An algorithm for optimal joint expansion with odd digits

Clemens Heuberger and Dunja Pucher

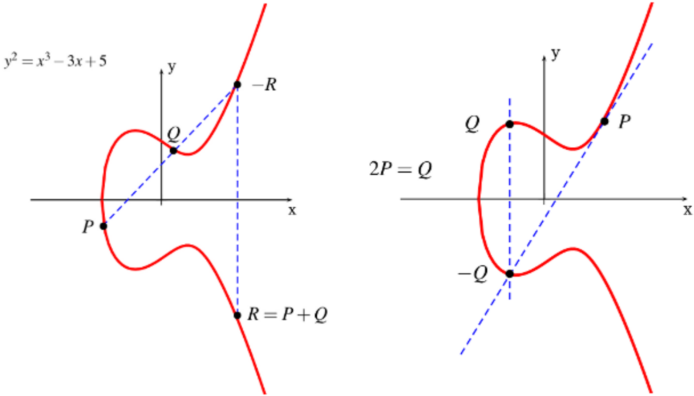
University of Klagenfurt

(Joint) Digit Expansions

$$13 = (1101)_2 \qquad \begin{pmatrix} 13 \\ 5 \end{pmatrix} = \begin{pmatrix} 1101 \\ 0101 \end{pmatrix}_2$$

- dimension ($d = 1$, $d = 2$)
- radix or basis ($r = 2$)
- digit set ($D = \{0, 1\}$)
- length ($\ell = 4$)
- (joint) Hamming weight ($w = 3$)

Cryptography over elliptic curves



$\Rightarrow$ double and add method

Double and add method & digit expansions

Calculate $13P$:

$$13 = (1101)_2$$
$$13P = 2(2(2(P) + P) + 0) + P$$

Calculate $13P + 5Q$ with Strauss' Algorithm ($P + Q$):

$$\begin{pmatrix} 13 \\ 5 \end{pmatrix} = \begin{pmatrix} 1101 \\ 0101 \end{pmatrix}_2$$
$$13P + 5Q = 2(2(2(P) + P + Q) + 0) + P + Q$$

$\#$ doublings $\sim$ length of the expansion
$\#$ additions $\sim$ (joint) Hamming weight of the expansion

Low-weight digit expansions

- increase number of zero columns
- introduce negative digits $\Rightarrow$ redundant number systems

Algorithms for minimal weight joint expansions

- $D = \{0, \pm 1\}$
  - Joint Sparse Form (JSF): Solinas, 2001, $d = 2$
  - Generalization of JSF: Proos, 2003, $d \geq 2$
  - Simple JSF: Grabner, Heuberger, Prodinger, 2004, $d \geq 2$
- other digit sets with **odd digits**
  - approximation algorithms
  - precomputed minimal average weights

Algorithm for $d = 2$ and $D = \{0, \pm 1, \pm 3\}$

Data: $N = (m, n)^T$, $m, n \in \mathbb{Z}$, $D = \{0, \pm 1, \pm 3\}$
Result: $A_{s-1} \dots A_1 A_0$, a minimal weight joint expansion
$s \leftarrow 0$
while $N \neq 0$ **do**
  select digits from D to form A_s, the least significant column of a representation of N
  $N \leftarrow \frac{1}{2}(N - A_s)$
  $s \leftarrow s + 1$
end

Output

$$\begin{pmatrix} 5 \\ 7 \end{pmatrix} = \cancel{\begin{pmatrix} 13 \\ 31 \end{pmatrix}_2} = \begin{pmatrix} 101 \\ 103 \end{pmatrix}_2 = \begin{pmatrix} 100\bar{3} \\ 100\bar{1} \end{pmatrix}_2$$

Shape Condition for pairs of integers

$$\begin{pmatrix} 73 \\ 47 \end{pmatrix} = \begin{pmatrix} 33001 \\ 3000\bar{1} \end{pmatrix}_2$$

- of any three consecutive columns at least one is a zero column
- a column with two odd digits is followed by a zero column
- a property regarding adjacent odd digits

Digit set $D = \{0, \pm 1, \pm 3\}$

- an even integer $\Rightarrow$ select digit $d = 0$
- an odd integer $\Rightarrow$ select a digit $d \in \{\pm 1, \pm 3\}$

Example: integer 27

$$\begin{aligned} d = 3 &\Rightarrow 27 - 3 = 24 \equiv 0 \pmod 8 \\ d = 1 &\Rightarrow 27 - 1 = 26 \equiv 2 \pmod 8 \\ d = -1 &\Rightarrow 27 + 1 = 28 \equiv 4 \pmod 8 \\ d = -3 &\Rightarrow 27 + 3 = 30 \equiv 6 \pmod 8 \end{aligned}$$

$\Rightarrow$ the digit set D contains a unique representative for all odd residue classes modulo 8

Case studies

- both integers are even
- both integers are odd
- one integer is odd and the other one is even

Results regarding the algorithm for $D = \{0, \pm 1, \pm 3\}$

- algorithm terminates
- outputs of the algorithm fulfil predefined syntactic constraints
- necessary look-ahead for a selection of the digits is 7

Finite State Machines (Transducers)

- convert binary expansions into expansions computed with the algorithm
- weight expansions computed with the algorithm
- convert arbitrary inputs with digits from D into expansions computed with the algorithm

Asymptotic moments for an expansion of length ℓ

- expectation: $281/786\ell + \mathcal{O}(1) \sim 0.36\ell + \mathcal{O}(1)$
- variance: $1397284/60698457\ell + \mathcal{O}(1) \sim 0.02\ell + \mathcal{O}(1)$

Bellman–Ford Algorithm

- there is no shorter path

Complexity

	$D = \{0, \pm1, \pm3\}$	$D = \{0, \pm1\}$
Precomputation	12 points	2 points
Average weight	0.36ℓ	0.5ℓ

$\Rightarrow$ costs for precomputation are offset after 71 bit

Thank you for your attention!

clemens.heuberger@aau.at
dupucher@edu.aau.at