All optimal expansions of all z'_ℓ start with $(1-\tau)$.

Other Digit Sets

w	μ	$\mathcal{D}$	
4	μ ($\ell \geq 0$)	MNR	$\mathsf{NAF}(z_\ell) = 0^\omega(\mu-\tau)\,(000(-3\mu+\tau))^{(\ell)}\,0000(1-\mu\tau)000(-1)$ $\mathsf{opt}(z_\ell) = \{0^\omega\,(000(3-\mu\tau))^{(\ell_2)}\,00(\mu-\tau)\,(000(-3\mu+\tau))^{(\ell_1)}\,0000(1-\mu\tau)000(-1) \mid \ell_1,\ell_2 \geq 0 \text{ and } \ell_1+\ell_2=\ell\}$ $\mathsf{NAF}(z'_\ell) = 0^\omega(-\mu)000(\mu-\tau)\,(000(-3\mu+\tau))^{(\ell)}\,0000(1-\mu\tau)\,000(-1)$ $\mathsf{opt}(z_\ell) = \{0^\omega\,(000(-3+\mu\tau))^{(\ell+1)}\,0000(-3\mu+\tau)00(1+\mu\tau)\}$
4	-1 ($\ell \geq 0$)	SNR	$\mathsf{NAF}(z_\ell) = 0^\omega(-1)\,(0000(-3+\tau)0)^{(\ell)}\,00(3-\tau)$ $\mathsf{opt}(z_\ell) = 0^\omega\,(00000(-3+\tau))^{(\ell)}\,001$ $\mathsf{NAF}(z'_\ell) = 0^\omega\,(00000(-3+\tau))^{(\ell)}\,000(3-\tau)$ $\mathsf{opt}(z_\ell) = 0^\omega\,(00000(-3+\tau))^{(\ell)}\,000(3-\tau)$
5	-1 ($\ell \geq 1$)	MNR	$\mathsf{NAF}(z_\ell) = 0^\omega(1-2\tau)\,(00000(-3-\tau))^{(\ell)}\,0000(1+3\tau)$ $\mathsf{opt}(z_\ell) = \{0^\omega(1-2\tau)\,(00000(-3-\tau))^{(\ell)}\,0000(1+3\tau)\}$ $\mathsf{NAF}(z'_\ell) = 0^\omega(-1)\,(0000(-3-\tau)0)^{(\ell)}\,000(1+3\tau)$ $\mathsf{opt}(z'_\ell) = \{0^\omega\,(00000(1+3\tau))^{(\ell)}\,000(-1)\}$
5	1 ($\ell \geq 1$)	MNR	$\mathsf{NAF}(z_\ell) = 0^\omega(-1+2\tau)00\,(00000(3-\tau))^{(\ell)}\,0000(1-3\tau)$ $\mathsf{opt}(z_\ell) = \{0^\omega(-1+2\tau)00\,(00000(3-\tau))^{(\ell)}\,0000(1-3\tau)\}$ $\mathsf{NAF}(z'_\ell) = 0^\omega(-1)\,(0000(3-\tau)0)^{(\ell)}\,000(1-3\tau)$ $\mathsf{opt}(z'_\ell) = \{0^\omega\,(00000(1-3\tau))^{(\ell)}\,000(-1)\}$
5	-1 ($\ell \geq 0$)	SNR	$\mathsf{NAF}(z_\ell) = 0^\omega(-1-\tau)\,(0000(-5-4\tau)000000(-5-4\tau))^{(\ell)}$ $0000(-5-4\tau)0000(3+3\tau)$ $\mathsf{opt}(z_\ell) = \{0^\omega\,(000000(-5-4\tau)0000(-5-4\tau))^{(\ell)}$ $000000(-3-3\tau)0001\}$ $\mathsf{NAF}(z'_\ell) = 0^\omega\,(0000(-5-4\tau)000000(-5-4\tau))^{(\ell)}$ $0000(-5-4\tau)0000(3+3\tau)$ $\mathsf{opt}(z'_\ell) = \{0^\omega\,(0000(-5-4\tau)000000(-5-4\tau))^{(\ell)}$ $0000(-5-4\tau)0000(3+3\tau)\}$
5	1 ($\ell \geq 1$)	SNR	$\mathsf{NAF}(z_\ell) = 0^\omega 1\,(000000(5-4\tau)0000(-5+4\tau))^{(\ell)}$ $0000(-3+\tau)0000(3-3\tau)$ $\mathsf{opt}(z_\ell) = \{0^\omega\,(0000000(-5+4\tau)000(-5+4\tau))^{(\ell)}$ $0000000(-5+4\tau)00(3+\tau)\}$ $\mathsf{NAF}(z'_\ell) = 0^\omega(-1+\tau)\,(0000(5-4\tau)0000(-5+4\tau)00)^{(\ell)}$ $00(-3+\tau)0000(3-3\tau)$ $\mathsf{opt}(z'_\ell) = \{0^\omega(1-\tau)\,(0000000(-5+4\tau)000(-5+4\tau))^{(\ell)}$ $0000(3-3\tau)\}$
5	-1 ($\ell \geq 0$)	$\mathsf{P}\bar{\tau}$	$\mathsf{NAF}(z_\ell) = 0^\omega(1+\tau)\,(00000(5-\tau))^{(\ell)}\,0000(-1-3\tau)$ $\mathsf{opt}(z_\ell) = \{0^\omega\,(00000(-1-3\tau))^{(\ell_2)}\,000(1+\tau)$ $(00000(5-\tau))^{(\ell_1)}\,0000(-1-3\tau)$

TABLE 1. Explicit elements z_ℓ and z'_ℓ for Theorem 1. For $w=4$, $\mu=1$ we have $\mathsf{SNR}(4)=\mathsf{MNR}(4)$. For $w=5$, $\mu=1$, $\mathcal{D}=\mathsf{P}\bar{\tau}(5)$, $\mathsf{opt}(z_\ell)$ is given by a regular expression, where "$\Vert$" denotes alternatives and * denotes the Kleene star.

w	μ	$\mathcal{D}$	
			$\mid \ell_1,\ell_2 \geq 0 \text{ and } \ell_1+\ell_2=\ell\}$ $\mathsf{NAF}(z'_\ell) = 0^\omega(1+\tau)0000(1+\tau)\,(00000(5-\tau))^{(\ell)}$ $0000(-1-3\tau)$ $\mathsf{opt}(z'_\ell) = \{0^\omega\,(00000(-3+7\tau))^{(\ell)}\,00000(-3+7\tau)00(-1+\tau)\}$
5	1 ($\ell \geq 0$)	$\mathsf{P}\bar{\tau}$	$\mathsf{NAF}(z_\ell) = 0^\omega(-1)\,(000000(-7+5\tau))^{(\ell+1)}$ $00000(-3+\tau)0000(-1+3\tau)$ $\mathsf{opt}(z_\ell) = \{\boldsymbol{\eta} \in 0^\omega\big(0000000000(5+\tau)00(3-\tau)$ $\Vert\,000000000(3-\tau)000(-5-\tau)$ $\Vert\,000000000000(-3+\tau)(-3-7\tau)$ $\Vert\,000000(-1+\tau)\big)^*$ $0000000000000(-3-7\tau)00000(-3-7\tau)(-1)$ $\mid \mathsf{length}(\boldsymbol{\eta}) = 23+7\ell\}$ $\mathsf{NAF}(z'_\ell) = 0^\omega\,(000000(-7+5\tau))^{(\ell)}\,00000(-3+\tau)$ $0000(-1+3\tau)$ $\mathsf{opt}(z'_\ell) = \{0^\omega\,(000000(-7+5\tau))^{(\ell)}\,000000000(3+7\tau)(-3+\tau),$ $0^\omega\,(000000(-7+5\tau))^{(\ell)}\,00000(-3+\tau)$ $0000(-1+3\tau)\}$
6	-1 ($\ell \geq 1$)	MNR	$\mathsf{NAF}(z_\ell) = 0^\omega 100000(1+3\tau)\,(00000(5+3\tau))^{(\ell)}\,00000(3+4\tau)$ $\mathsf{opt}(z_\ell) = \{0^\omega(3+4\tau)\,(00000(5+3\tau))^{(\ell)}\,0000(-1-2\tau)\}$ $\mathsf{NAF}(z'_\ell) = 0^\omega(1+3\tau)\,(00000(5+3\tau))^{(\ell)}\,00000(3+4\tau)$ $\mathsf{opt}(z'_\ell) = \{0^\omega(1+3\tau)\,(00000(5+3\tau))^{(\ell)}\,00000(3+4\tau)\}$
6	1 ($\ell \geq 1$)	MNR	$\mathsf{NAF}(z_\ell) = 0^\omega(1-3\tau)\,(00000(5-3\tau))^{(\ell)}\,00000(3-4\tau)$ $\mathsf{opt}(z_\ell) = \{0^\omega(1-3\tau)\,(00000(5-3\tau))^{(\ell)}\,00000(3-4\tau)\}$ $\mathsf{NAF}(z'_\ell) = 0^\omega 100000(1-3\tau)\,(00000(5-3\tau))^{(\ell)}\,00000(3-4\tau)$ $\mathsf{opt}(z'_\ell) = \{0^\omega(-3+4\tau)\,(00000(-5+3\tau))^{(\ell)}\,0000(-1+2\tau)\}$
6	-1 ($\ell \geq 1$)	SNR	$\mathsf{NAF}(z_\ell) = 0^\omega\,(000000(1-2\tau))^{(\ell)}\,00000(-5-\tau)$ $\mathsf{opt}(z_\ell) = \{0^\omega\,(000000(1-2\tau))^{(\ell)}\,00000(-5-\tau)\}$ $\mathsf{NAF}(z'_\ell) = 0^\omega(-1)(00000(1-2\tau)0)^{(\ell)}0000(-5-\tau)$ $\mathsf{opt}(z'_\ell) = \{0^\omega\,(000000(-5-4\tau))^{(\ell)}\,00001\}$
6	1 ($\ell \geq 1$)	SNR	$\mathsf{NAF}(z_\ell) = 0^\omega(3-\tau)\,(000000000900000000(-9))^{(\ell)}$ $000000(1-3\tau)00000(7-\tau)$ $\mathsf{opt}(z_\ell) = \{0^\omega(3-\tau)\,(000000000900000000(-9))^{(\ell)}$ $000000(1-3\tau)00000(7-\tau)\}$ $\mathsf{NAF}(z'_\ell) = 0^\omega 100000(1-3\tau)\,(0000000900000000(-9)0)^{(\ell+1)}$ $00000(1-3\tau)00000(7-\tau)$ $\mathsf{opt}(z'_\ell) = \{0^\omega(-9)\,(00000000(9-2\tau)00000000(-9+2\tau))^{(\ell)}$ $00000000(9-2\tau)000000(3+\tau)$ $0000000(-9+2\tau)000(-1+3\tau)\}$

TABLE 1. Explicit elements z_ℓ and z'_ℓ for Theorem 1 (continued).

Symbolic Computations with Automata

- Guess critical pairs z_ℓ, z'_ℓ from experiments (depth search) and rewrite them manually as regular expressions.
- Construct all automata in Mathematica (automatically)
- Interpret resulting transducer manually.
- Largest case: $w = 6$, $\mu = 1$, $\mathcal{D} = \mathrm{SNR}(6)$, $\mathcal{A}_H$ has 235 138 states, 65 days on a Intel® Core™ 2 Duo CPU E6850 at 3.00 GHz running Mathematica® 5.2 under Linux 2.6.22.

Joint expansions

- Let $n_1, n_2 \in \mathbb{Z}[\tau]$ and consider a signed joint expansion $(c_j^{(i)})_{\substack{i=1,2\\ j\geq 0}} \in \{-1, 0, 1\}^{\{1,2\}\times\mathbb{N}_0}$ of n_1 and n_2, i.e.,

$$n_i = \sum_{j\geq 0} c_j^{(i)} \tau^i.$$

- Joint Hamming weight: number of nonzero columns (corresponds to the number of additions when computing a linear combination $n_1P_1 + n_2P_2$ of two points P_1, P_2 using the precomputed points $P_1 \pm P_2$ on an elliptic curve).

τ-Joint Sparse Form

- τ-Joint-Sparse-Form (Ciet, Lange, Sica, Quisquater 2003): Syntactically defined expansion, analogous to binary case, not optimal. Expected density: 0.5.
- various proposals . . .
- E.g., transducer with 14889 states (CH, unpublished), expected density 0.475102
- Chaos proved.