Analysis of the Binary Asymmetric Joint Sparse Form

Clemens Heuberger* Sara Kropf

Alpen-Adria-Universität Klagenfurt and TU Graz
Supported by the Austrian Science Fund: W1230

Menorca, 2013-05-29

Digital Expansions and Scalar Multiplication

Scalar multiplication nP in abelian group G ($P \in G$, $n \in \mathbb{N}$) using digital expansion

$$n = \sum_{j=0}^{\ell-1} \eta_j 2^j$$

with digits from some digit set $\mathcal{D} \subseteq \mathbb{Z}$:

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

Digital Expansions and Scalar Multiplication

Scalar multiplication nP in abelian group G ($P \in G$, $n \in \mathbb{N}$) using digital expansion

$$n = \sum_{j=0}^{\ell-1} \eta_j 2^j$$

with digits from some digit set $\mathcal{D} \subseteq \mathbb{Z}$:

$$27 = \operatorname{value}_2(100\bar{1}0\bar{1}), \qquad (\bar{1} := -1)$$

$$(1 \qquad)_2 P = \qquad P \qquad .$$

Digital Expansions and Scalar Multiplication

Scalar multiplication nP in abelian group G ($P \in G$, $n \in \mathbb{N}$) using digital expansion

$$n = \sum_{j=0}^{\ell-1} \eta_j 2^j$$

with digits from some digit set $\mathcal{D} \subseteq \mathbb{Z}$:

$$27 = \mathrm{value}_2(100\bar{1}0\bar{1}), \qquad (\bar{1} := -1)$$

$$(10\qquad)_2 P = \qquad 2(P) + 0 \qquad .$$

Digital Expansions and Scalar Multiplication

Scalar multiplication nP in abelian group G ($P \in G$, $n \in \mathbb{N}$) using digital expansion

$$n = \sum_{j=0}^{\ell-1} \eta_j 2^j$$

with digits from some digit set $\mathcal{D} \subseteq \mathbb{Z}$:

$$27 = \mathrm{value}_2(100\bar{1}0\bar{1}), \qquad (\bar{1} := -1)$$

$$(100\quad)_2 P = \qquad 2(2(P) + 0) + 0 \qquad .$$

Digital Expansions and Scalar Multiplication

Scalar multiplication nP in abelian group G ($P \in G$, $n \in \mathbb{N}$) using digital expansion

$$n = \sum_{j=0}^{\ell-1} \eta_j 2^j$$

with digits from some digit set $\mathcal{D} \subseteq \mathbb{Z}$:

$$27 = \mathrm{value}_2(100\bar{1}0\bar{1}), \qquad (\bar{1} := -1)$$

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

Digital Expansions and Scalar Multiplication

Scalar multiplication nP in abelian group G ($P \in G$, $n \in \mathbb{N}$) using digital expansion

$$n = \sum_{j=0}^{\ell-1} \eta_j 2^j$$

with digits from some digit set $\mathcal{D} \subseteq \mathbb{Z}$:

$$27 = \mathrm{value}_2(100\bar{1}0\bar{1}), \qquad (\bar{1} := -1)$$

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

Digital Expansions and Scalar Multiplication

Scalar multiplication nP in abelian group G ($P \in G$, $n \in \mathbb{N}$) using digital expansion

$$n = \sum_{j=0}^{\ell-1} \eta_j 2^j$$

with digits from some digit set $\mathcal{D} \subseteq \mathbb{Z}$:

$$27 = \operatorname{value}_2(100\bar{1}0\bar{1}), \qquad (\bar{1} := -1)$$

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

Digital Expansions and Scalar Multiplication

Scalar multiplication nP in abelian group G ($P \in G$, $n \in \mathbb{N}$) using digital expansion

$$n = \sum_{j=0}^{\ell-1} \eta_j 2^j$$

with digits from some digit set $\mathcal{D} \subseteq \mathbb{Z}$:

$$27 = \mathrm{value}_2(100\bar{1}0\bar{1}), \qquad (\bar{1} := -1)$$

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

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

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

Digital Expansions and Scalar Multiplication

Scalar multiplication nP in abelian group G ($P \in G$, $n \in \mathbb{N}$) using digital expansion

$$n = \sum_{j=0}^{\ell-1} \eta_j 2^j$$

with digits from some digit set $\mathcal{D} \subseteq \mathbb{Z}$:

$$27 = \mathrm{value}_2(100\bar{1}0\bar{1}), \qquad (\bar{1} := -1)$$

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

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

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

Digital Expansions and Scalar Multiplication

Scalar multiplication nP in abelian group G ($P \in G$, $n \in \mathbb{N}$) using digital expansion

$$n = \sum_{j=0}^{\ell-1} \eta_j 2^j$$

with digits from some digit set $\mathcal{D} \subseteq \mathbb{Z}$:

$$27 = \mathrm{value}_2(100\bar{1}0\bar{1}), \qquad (\bar{1} := -1)$$

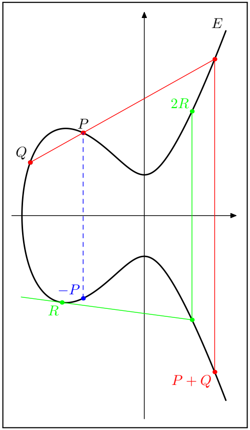
$$27P = (100\bar{1}0\bar{1})_2 P = 2(2(2(2(2(P) + 0) + 0) - P) + 0) - P.$$

- Number of additions/subtractions $\sim$ Hamming weight of the binary expansion
- Number of multiplications $\sim$ length of the expansion
- Precompute ηP for digits $\eta \in \mathcal{D}$.

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

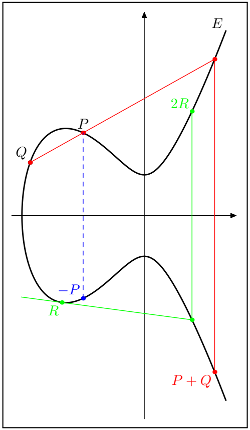
Application: Elliptic Curve Cryptography

- Elliptic Curve $E : y^2 = x^3 + ax^2 + bx + c$



Application: 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!

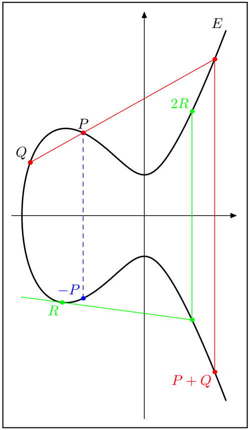


Application: Elliptic Curve Cryptography

- 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!
- In some elliptic curve cryptosystems (Elliptic Curve Digital Signature Algorithm (ECDSA) and El Gamal), the calculation of

$$\ell P + mQ \text{ or } \ell P + mQ + nR$$

for $\ell, m, n \in \mathbb{Z}$ and $P, Q, R \in E$ is also necessary.



Joint Expansions for Linear Combinations

Instead of computing ℓP and mQ separately and adding the results $\ell P + mQ$:

Joint Expansions for Linear Combinations

Instead of computing ℓP and mQ separately and adding the results $\ell P + mQ$:

- Compute digital expansion ("joint expansion") of the vector

$$\begin{pmatrix} \ell \\ m \end{pmatrix} = \sum_{j=0}^{\ell-1} \boldsymbol{\eta}_j 2^j$$

where the digits $\boldsymbol{\eta}_j$ are now vectors.

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

Joint Expansions for Linear Combinations

Instead of computing ℓP and mQ separately and adding the results $\ell P + mQ$:

- Compute digital expansion ("joint expansion") of the vector

$$\begin{pmatrix} \ell \\ m \end{pmatrix} = \sum_{j=0}^{\ell-1} \boldsymbol{\eta}_j 2^j$$

  where the digits $\boldsymbol{\eta}_j$ are now vectors.

- Precompute $\eta^{(1)} P + \eta^{(2)} Q$ for all $\boldsymbol{\eta} = \left(\begin{smallmatrix} \eta^{(1)} \\ \eta^{(2)} \end{smallmatrix}\right) \in \mathcal{D}$.

Joint Expansions for Linear Combinations

Instead of computing ℓP and mQ separately and adding the results $\ell P + mQ$:

- Compute digital expansion ("joint expansion") of the vector

$$\begin{pmatrix} \ell \\ m \end{pmatrix} = \sum_{j=0}^{\ell-1} \boldsymbol{\eta}_j 2^j$$

  where the digits $\boldsymbol{\eta}_j$ are now vectors.
- Precompute $\eta^{(1)} P + \eta^{(2)} Q$ for all $\boldsymbol{\eta} = \left(\begin{smallmatrix} \eta^{(1)} \\ \eta^{(2)} \end{smallmatrix}\right) \in \mathcal{D}$.
- Number of group additions $\sim$ number of nonzero digit vectors ("joint weight").

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

Asymmetric Joint Sparse Form

- For joint expansions of vectors of dimension d, consider the digit set
$$\mathcal{D} = \{\ell, \dots, -1, 0, 1, \dots, u\}^d$$
for $\ell \leq 0$ and $u \geq 1$.

Asymmetric Joint Sparse Form

- For joint expansions of vectors of dimension d, consider the digit set
$$\mathcal{D} = \{\ell, \dots, -1, 0, 1, \dots, u\}^d$$
for $\ell \leq 0$ and $u \geq 1$.
- For given $\mathbf{n} \in \mathbb{Z}^d$, find a joint expansion over the digit set $\mathcal{D}$ minimising the joint weight over all such expansions.

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

Asymmetric Joint Sparse Form

- For joint expansions of vectors of dimension d, consider the digit set
$$\mathcal{D} = \{\ell, \dots, -1, 0, 1, \dots, u\}^d$$
for $\ell \leq 0$ and $u \geq 1$.
- For given $\mathbf{n} \in \mathbb{Z}^d$, find a joint expansion over the digit set $\mathcal{D}$ minimising the joint weight over all such expansions.
- The minimal expansion is called the Asymmetric Joint Sparse Form.

Asymmetric Joint Sparse Form

- For joint expansions of vectors of dimension d, consider the digit set
$$\mathcal{D} = \{\ell, \ldots, -1, 0, 1, \ldots, u\}^d$$
for $\ell \leq 0$ and $u \geq 1$.
- For given $\mathbf{n} \in \mathbb{Z}^d$, find a joint expansion over the digit set $\mathcal{D}$ minimising the joint weight over all such expansions.
- The minimal expansion is called the Asymmetric Joint Sparse Form.
- Analyse the joint weight of this expansion.

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

Colexicographically Minimal Expansion

- Consider two joint expansions $\eta_{L-1} \ldots \eta_0$ and $\eta'_{L-1} \ldots \eta'_0$ of the same integer vector $\mathbf{n}$.

Colexicographically Minimal Expansion

- Consider two joint expansions $\boldsymbol{\eta}_{L-1} \ldots \boldsymbol{\eta}_0$ and $\boldsymbol{\eta}'_{L-1} \ldots \boldsymbol{\eta}'_0$ of the same integer vector $\mathbf{n}$.
- Set $c_j = [\boldsymbol{\eta}_j \neq 0]$ and $c'_j = [\boldsymbol{\eta}'_j \neq 0]$ for all j.

Colexicographically Minimal Expansion

- Consider two joint expansions $\boldsymbol{\eta}_{L-1} \ldots \boldsymbol{\eta}_0$ and $\boldsymbol{\eta}'_{L-1} \ldots \boldsymbol{\eta}'_0$ of the same integer vector $\mathbf{n}$.
- Set $c_j = [\boldsymbol{\eta}_j \neq 0]$ and $c'_j = [\boldsymbol{\eta}'_j \neq 0]$ for all j.
- We say that $\boldsymbol{\eta}_{L-1} \ldots \boldsymbol{\eta}_0$ is colexicographically smaller than $\boldsymbol{\eta}'_{L-1} \ldots \boldsymbol{\eta}'_0$ if there is a J such that

$$c_J < c'_J, \quad c_{J-1} = c'_{J-1}, \ldots, c_0 = c'_0.$$

Colexicographically Minimal Expansion

- Consider two joint expansions $\boldsymbol{\eta}_{L-1} \dots \boldsymbol{\eta}_0$ and $\boldsymbol{\eta}'_{L-1} \dots \boldsymbol{\eta}'_0$ of the same integer vector $\mathbf{n}$.
- Set $c_j = [\boldsymbol{\eta}_j \neq 0]$ and $c'_j = [\boldsymbol{\eta}'_j \neq 0]$ for all j.
- We say that $\boldsymbol{\eta}_{L-1} \dots \boldsymbol{\eta}_0$ is colexicographically smaller than $\boldsymbol{\eta}'_{L-1} \dots \boldsymbol{\eta}'_0$ if there is a J such that

$$c_J < c'_J, \quad c_{J-1} = c'_{J-1}, \dots, c_0 = c'_0.$$

- We say that $\boldsymbol{\eta}_{L-1} \dots \boldsymbol{\eta}_0$ is a colexicographically minimal expansion if there is no colexicographically smaller expansion of the same integer vector.

Colexicographically Minimal Expansion

- Consider two joint expansions $\boldsymbol{\eta}_{L-1} \dots \boldsymbol{\eta}_0$ and $\boldsymbol{\eta}'_{L-1} \dots \boldsymbol{\eta}'_0$ of the same integer vector $\mathbf{n}$.
- Set $c_j = [\boldsymbol{\eta}_j \neq 0]$ and $c'_j = [\boldsymbol{\eta}'_j \neq 0]$ for all j.
- We say that $\boldsymbol{\eta}_{L-1} \dots \boldsymbol{\eta}_0$ is colexicographically smaller than $\boldsymbol{\eta}'_{L-1} \dots \boldsymbol{\eta}'_0$ if there is a J such that

$$c_J < c'_J, \quad c_{J-1} = c'_{J-1}, \dots, c_0 = c'_0.$$

- We say that $\boldsymbol{\eta}_{L-1} \dots \boldsymbol{\eta}_0$ is a colexicographically minimal expansion if there is no colexicographically smaller expansion of the same integer vector.
- Example:

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

First expansion is colexicographically smaller.

Colexicographically Minimal Expansions (2)

- "colexicographically" = "lexicographically from right to left, i.e., least significant to most significant digit"

Colexicographically Minimal Expansions (2)

- "colexicographically" = "lexicographically from right to left, i.e., least significant to most significant digit"
- colexicographically minimal expansion: greedy for zeros from right to left.

Colexicographically Minimal Expansions (2)

- "colexicographically" = "lexicographically from right to left, i.e., least significant to most significant digit"
- colexicographically minimal expansion: greedy for zeros from right to left.

Theorem (H.-Muir 2007)

Let $\eta_{L-1} \ldots \eta_0$ be a colexicographically minimal expansion of $\mathbf{n} \in \mathbb{Z}^d$ over the digit set

$$\mathcal{D} = \{\ell, \ldots, -1, 0, 1, \ldots, u\}^d.$$

Colexicographically Minimal Expansions (2)

- "colexicographically" $=$ "lexicographically from right to left, i.e., least significant to most significant digit"
- colexicographically minimal expansion: greedy for zeros from right to left.

Theorem (H.-Muir 2007)

Let $\eta_{L-1} \ldots \eta_0$ be a colexicographically minimal expansion of $\mathbf{n} \in \mathbb{Z}^d$ over the digit set

$$\mathcal{D} = \{\ell, \ldots, -1, 0, 1, \ldots, u\}^d.$$

Then $\eta_{L-1} \ldots \eta_0$ minimises the joint weight over all joint expansions of $\mathbf{n}$ over the digit set $\mathcal{D}$.

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

Computing a Colexicographically Minimal Expansion

- Let $\mathbf{n} \in \mathbb{Z}^d$ be given.

Computing a Colexicographically Minimal Expansion

- Let $\mathbf{n} \in \mathbb{Z}^d$ be given.
- If all coordinates of $\mathbf{n}$ are even, choose a digit 0 and continue with $(1/2)\mathbf{n}$.

Computing a Colexicographically Minimal Expansion

- Let $\mathbf{n} \in \mathbb{Z}^d$ be given.
- If all coordinates of $\mathbf{n}$ are even, choose a digit 0 and continue with $(1/2)\mathbf{n}$.
- Otherwise, we have a non-zero least significant digit. Choose $w \geq 1$ maximally such that there is at least one $\boldsymbol{\eta} \in \mathcal{D}$ with $\mathbf{n} \equiv \boldsymbol{\eta} \pmod{2^w}$.

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

Computing a Colexicographically Minimal Expansion

- Let $\mathbf{n} \in \mathbb{Z}^d$ be given.
- If all coordinates of $\mathbf{n}$ are even, choose a digit 0 and continue with $(1/2)\mathbf{n}$.
- Otherwise, we have a non-zero least significant digit. Choose $w \geq 1$ maximally such that there is at least one $\boldsymbol{\eta} \in \mathcal{D}$ with $\mathbf{n} \equiv \boldsymbol{\eta} \pmod{2^w}$.
- This guarantees zeros at positions $1, \ldots, w - 1$.

Computing a Colexicographically Minimal Expansion

- Let $\mathbf{n} \in \mathbb{Z}^d$ be given.
- If all coordinates of $\mathbf{n}$ are even, choose a digit 0 and continue with $(1/2)\mathbf{n}$.
- Otherwise, we have a non-zero least significant digit. Choose $w \geq 1$ maximally such that there is at least one $\boldsymbol{\eta} \in \mathcal{D}$ with $\mathbf{n} \equiv \boldsymbol{\eta} \pmod{2^w}$.
- This guarantees zeros at positions $1, \ldots, w-1$.
- By maximality of w, we will have a non-zero digit at position w.

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

Computing a Colexicographically Minimal Expansion

- Let $\mathbf{n} \in \mathbb{Z}^d$ be given.
- If all coordinates of $\mathbf{n}$ are even, choose a digit 0 and continue with $(1/2)\mathbf{n}$.
- Otherwise, we have a non-zero least significant digit. Choose $w \geq 1$ maximally such that there is at least one $\boldsymbol{\eta} \in \mathcal{D}$ with $\mathbf{n} \equiv \boldsymbol{\eta} \pmod{2^w}$.
- This guarantees zeros at positions $1, \ldots, w-1$.
- By maximality of w, we will have a non-zero digit at position w.
- If there are two digits $\boldsymbol{\eta}$, $\boldsymbol{\eta}'$ with $\boldsymbol{\eta} \equiv \boldsymbol{\eta}' \equiv \mathbf{n} \pmod{2^w}$, choose the one that leads to a larger w in the next step.

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT I WIEN GRAZ

Computing a Colexicographically Minimal Expansion

- Let $\mathbf{n} \in \mathbb{Z}^d$ be given.
- If all coordinates of $\mathbf{n}$ are even, choose a digit 0 and continue with $(1/2)\mathbf{n}$.
- Otherwise, we have a non-zero least significant digit. Choose $w \geq 1$ maximally such that there is at least one $\boldsymbol{\eta} \in \mathcal{D}$ with $\mathbf{n} \equiv \boldsymbol{\eta} \pmod{2^w}$.
- This guarantees zeros at positions $1, \ldots, w-1$.
- By maximality of w, we will have a non-zero digit at position w.
- If there are two digits $\boldsymbol{\eta}$, $\boldsymbol{\eta}'$ with $\boldsymbol{\eta} \equiv \boldsymbol{\eta}' \equiv \mathbf{n} \pmod{2^w}$, choose the one that leads to a larger w in the next step.
- If this does not break the tie, choose the digit such that the number of choices for the digit in the next step is maximised.

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

Computing a Colexicographically Minimal Expansion

- Let $\mathbf{n} \in \mathbb{Z}^d$ be given.
- If all coordinates of $\mathbf{n}$ are even, choose a digit 0 and continue with $(1/2)\mathbf{n}$.
- Otherwise, we have a non-zero least significant digit. Choose $w \geq 1$ maximally such that there is at least one $\boldsymbol{\eta} \in \mathcal{D}$ with $\mathbf{n} \equiv \boldsymbol{\eta} \pmod{2^w}$.
- This guarantees zeros at positions $1, \ldots, w-1$.
- By maximality of w, we will have a non-zero digit at position w.
- If there are two digits $\boldsymbol{\eta}$, $\boldsymbol{\eta}'$ with $\boldsymbol{\eta} \equiv \boldsymbol{\eta}' \equiv \mathbf{n} \pmod{2^w}$, choose the one that leads to a larger w in the next step.
- If this does not break the tie, choose the digit such that the number of choices for the digit in the next step is maximised.
- Continue with $2^{-w}(\mathbf{n} - \boldsymbol{\eta})$.

Algorithm

Input: $\mathbf{n} = (n_1, n_2, \dots, n_d)^\mathsf{T} \in \mathbb{Z}^d$, $\ell \le 0$, $u \ge 1$ (with all components of $\mathbf{n}$ non-negative if $\ell = 0$).
Output: $A_{s-1} \dots A_1 A_0$, a colexicographically minimal & minimal weight representation of $\mathbf{n}$.

$D_{\ell,u} \leftarrow \{a \in \mathbb{Z} : \ell \le a \le u\}$
$w \leftarrow$ the integer such that $2^{w-1} \le \#D_{\ell,u} < 2^w$
$\mathrm{unique}(D_{\ell,u}) \leftarrow \{a \in D_{\ell,u} : u - 2^{w-1} < a < \ell + 2^{w-1}\}$
$\mathrm{nonunique}(D_{\ell,u}) \leftarrow \{a \in D_{\ell,u} : a \le u - 2^{w-1} \text{ or } \ell + 2^{w-1} \le a\}$
{these sets respectively consist of the digits which are unique and non-unique modulo 2^{w-1}.}
$s \leftarrow 0$, $L \leftarrow (\ell, \ell, \dots, \ell)^\mathsf{T}$
while $\mathbf{n} \ne \vec{0}$ **do**
  if $\mathbf{n} \equiv \vec{0} \pmod 2$ **then**
    {We can make column s zero, so we do this.}
    $A \leftarrow \vec{0}$
  else
    {We cannot make column s zero, thus it will be nonzero.}
    $A \leftarrow L + ((\mathbf{n} - L) \bmod 2^{w-1})$
    $\mathcal{I}_{\mathrm{unique}} \leftarrow \{i \in \{1, 2, \dots, d\} : a_i \in \mathrm{unique}(D_{\ell,u})\}$
    $\mathcal{I}_{\mathrm{nonunique}} \leftarrow \{i \in \{1, 2, \dots, d\} : a_i \in \mathrm{nonunique}(D_{\ell,u})\}$
    $\mathbf{m} \leftarrow (\mathbf{n} - A)/2^{w-1}$
    if $m_i \equiv 0 \pmod 2$ for all $i \in \mathcal{I}_{\mathrm{unique}}$ **then**
      {We can make column $s + w - 1$ zero.}
      for $i \in \mathcal{I}_{\mathrm{nonunique}}$ such that m_i is odd **do**
        $a_i \leftarrow a_i + 2^{w-1}$
        $m_i \leftarrow m_i - 1$
    else
      {Column $s + w - 1$ will be nonzero.}
      {Use redundancy at column s to increase redundancy at column $s + w - 1$.}
      for $i \in \mathcal{I}_{\mathrm{nonunique}}$ such that $\ell + ((m_i - \ell) \bmod 2^{w-1}) = u - 2^{w-1} + 1$ **do**
        $a_i \leftarrow a_i + 2^{w-1}$
        $m_i \leftarrow m_i - 1$
    {We have $\mathbf{n} \equiv A \pmod{2^{w-1}}$ and $\mathbf{m} = (\mathbf{n} - A)/2^{w-1}$.}
  $A_s \leftarrow A$
  $\mathbf{n} \leftarrow (\mathbf{n} - A)/2$
  $s \leftarrow s + 1$
return $A_{s-1} \dots A_1 A_0$

Analysis — Result

For $N > 0$, let H_N be the joint weight of a random $\mathbf{n}$ with $0 \leq n_i < N$ for all i (equipped with equidistribution).

Analysis — Result

For $N > 0$, let H_N be the joint weight of a random $\mathbf{n}$ with $0 \le n_i < N$ for all i (equipped with equidistribution).

Theorem (H.-Kropf 2013)

There exist constants $e_{\ell,u,d}$, $v_{\ell,u,d} \in \mathbb{R}$ and $\delta > 0$ such that

$$\mathbb{E}(H_N) = e_{\ell,u,d} \log_2 N + \Psi_1(\log_2 N) + \mathcal{O}(N^{-\delta} \log N),$$
$$\mathbb{V}(H_N) = v_{\ell,u,d} \log_2 N + \Psi_2(\log_2 N) + \mathcal{O}(N^{-\delta} \log^2 N),$$

where Ψ_1 and Ψ_2 are continuous, 1-periodic functions on $\mathbb{R}$.

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

Analysis — Result

For $N > 0$, let H_N be the joint weight of a random $\mathbf{n}$ with $0 \leq n_i < N$ for all i (equipped with equidistribution).

Theorem (H.-Kropf 2013)

There exist constants $e_{\ell,u,d}$, $v_{\ell,u,d} \in \mathbb{R}$ and $\delta > 0$ such that

$$\mathbb{E}(H_N) = e_{\ell,u,d} \log_2 N + \Psi_1(\log_2 N) + \mathcal{O}(N^{-\delta} \log N),$$
$$\mathbb{V}(H_N) = v_{\ell,u,d} \log_2 N + \Psi_2(\log_2 N) + \mathcal{O}(N^{-\delta} \log^2 N),$$

where Ψ_1 and Ψ_2 are continuous, 1-periodic functions on $\mathbb{R}$. Furthermore, we have the central limit theorem

$$\mathbb{P}\left(\frac{H_N - e_{\ell,u,d} \log_2 N}{\sqrt{v_{\ell,u,d} \log_2 N}} < x\right) = \int_{-\infty}^{x} e^{\frac{-t^2}{2}}\, dt + \mathcal{O}\left(\frac{1}{\sqrt[4]{\log N}}\right)$$

for all $x \in \mathbb{R}$.

Constants for Expectation and Variance

- For $d = 1$, we have

$$e_{\ell,u,1} = \frac{1}{w-1+\lambda} \quad \text{and} \quad v_{\ell,u,1} = \frac{(3-\lambda)\lambda}{(w-1+\lambda)^3},$$

where

$$\lambda = \frac{2(u-\ell+1) - (-1)^{\ell} - (-1)^{u}}{2^w},$$
$$2^{w-1} \leq u-\ell+1 < 2^w.$$

Constants for Expectation and Variance

- For $d = 1$, we have

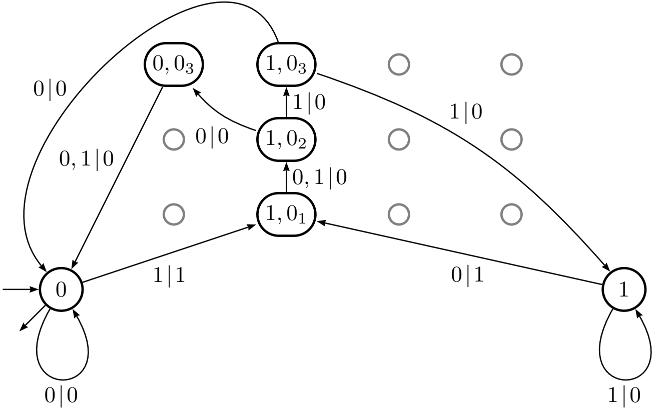
$$e_{\ell,u,1} = \frac{1}{w - 1 + \lambda} \quad \text{and} \quad v_{\ell,u,1} = \frac{(3-\lambda)\lambda}{(w-1+\lambda)^3},$$

  where

$$\lambda = \frac{2(u - \ell + 1) - (-1)^{\ell} - (-1)^{u}}{2^w},$$
$$2^{w-1} \leq u - \ell + 1 < 2^w.$$

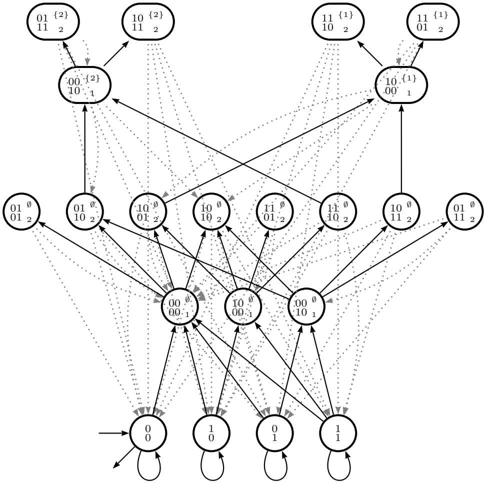
- For $d \in \{2, 3, 4\}$, the constants $e_{\ell,u,d}$ and $v_{\ell,u,d}$ have been calculated.

Transducer to Compute the Weight



Transducer to compute the weight from the standard binary expansion for $d = 1$, $\ell = -3$, $u = 11$. Gray states correspond to states which are present in the general description of the transducer, but are non-accessible here.

Transducer to Compute the Weight (2)



Transducer to compute the weight from the standard binary expansion for $d = 2$, $\ell = -2$, $u = 3$.

Transducer to Compute the Weight (3)

- For general d, ℓ, u, a general description of the transducer is available.

Transducer to Compute the Weight (3)

- For general d, ℓ, u, a general description of the transducer is available.
- $< 8^d w$ states, where $2^{w-1} \leq u - \ell + 1 < 2^w$.

Transducer to Compute the Weight (3)

- For general d, ℓ, u, a general description of the transducer is available.
- $< 8^d w$ states, where $2^{w-1} \leq u - \ell + 1 < 2^w$.
- strongly connected.

Transducer to Compute the Weight (3)

- For general d, ℓ, u, a general description of the transducer is available.
- $< 8^d w$ states, where $2^{w-1} \leq u - \ell + 1 < 2^w$.
- strongly connected.
- aperiodic.

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

Transition and Adjacency Matrices

- Fix order of the states, initial state is last.

Transition and Adjacency Matrices

- Fix order of the states, initial state is last.
- For $\boldsymbol{\varepsilon} \in \{0,1\}^d$ let $M_{\boldsymbol{\varepsilon}} = M_{\boldsymbol{\varepsilon}}(y)$ be the matrix with entry y^h at position r, s if there is a transition $r \xrightarrow{\varepsilon|h} s$ and 0 otherwise.

Transition and Adjacency Matrices

- Fix order of the states, initial state is last.
- For $\varepsilon \in \{0,1\}^d$ let $M_\varepsilon = M_\varepsilon(y)$ be the matrix with entry y^h at position r, s if there is a transition $r \xrightarrow{\varepsilon | h} s$ and 0 otherwise.
- Set $A = A(y) = \sum_{\varepsilon \in \{0,1\}^d} M_\varepsilon(y)$.

Transition and Adjacency Matrices

- Fix order of the states, initial state is last.
- For $\varepsilon \in \{0,1\}^d$ let $M_\varepsilon = M_\varepsilon(y)$ be the matrix with entry y^h at position r, s if there is a transition $r \xrightarrow{\varepsilon|h} s$ and 0 otherwise.
- Set $A = A(y) = \sum_{\varepsilon\in\{0,1\}^d} M_\varepsilon(y)$.

Example for $d = 2$, $\ell = -2$, $u = 3$:

$$A = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
3y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
y & 0 & 0 & 0 & y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
y & 0 & 0 & y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
2y & y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
y & 0 & 0 & 0 & y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
y & 0 & 0 & y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
2y & 0 & y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
y & 0 & 0 & y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
y & 0 & 0 & 0 & y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
y & y & y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
2y & 0 & y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
2y & y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
3y & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}$$

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

Probability generating function

Let

$$h(\mathbf{n}) = \text{joint weight of AJSF of } \mathbf{n},$$

Probability generating function

Let

$$h(\mathbf{n}) = \text{joint weight of AJSF of } \mathbf{n},$$

$$E(N; y) = \mathbb{E}(u^{H_N}) = \frac{1}{N^d} \sum_{\substack{\mathbf{n} \geq \mathbf{0} \\ \|\mathbf{n}\|_\infty < N}} y^{h(\mathbf{n})}.$$

Probability generating function

Let

$$h(\mathbf{n}) = \text{joint weight of AJSF of } \mathbf{n},$$

$$E(N; y) = \mathbb{E}(u^{H_N}) = \frac{1}{N^d} \sum_{\substack{\mathbf{n} \geq \mathbf{0} \\ \|\mathbf{n}\|_\infty < N}} y^{h(\mathbf{n})}.$$

Writing the standard binary expansion of $\mathbf{n}$ as $\varepsilon_J(\mathbf{n}) \ldots \varepsilon_0(\mathbf{n})$, we have

$$y^{h(\mathbf{n})} = u^\mathsf{T} \left(\prod_{j=0}^{J} M_{\varepsilon_j(\mathbf{n})}(y) \right) v$$

for suitable vectors u and $v = v(y)$.

Probability generating function

Let

$$h(\mathbf{n}) = \text{joint weight of AJSF of } \mathbf{n},$$

$$E(N;y) = \mathbb{E}(u^{H_N}) = \frac{1}{N^d} \sum_{\substack{\mathbf{n}\geq \mathbf{0} \\ \|\mathbf{n}\|_\infty < N}} y^{h(\mathbf{n})}.$$

Writing the standard binary expansion of $\mathbf{n}$ as $\varepsilon_J(\mathbf{n})\ldots\varepsilon_0(\mathbf{n})$, we have

$$y^{h(\mathbf{n})} = u^{\mathsf{T}} \left(\prod_{j=0}^{J} M_{\varepsilon_j(\mathbf{n})}(y) \right) v$$

for suitable vectors u and $v = v(y)$. We consider

$$F(N;y) = \sum_{\substack{\mathbf{n}\geq \mathbf{0} \\ \|\mathbf{n}\|_\infty < N}} \prod_{j=0}^{J} M_{\varepsilon_j(\mathbf{n})}(y).$$

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

Recursion for F $(d = 1)$

We consider

$$F(N; y) = \sum_{0 \le n < N} \prod_{j=0}^{J} M_{\varepsilon_j(n)}(y),$$

Recursion for F $(d = 1)$

We consider

$$F(N;y) = \sum_{0 \le n < N} \prod_{j=0}^{J} M_{\varepsilon_j(n)}(y),$$

which fulfils the recursion

$$F(2N;y) = A(y)F(N;y),$$
$$F(2N+1;y) = A(y)F(N;y) + M_0 \prod_{j=0}^{J} M_{\varepsilon_j(N)}(y),$$

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

Recursion for F $(d = 1)$

We consider

$$F(N; y) = \sum_{0 \leq n < N} \prod_{j=0}^{J} M_{\varepsilon_j(n)}(y),$$

which fulfils the recursion

$$F(2N; y) = A(y)F(N; y),$$
$$F(2N+1; y) = A(y)F(N; y) + M_0 \prod_{j=0}^{J} M_{\varepsilon_j(N)}(y),$$

yielding

$$F(N; y) = \sum_{j=0}^{J} \varepsilon_j(N) A(y)^j M_0(y) \prod_{k=j+1}^{J} M_{\varepsilon_k(N)}(y).$$

Periodic Fluctuation ($d = 1$)

We consider

$$F(N; y) = \sum_{j=0}^{J} \varepsilon_j(N) A(y)^j M_0(y) \prod_{k=j+1}^{J} M_{\varepsilon_k(N)}(y).$$

Periodic Fluctuation ($d = 1$)

We consider

$$F(N; y) = \sum_{j=0}^{J} \varepsilon_j(N) A(y)^j M_0(y) \prod_{k=j+1}^{J} M_{\varepsilon_k(N)}(y).$$

Let $\mu(y)$ be the dominant eigenvalue of $A(y)$. Note that $\mu(1) = 2$.

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ

Periodic Fluctuation ($d = 1$)

We consider

$$F(N; y) = \sum_{j=0}^{J} \varepsilon_j(N) A(y)^j M_0(y) \prod_{k=j+1}^{J} M_{\varepsilon_k(N)}(y).$$

Let $\mu(y)$ be the dominant eigenvalue of $A(y)$. Note that $\mu(1) = 2$. Write $T^{-1}AT = D + R$ for $D = \operatorname{diag}(\mu, 0, \ldots, 0)$ and obtain

$$F(N; y) = \mu(y)^J \sum_{j=0}^{J} \varepsilon_j(N) T D^{-(J-j)} T^{-1} M_0(y) \prod_{k=j+1}^{J} M_{\varepsilon_k(N)}(y) + O(\ldots).$$

Periodic Fluctuation ($d = 1$)

We consider

$$F(N;y) = \sum_{j=0}^{J} \varepsilon_j(N) A(y)^j M_0(y) \prod_{k=j+1}^{J} M_{\varepsilon_k(N)}(y).$$

Let $\mu(y)$ be the dominant eigenvalue of $A(y)$. Note that $\mu(1) = 2$. Write $T^{-1}AT = D + R$ for $D = \operatorname{diag}(\mu, 0, \ldots, 0)$ and obtain

$$F(N;y) = \mu(y)^J \sum_{j=0}^{J} \varepsilon_j(N) T D^{-(J-j)} T^{-1} M_0(y) \prod_{k=j+1}^{J} M_{\varepsilon_k(N)}(y) + O(\ldots).$$

We finally get

$$F(N;y) = \mu(y)^{\log_2 N} \Psi(\{\log_2 N\}; y) + O(\ldots)$$

where $\Psi(x;y)$ is 1-periodic in x.

ALPEN-ADRIA UNIVERSITÄT KLAGENFURT | WIEN GRAZ