Analysis of Parameters of Multi-Base Representations of an Integer

Daniel Krenn

(joint works with Dimbinaina Ralaivaosaona and Stephan Wagner)

June 12, 2015

DOCTORAL PROGRAM DISCRETE MATHEMATICS
TU & KFU GRAZ · MU LEOBEN AUSTRIA

Der Wissenschaftsfonds.

Supported by the Austrian Science Fund (FWF), projects I1136 & P24644 & W1230.

Multi-Base Representations

Representations

$$n = \sum_j d_j p_1^{\alpha_{1j}} p_2^{\alpha_{2j}} \dots p_m^{\alpha_{mj}}$$

- digits d_j out of digit set $\{0, 1, \dots, d-1\}$
- bases $p_1, \dots, p_m$ (coprime positive integers)
- non-negative integers α_{ij}
- all $p_1^{\alpha_{1j}} p_2^{\alpha_{2j}} \dots p_m^{\alpha_{mj}}$ distinct

Multi-Base Representations

Representations

$$n = \sum_j d_j p_1^{\alpha_{1j}} p_2^{\alpha_{2j}} \dots p_m^{\alpha_{mj}}$$

- digits d_j out of digit set $\{0, 1, \dots, d-1\}$
- bases $p_1, \dots, p_m$ (coprime positive integers)
- non-negative integers α_{ij}
- all $p_1^{\alpha_{1j}} p_2^{\alpha_{2j}} \dots p_m^{\alpha_{mj}}$ distinct

Questions

How many representations does a number have?

How do these representations behave?

Motivation from Cryptography

calculate

$$nP = P + \cdots + P$$

as efficiently as possible

(P group element, $n \in \mathbb{N}_0$)

Motivation from Cryptography

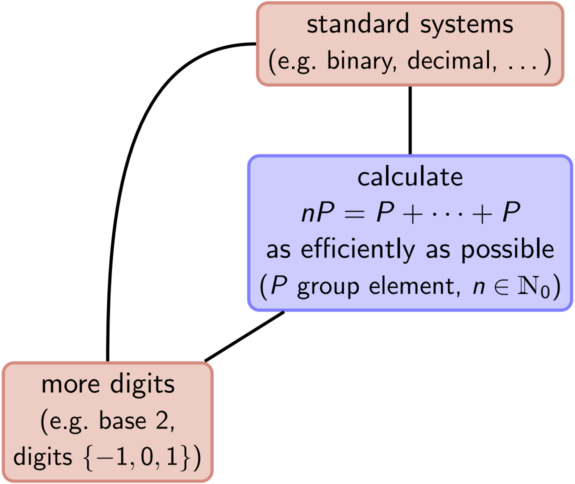
standard systems
(e.g. binary, decimal, . . .)

calculate

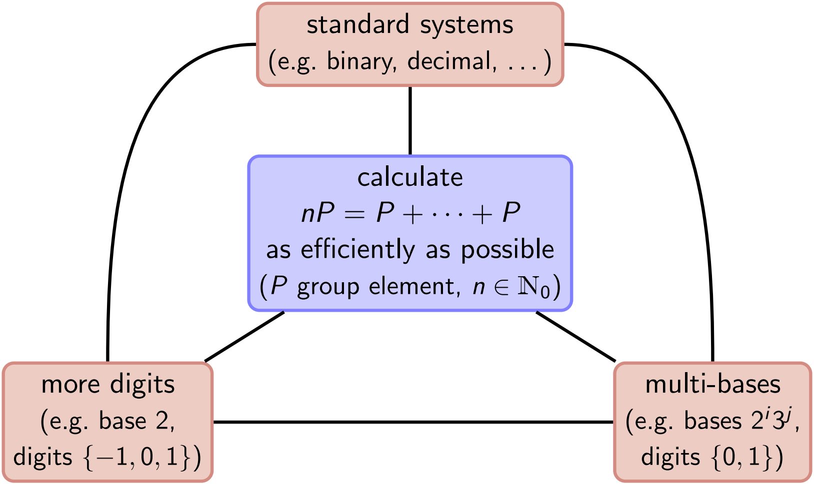
$$nP = P + \cdots + P$$

as efficiently as possible
(P group element, $n \in \mathbb{N}_0$)

Motivation from Cryptography



Motivation from Cryptography



Counting 2–3-Expansions

- set-up
  - bases 2 and 3
  - digits 0 and 1
- partitions into powers of 3
  - expansion of n

$$n = b_0 + 3b_1 + 9b_2 + \cdots + 3^\ell b_\ell$$

  - b_j in binary

Counting 2–3-Expansions

- set-up
  - bases 2 and 3
  - digits 0 and 1
- partitions into powers of 3
  - expansion of n

    $$n = b_0 + 3b_1 + 9b_2 + \cdots + 3^\ell b_\ell$$

  - b_j in binary

Recursion

number of representations

$$P_n = \begin{cases} P_{n-1} + P_{n/3} & \text{if } 3 \mid n \\ P_{n-1} & \text{if } 3 \nmid n \end{cases}$$

Counting 2–3-Expansions

- set-up
  - bases 2 and 3
  - digits 0 and 1
- partitions into powers of 3
  - expansion of n

    $$n = b_0 + 3b_1 + 9b_2 + \cdots + 3^\ell b_\ell$$

  - b_j in binary

Recursion

number of representations

$$P_n = \begin{cases} P_{n-1} + P_{n/3} & \text{if } 3 \mid n \\ P_{n-1} & \text{if } 3 \nmid n \end{cases}$$

- $\rightsquigarrow$ asymptotic formula
- generalization to 2–p-expansions

Number of Representations

Theorem (K–Ralaivaosaona–Wagner 2014)

- *fix bases* $p_1, \ldots, p_m$ $(m \geq 2)$
- *fix digit set* $\{0, \ldots, d-1\}$
- *number of multi-base representations* P_n *of* n

$$\begin{aligned}\log P_n = \kappa(\log n)^m &+ C_1 (\log n)^{m-1} \log\log n \\ &+ C_2 (\log n)^{m-1} \\ &+ O\big((\log n)^{m-2} \log\log n\big)\end{aligned}$$

- *with*

$$\kappa = \frac{\log d}{m!} \prod_{i=1}^{m} \frac{1}{\log p_i}$$

Parameters

Theorem (K–Ralaivaosaona–Wagner 2014, 2015)

- *fix bases* $p_1, \ldots, p_m$ $(m \geq 2)$
- *fix digit set* $\{0, \ldots, d-1\}$
- *asymptotic normal distribution of*
  - *sum of digits*

    $$\mu \sim \frac{\kappa(d-1)}{2\log d}(\log n)^m \qquad \sigma^2 \sim \frac{\kappa(d-1)(d+1)}{12\log d}(\log n)^m$$
  - *Hamming weight*

    $$\mu \sim \frac{\kappa(d-1)}{d\log d}(\log n)^m \qquad \sigma^2 \sim \frac{\kappa(d-1)}{d^2\log d}(\log n)^m$$
  - *occurrence of a fixed digit*

    $$\mu \sim \frac{\kappa}{d\log d}(\log n)^m \qquad \sigma^2 \sim \frac{\kappa(d-1)}{d^2\log d}(\log n)^m$$

The Generating Function

- representations

$$n = \sum_j d_j p_1^{\alpha_{1j}} p_2^{\alpha_{2j}} \dots p_m^{\alpha_{mj}}$$

  - digits $d_j \in \{0, 1, \dots, d-1\}$
  - power products $\mathcal{B} = \{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} \mid \alpha_i \in \mathbb{N}_0\}$

The Generating Function

- representations

$$n = \sum_j d_j p_1^{\alpha_{1j}} p_2^{\alpha_{2j}} \dots p_m^{\alpha_{mj}}$$

- digits $d_j \in \{0, 1, \dots, d-1\}$
- power products $\mathcal{B} = \{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} \mid \alpha_i \in \mathbb{N}_0\}$

Counting Generating Function

$$F(z) = \sum_{n \in \mathbb{N}_0} P_n z^n = \prod_{b \in \mathcal{B}} \left(1 + z^b + z^{2b} + \dots + z^{(d-1)b}\right)$$

The Generating Function

- representations

$$n = \sum_j d_j p_1^{\alpha_{1j}} p_2^{\alpha_{2j}} \dots p_m^{\alpha_{mj}}$$

  - digits $d_j \in \{0, 1, \dots, d-1\}$
  - power products $\mathcal{B} = \{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} \mid \alpha_i \in \mathbb{N}_0\}$

Counting Generating Function

$$F(z) = \sum_{n \in \mathbb{N}_0} P_n z^n = \prod_{b \in \mathcal{B}} \left(1 + z^b + z^{2b} + \dots + z^{(d-1)b}\right)$$

- encode parameter: $F(z, u)$

Saddle-Point Method

Saddle-Point Method

- extract coefficients (Cauchy's integral formula)

$$P_n = [z^n]F(z) = \frac{1}{2\pi i} \oint_{\mathcal{C}} F(z) \frac{dz}{z^{n+1}}$$

Saddle-Point Method

- extract coefficients (Cauchy's integral formula)

$$P_n = [z^n]F(z) = \frac{1}{2\pi i} \oint_{\mathcal{C}} F(z) \frac{dz}{z^{n+1}}$$

- substitute $z = e^{-(r+i\tau)}$

$$P_n = \frac{1}{2\pi} \int_{-\pi}^{\pi} \exp\left(nr + f(r+i\tau) + in\tau\right) d\tau$$

with $f(r+i\tau) = \log F(e^{-(r+i\tau)})$

Saddle-Point Method

- extract coefficients (Cauchy's integral formula)

$$P_n = [z^n]F(z) = \frac{1}{2\pi i}\oint_{\mathcal{C}} F(z)\frac{dz}{z^{n+1}}$$

- substitute $z = e^{-(r+i\tau)}$

$$P_n = \frac{1}{2\pi}\int_{-\pi}^{\pi} \exp\left(nr + f(r+i\tau) + in\tau\right) d\tau$$

with $f(r+i\tau) = \log F(e^{-(r+i\tau)})$

- saddle-point equation $n = -f'(r)$

$$nr + f(r+i\tau) + in\tau = nr + f(r) - f''(r)\frac{\tau^2}{2} + \cdots$$

Saddle-Point Method

- extract coefficients (Cauchy's integral formula)

$$P_n = [z^n]F(z) = \frac{1}{2\pi i} \oint_{\mathcal{C}} F(z) \frac{dz}{z^{n+1}}$$

- substitute $z = e^{-(r+i\tau)}$

$$P_n = \frac{1}{2\pi} \int_{-\pi}^{\pi} \exp\left(nr + f(r+i\tau) + in\tau\right) d\tau$$

with $f(r+i\tau) = \log F(e^{-(r+i\tau)})$

- saddle-point equation $n = -f'(r)$

$$nr + f(r+i\tau) + in\tau = nr + f(r) - f''(r)\frac{\tau^2}{2} + \cdots$$

- asymptotics

$$P_n \sim \frac{e^{nr+f(r)}}{2\pi} \int_{-\infty}^{\infty} \exp\left(-f''(r)\frac{\tau^2}{2}\right) d\tau = \frac{e^{nr+f(r)}}{\sqrt{2\pi f''(r)}}$$

Mellin & Friends

- function

$$f(r) = \sum_{b \in \mathcal{B}} \log \left(1 + e^{-br} + e^{-2br} + \cdots + e^{-(d-1)br}\right)$$

Mellin & Friends

- function

$$f(r) = \sum_{b \in \mathcal{B}} \log\left(1 + e^{-br} + e^{-2br} + \cdots + e^{-(d-1)br}\right)$$

- Mellin transform

$$Y(s) = \int_0^\infty \log\left(1+e^{-r}+e^{-2r}+\cdots+e^{-(d-1)r}\right) r^{s-1}\, dr \underset{s\to 0}{\sim} \frac{\log d}{s}$$

Mellin & Friends

- function

$$f(r) = \sum_{b \in \mathcal{B}} \log\left(1 + e^{-br} + e^{-2br} + \dots + e^{-(d-1)br}\right)$$

- Mellin transform

$$Y(s) = \int_0^\infty \log\left(1+e^{-r}+e^{-2r}+\dots+e^{-(d-1)r}\right) r^{s-1}\, dr \underset{s \to 0}{\sim} \frac{\log d}{s}$$

- Dirichlet series

$$D(s) = \sum_{b \in \mathcal{B}} b^{-s} = \prod_{i=1}^{m} \frac{1}{1 - p_i^{-s}} \underset{s \to 0}{\sim} \prod_{i=1}^{m} \frac{1}{s \log p_i}$$

Mellin & Friends

- function

$$f(r) = \sum_{b \in \mathcal{B}} \log\left(1 + e^{-br} + e^{-2br} + \dots + e^{-(d-1)br}\right)$$

- Mellin transform

$$Y(s) = \int_0^\infty \log\left(1+e^{-r}+e^{-2r}+\dots+e^{-(d-1)r}\right) r^{s-1}\,dr \underset{s\to 0}{\sim} \frac{\log d}{s}$$

- Dirichlet series

$$D(s) = \sum_{b \in \mathcal{B}} b^{-s} = \prod_{i=1}^{m} \frac{1}{1-p_i^{-s}} \underset{s\to 0}{\sim} \prod_{i=1}^{m} \frac{1}{s \log p_i}$$

- inverse Mellin transform

$$f(r) = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} Y(s) D(s) r^{-s}\,ds \underset{r\to 0^+}{\sim} \frac{a_m}{m!} (\log 1/r)^m$$

Tails

- step one

$$\frac{|F(z)|}{F(|z|)} \leq \exp\left(-C \sum_{b\in\mathcal{B}(r)} \|by\|^2\right)$$

1

  - with $z = e^{-r+2\pi iy}$
  - $\mathcal{B}(r)$ for $\mathcal{B} \cap [1, 1/r] = \{b \in \mathcal{B} \mid br \leq 1\}$
  - distance to nearest integer $\|\cdot\|$

Tails

2

- step one

$$\frac{|F(z)|}{F(|z|)} \leq \exp\left(-C \sum_{b \in \mathcal{B}(r)} \|by\|^2\right)$$

  - with $z = e^{-r+2\pi iy}$
  - $\mathcal{B}(r)$ for $\mathcal{B} \cap [1, 1/r] = \{b \in \mathcal{B} \mid br \leq 1\}$
  - distance to nearest integer $\|\cdot\|$
- step two

$$\sum_{b \in \mathcal{B}(r)} \|by\|^2 \geq (\log(1/r))^{m-1} \times \text{something}$$

  - Dirichlet's approximation theorem
  - pigeonhole principle
  - problem if $m = 2$: valid except y in “small” set

Tails

3

- step one

$$\frac{|F(z)|}{F(|z|)} \leq \exp\left(-C \sum_{b \in \mathcal{B}(r)} \|by\|^2\right)$$

  - with $z = e^{-r+2\pi iy}$
  - $\mathcal{B}(r)$ for $\mathcal{B} \cap [1, 1/r] = \{b \in \mathcal{B} \mid br \leq 1\}$
  - distance to nearest integer $\|\cdot\|$
- step two

$$\sum_{b \in \mathcal{B}(r)} \|by\|^2 \geq (\log(1/r))^{m-1} \times \text{something}$$

  - Dirichlet's approximation theorem
  - pigeonhole principle
  - problem if $m = 2$: valid except y in "small" set
- step three
  - apply bounds

Plugging Everything Together...

Representations

$$n = \sum_j d_j p_1^{\alpha_{1j}} p_2^{\alpha_{2j}} \dots p_m^{\alpha_{mj}}$$

- $d_j \in \{0, 1, \dots, d-1\}$
- bases $p_1, \dots, p_m$

Plugging Everything Together...

$$P_n = [z^n]F(z) \sim \frac{e^{nr+f(r)}}{\sqrt{2\pi f''(r)}}$$

Representations

$$n = \sum_j d_j p_1^{\alpha_{1j}} p_2^{\alpha_{2j}} \dots p_m^{\alpha_{mj}}$$

- $d_j \in \{0, 1, \dots, d-1\}$
- bases $p_1, \dots, p_m$

Plugging Everything Together...

$$P_n = [z^n]F(z) \sim \frac{e^{nr+f(r)}}{\sqrt{2\pi f''(r)}}$$

$+$

$$n = -f'(r) \;\Rightarrow\; \log 1/r \sim \log n$$

Representations

$$n = \sum_j d_j p_1^{\alpha_{1j}} p_2^{\alpha_{2j}} \dots p_m^{\alpha_{mj}}$$

- $d_j \in \{0, 1, \dots, d-1\}$
- bases $p_1, \dots, p_m$

Plugging Everything Together...

$$P_n = [z^n]F(z) \sim \frac{e^{nr+f(r)}}{\sqrt{2\pi f''(r)}}$$

$$+$$

$$n = -f'(r) \;\Rightarrow\; \log 1/r \sim \log n$$

$$+$$

$$f(r) \sim \frac{a_m}{m!}(\log 1/r)^m$$

Representations

$$n = \sum_j d_j p_1^{\alpha_{1j}} p_2^{\alpha_{2j}} \dots p_m^{\alpha_{mj}}$$

- $d_j \in \{0, 1, \dots, d-1\}$
- bases $p_1, \dots, p_m$

Plugging Everything Together...

$$P_n = [z^n]F(z) \sim \frac{e^{nr+f(r)}}{\sqrt{2\pi f''(r)}}$$

$$+$$

$$n = -f'(r) \;\Rightarrow\; \log 1/r \sim \log n$$

$$+$$

$$f(r) \sim \frac{a_m}{m!}(\log 1/r)^m$$

$$+$$

tail bounds

Representations

$$n = \sum_j d_j p_1^{\alpha_{1j}} p_2^{\alpha_{2j}} \dots p_m^{\alpha_{mj}}$$

- $d_j \in \{0, 1, \dots, d-1\}$
- bases $p_1, \dots, p_m$

Plugging Everything Together...

Representations

$$n = \sum_j d_j p_1^{\alpha_{1j}} p_2^{\alpha_{2j}} \dots p_m^{\alpha_{mj}}$$

- $d_j \in \{0, 1, \dots, d-1\}$
- bases $p_1, \dots, p_m$

$$P_n = [z^n]F(z) \sim \frac{e^{nr+f(r)}}{\sqrt{2\pi f''(r)}}$$

$+$

$$n = -f'(r) \;\Rightarrow\; \log 1/r \sim \log n$$

$+$

$$f(r) \sim \frac{a_m}{m!}(\log 1/r)^m$$

$+$

tail bounds

$$\Longrightarrow \log P_n \sim \frac{\log d}{m!} \prod_{i=1}^{m} \frac{1}{\log p_i} (\log n)^m$$

Central Limit Theorem, Mean and Variance

Probability Generating Function

$$P_n(u) = \frac{[z^n]F(z,u)}{[z^n]F(z,1)}$$

- estimates and bounds uniformly in u around 1

Central Limit Theorem, Mean and Variance

Probability Generating Function

$$P_n(u) = \frac{[z^n]F(z,u)}{[z^n]F(z,1)}$$

- estimates and bounds uniformly in u around 1
  - (weak) convergence to Gaussian distribution

Central Limit Theorem, Mean and Variance

Probability Generating Function

$$P_n(u) = \frac{[z^n]F(z,u)}{[z^n]F(z,1)}$$

- estimates and bounds uniformly in u around 1
  - (weak) convergence to Gaussian distribution
- verify asymptotic behavior of moments
  - $\rightsquigarrow$ mean and variance