The Double-Base Number System

Theory, Applications and Open Problems

Laurent Imbert

CNRS, LIRMM, Université Montpellier 2

10 years of collaborations with V. Dimitrov, Univ. of Calgary, Canada

CASED, TUD – April 8, 2010

Today's menu

- (p, q)-ary partitions
- The double-base number system: $(p, q) = (2, 3)$
- Definition, representation, properties
- Applications to arithmetic and cryptography
- strictly chained (p, q)-ary partitions
- Open problems

Integer Partitions

A *partition* of an integer n is a nonincreasing sequence of positive integers $a_1, a_2, \ldots, a_k$ whose sum is n. Each a_i is called a *part*.

For example, the 5 partitions of 4 are:

$$\begin{aligned} 4 &= 4 \\ &= 3 + 1 \\ &= 2 + 2 \\ &= 2 + 1 + 1 \\ &= 1 + 1 + 1 + 1 \end{aligned}$$

The partitions of n correspond to the set of solutions $(k_1, k_2, \ldots, k_n)$ in nonnegative integers to the diophantine equation

$$1k_1 + 2k_2 + 3k_3 + \cdots + nk_n = n$$

The Partitions Zoo

- Partitions with distinct parts, partitions with odd parts
- Partitions whose largest part is k, partitions with k parts
- Partitions into primes (Goldbach conjecture)
- m-ary partitions: partitions as a sum of powers of m for a fixed $m \geq 2$ (e.g. binary partitions)
- Partitions with parts occuring at most twice or thrice
- Chain, umbrella partitions: partitions constrained by divisibility conditions
- etc.

(p, q)-ary Partitions

A *(p, q)-ary partition* is a partition where the parts are divisible by no primes other than p or q

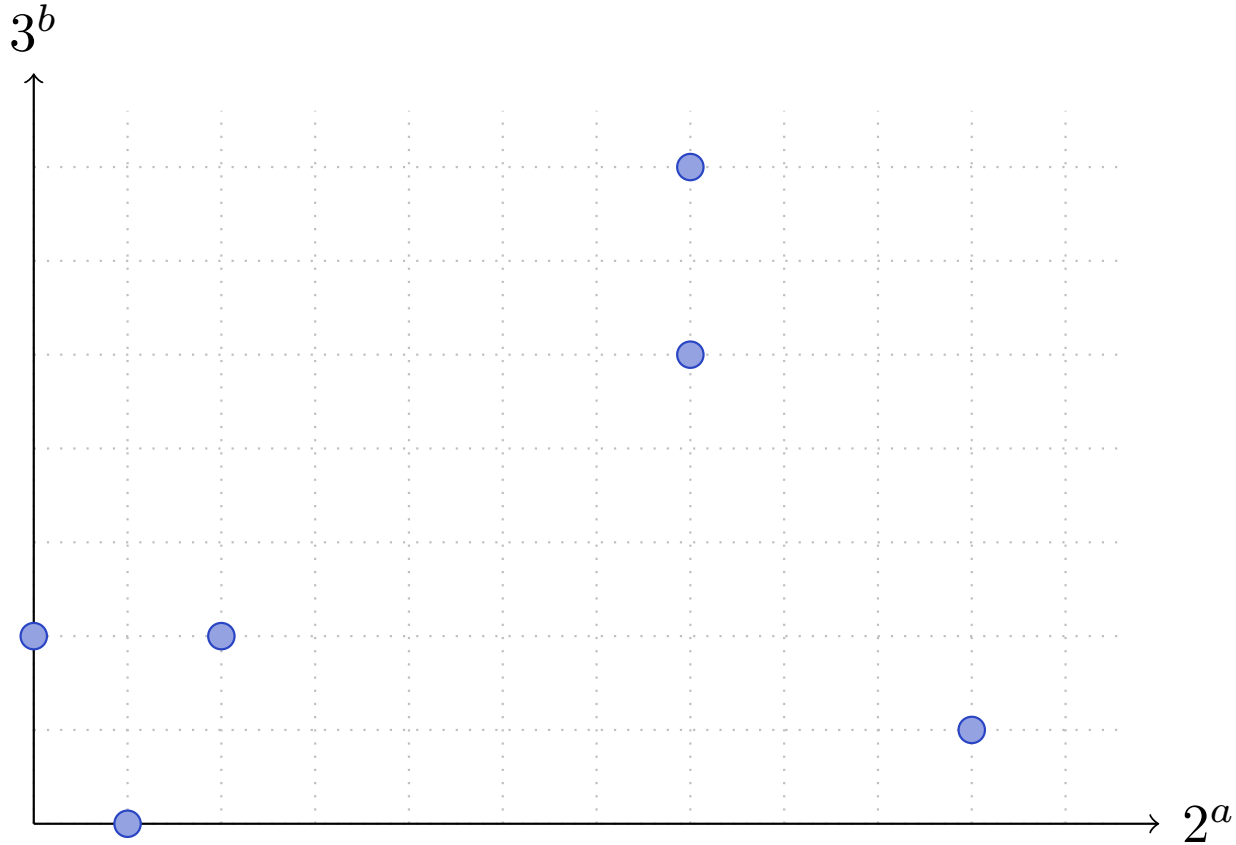
Historically, a *double-base representation* of $n > 0$ is a $(2, 3)$-ary partition of n with distinct parts

$$n = 2^{a_1}3^{b_1} + 2^{a_2}3^{b_2} \cdots + 2^{a_m}3^{b_m}$$

with $a_i, b_i \geq 0$ for $i = 1, \ldots, m$

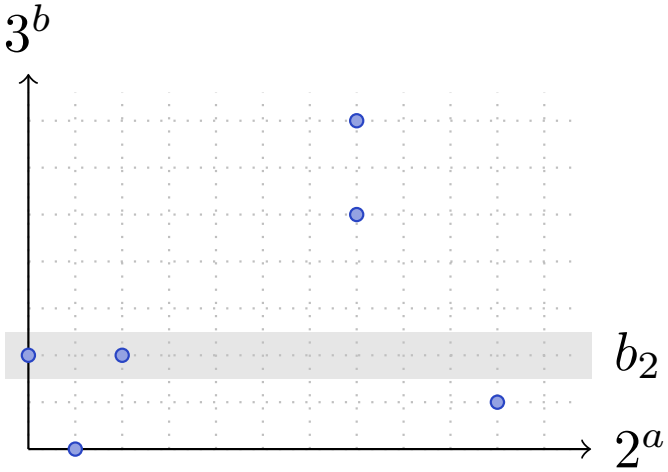
A number of the form 2^a3^b is called a *$\{2, 3\}$-integer*

Representation of (p, q)-ary Partitions



$$314159 = 2^7 3^7 + 2^7 3^5 + 2^{10} 3^1 + 2^2 3^2 + 2^0 3^2 + 2^1 3^0$$

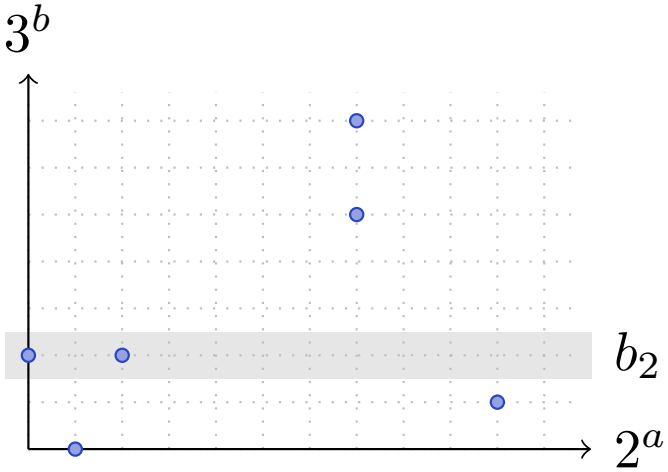
Number of Double-Base Representations



One-to-one correspondence with the solutions $(b_0, \ldots, b_{r-1})$ to the diophantine equation

$$n = b_0 + 3b_1 + 3^2 b_2 + \cdots + 3^{r-1} b_{r-1}$$

Number of Double-Base Representations



One-to-one correspondence with the solutions $(b_0, \ldots, b_{r-1})$ to the diophantine equation

$$n = b_0 + 3b_1 + 3^2 b_2 + \cdots + 3^{r-1} b_{r-1}$$

\# Double-base rep. of $n > 0$ = \# 3-ary partitions of n

$$f(n) = \begin{cases} f(n-1) + f(n/3) & \text{if } 3|n \\ f(n-1) & \text{otherwise} \end{cases}$$

Sloane's integer sequence # A005704

$f(1) = 1,\ f(10) = 5,\ f(50) = 72,\ f(100) = 402,\ f(500) = 75171$

Length of Double-Base Representations

The *Length* of a double-base representation is equal to the number of parts in

$$n = 2^{a_1}3^{b_1} + \cdots + 2^{a_m}3^{b_m}$$

Theorem [Dimitrov 95]: $m \in O(\log n / \log \log n)$

Length of Double-Base Representations

The *Length* of a double-base representation is equal to the number of parts in

$$n = 2^{a_1}3^{b_1} + \cdots + 2^{a_m}3^{b_m}$$

Theorem [Dimitrov 95]: $m \in O(\log n / \log\log n)$

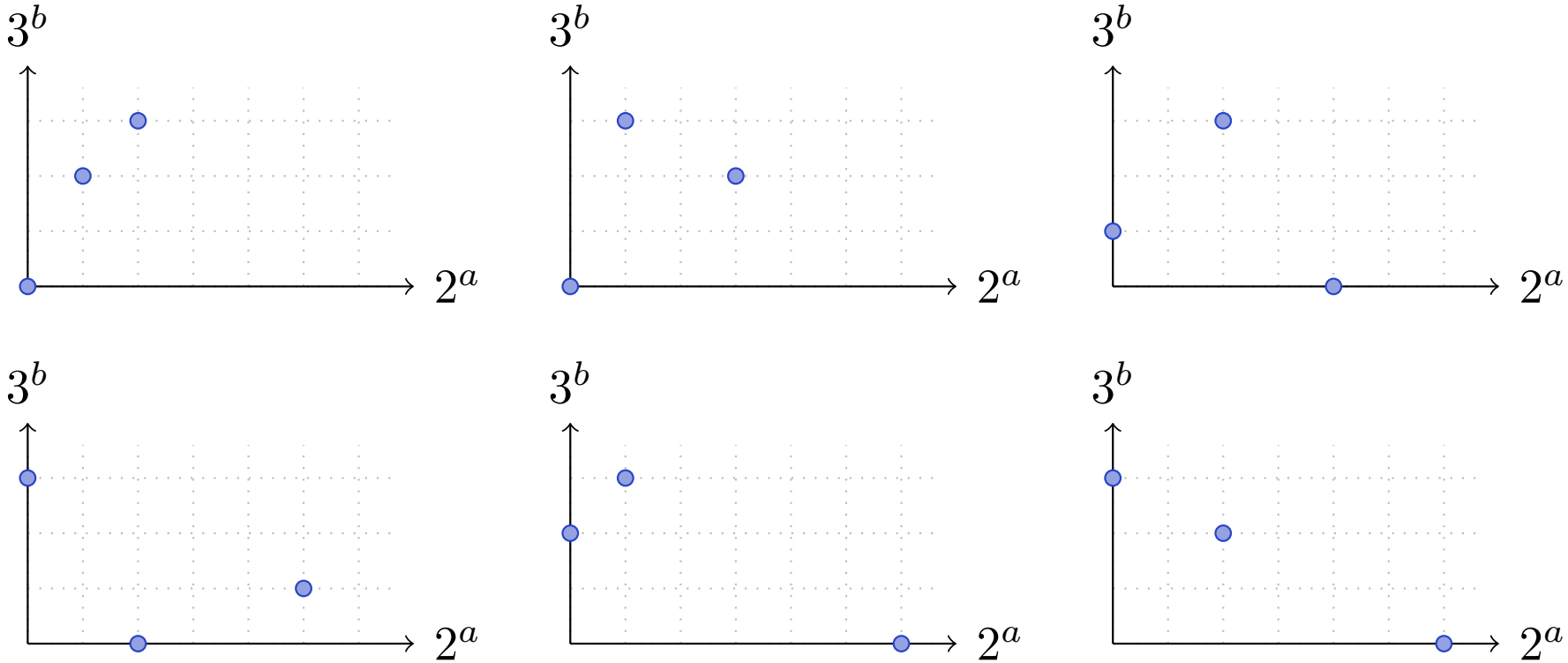
Smallest $n > 0$ requiring m parts

m		$\log n / \log\log n$
2	5	3.38
3	23	2.74
4	431	3.36
5	18,431	4.29
6	3,448,733	5.55
7	1,441,896,119	6.91

Canonic Double-Base Representations

Representations of minimal length (shortest partitions)

Example: 127 has 783 representations, among which 6 are canonic



Canonic representations are difficult to compute!

Computing Double-Base Representations

Input: An integer $n > 0$

Output: The sequence (a_i, b_i) s.t. $n = \sum_i 2^{a_i} 3^{b_i}$ with $a_i, b_i \geqslant 0$

1: while $n \neq 0$ do
2: Compute the best default approx of n of the form $z = 2^a 3^b$
3: print (a, b)
4: $n \leftarrow n - z$
5: end while

Computing Double-Base Representations

Input: An integer $n > 0$

Output: The sequence (a_i, b_i) s.t. $n = \sum_i 2^{a_i} 3^{b_i}$ with $a_i, b_i \geqslant 0$

1: while $n \neq 0$ do
2: Compute the best default approx of n of the form $z = 2^a 3^b$
3: print (a, b)
4: $n \leftarrow n - z$
5: end while

Does not produce canonic representations...
(E.g: $41 = 36 + 4 + 1 = 32 + 9$)

but satisfies length in $O(\log n / \log \log n)$

Computing Double-Base Representations

Input: An integer $n > 0$
Output: The sequence (a_i, b_i) s.t. $n = \sum_i 2^{a_i} 3^{b_i}$ with $a_i, b_i \geqslant 0$

1: while $n \neq 0$ do
2: Compute the best default approx of n of the form $z = 2^a 3^b$
3: print (a, b)
4: $n \leftarrow n - z$
5: end while

Does not produce canonic representations...
(E.g: $41 = 36 + 4 + 1 = 32 + 9$)

but satisfies length in $O(\log n / \log \log n)$

Minor modifications allow to compute *signed* double-base representations

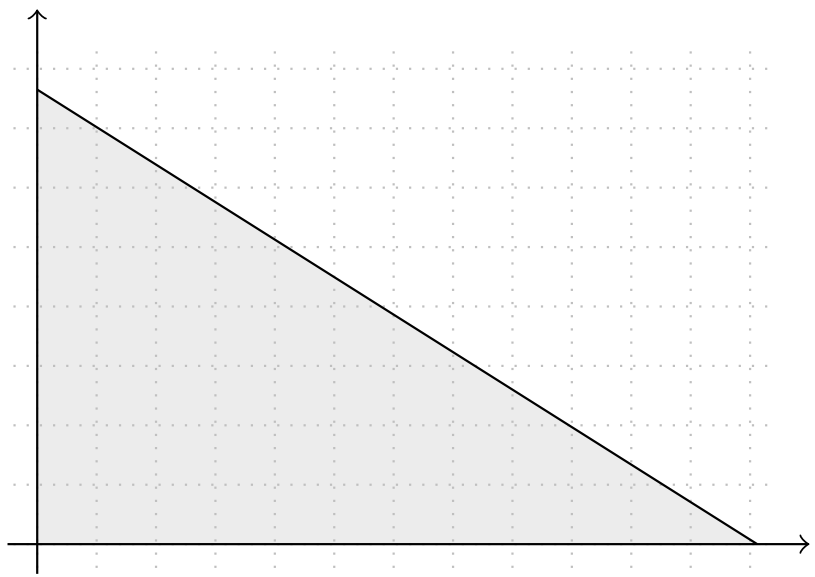
$$n = \pm 2^{a_1} 3^{b_1} \pm 2^{a_2} 3^{b_2} \pm 2^{a_m} 3^{b_m}$$

Best Approximations of the Form $2^a 3^b$

Compute $a, b \geqslant 0$ such that $2^a 3^b = \max\{2^c 3^d \leqslant n \ ; \ (c,d) \in \mathbb{N} \times \mathbb{N}\}$

$$c\alpha + d < a\alpha + b \leqslant \log_3 n \qquad (\alpha = \log_3 2)$$

Solutions: points with integer coordinates under the line of equation $y = -\alpha x + \log_3 n$

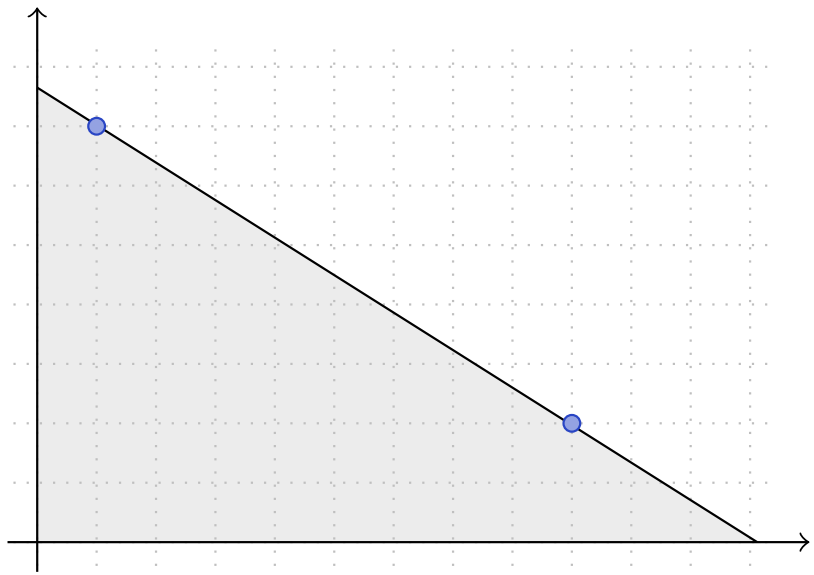


Best Approximations of the Form $2^a 3^b$

Compute $a, b \geqslant 0$ such that $2^a 3^b = \max\{2^c 3^d \leqslant n \ ; \ (c,d) \in \mathbb{N} \times \mathbb{N}\}$

$$c\alpha + d < a\alpha + b \leqslant \log_3 n \qquad (\alpha = \log_3 2)$$

Solutions: points with integer coordinates under the line of equation $y = -\alpha x + \log_3 n$



Best left approx: (a, b) s.t. $\delta(a) = \min\{\delta(x) = \{-\alpha x + \log_3 n\}\}$

Single Constant Multiplication (SCM)

Given an integer constant $C > 0$, find a program which computes $C \times x$ with as few operations $\in \{+/-, \ll\}$ as possible.

Complexity model: $+$ and $-$ have the same cost, $\ll$ are negligible

Single Constant Multiplication (SCM)

Given an integer constant $C > 0$, find a program which computes $C \times x$ with as few operations $\in \{+/-, \ll\}$ as possible.

Complexity model: $+$ and $-$ have the same cost, $\ll$ are negligible

- Naive approach: $151 = (10010111)_2$
  $151x = (x \ll 7) + (x \ll 4) + (x \ll 2) + (x \ll 1) + x$

Single Constant Multiplication (SCM)

Given an integer constant $C > 0$, find a program which computes $C \times x$ with as few operations $\in \{+/-, \ll\}$ as possible.

Complexity model: $+$ and $-$ have the same cost, $\ll$ are negligible

- Naive approach: $151 = (10010111)_2$
  $151x = (x \ll 7) + (x \ll 4) + (x \ll 2) + (x \ll 1) + x$
- Signed digits: $151 = (1010\bar{1}00\bar{1})_{SD2}$
  $151x = (x \ll 7) + (x \ll 5) - (x \ll 3) - x$

Single Constant Multiplication (SCM)

Given an integer constant $C > 0$, find a program which computes $C \times x$ with as few operations $\in \{+/-, \ll\}$ as possible.

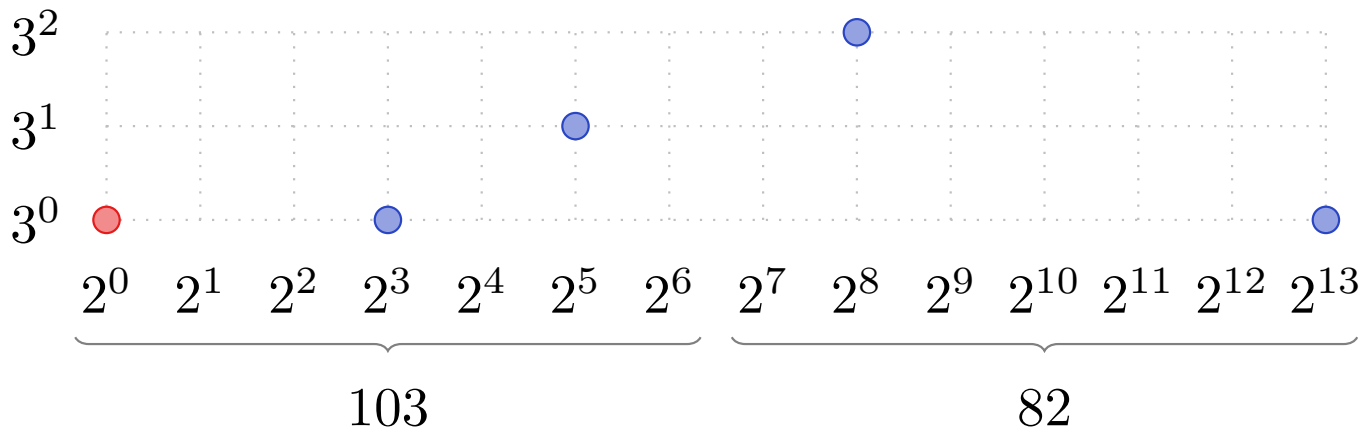
Complexity model: $+$ and $-$ have the same cost, $\ll$ are negligible

- Naive approach: $151 = (10010111)_2$
  $151x = (x \ll 7) + (x \ll 4) + (x \ll 2) + (x \ll 1) + x$
- Signed digits: $151 = (1010\bar{1}00\bar{1})_{SD2}$
  $151x = (x \ll 7) + (x \ll 5) - (x \ll 3) - x$
- Pattern search [Lefèvre 01, Boullis & Tisserand 05]

  Lefèvre's conjecture: SCM is sublinear

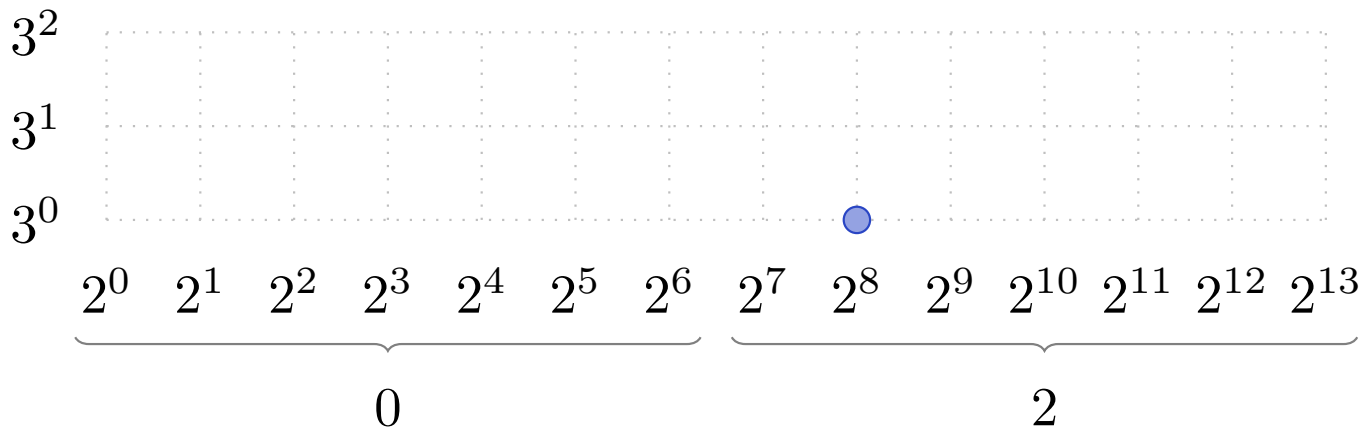
A Double-base Approach to SCM

$$C = 10599 = (1010010\ 1100111)_2 = 82 \times 2^7 + 103$$



A Double-base Approach to SCM

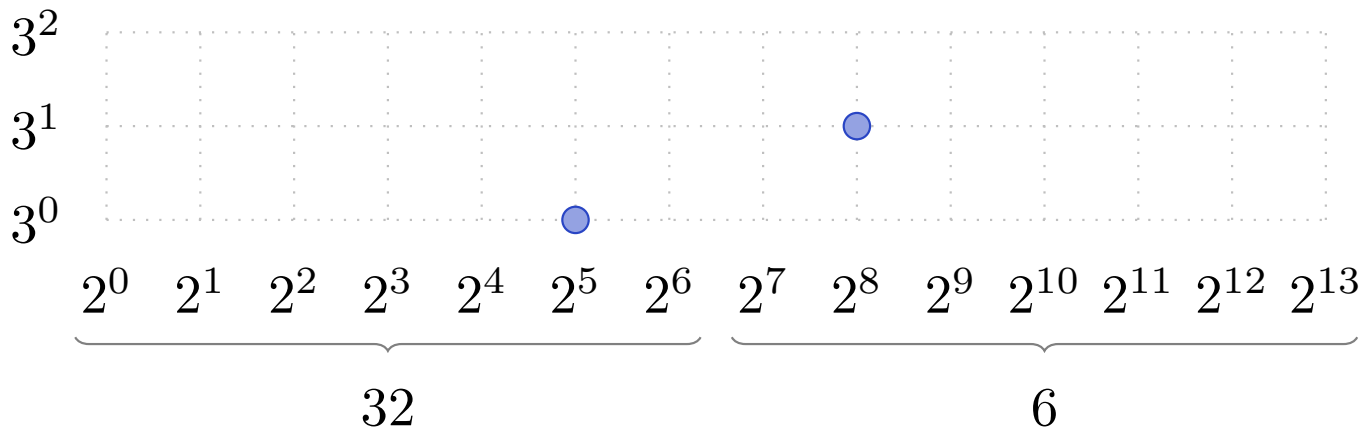
$$C = 10599 = (1010010\ 1100111)_2 = 82 \times 2^7 + 103$$



$$x_0 = (x \ll 8)$$

A Double-base Approach to SCM

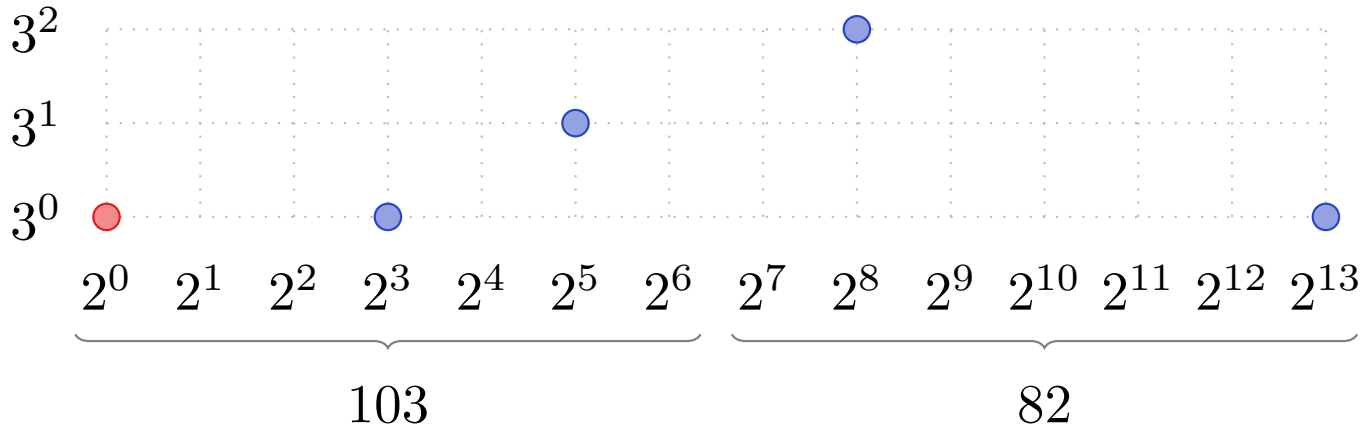
$$C = 10599 = (1010010\ 1100111)_2 = 82 \times 2^7 + 103$$



$$x_0 = (x \ll 8)$$
$$x_1 = 3x_0 + (x \ll 5)$$

A Double-base Approach to SCM

$$C = 10599 = (1010010\ 1100111)_2 = 82 \times 2^7 + 103$$



$$x_0 = (x \ll 8)$$
$$x_1 = 3x_0 + (x \ll 5)$$
$$x_2 = 3x_1 + (x \ll 13) + (x \ll 3) - x$$

Complexity

If $C = \sum_{i=0}^{m-1} \pm 2^{a_i} 3^{b_i}$, with $b_{max} = \max_i\{b_i\}$, then

$$\#\text{ add } = m + b_{max} - 1$$

Theorem [DIZ 07]: Let $C > 0$ of size n. Then, the multiplication by C can be computed in $O(n/\log n)$ additions.

Sketch of proof:

1. Split C into $\log n$ blocks of size $n/\log n$ each
2. Express each block in double-base gives $b_{max} \in O(n/\log n)$
3. $m = \sum_j m_j$ with $m_j \in O(n/\log n^2)$
4. $m \in O(n/\log n)$

Example

The multiplication by any 300-bit constant can be computed with at most 77 additions.

- Split its binary representation into ten 30-bit blocks
- Every block can be represented with at most six $\{2, 3\}$-integers (Because $2^{30} < 1,441,896,119 < 2^{31}$)
- The highest power of 3 that might occur is 18 (Because $3^{18} < 2^{30} < 3^{19}$)
- Therefore, in the worst case, one will need $10 \times 6 + 18 - 1 = 77$ additions

Matrix Polynomial

Evaluate the matrix polynomial

$$G(N, A) = I + A + A^2 + \cdots + A^{N-1}$$

without matrix inversion

- Horner: $G(N, A) = A(A(\ldots(A + I)\ldots) + I) + I$ (too slow)
- Smart decompositions: If $N = JK$, then

$$G(N, A) = G(J, A) \times G(K, A^J)$$

Binary Decomposition

$$G(N, A) = \begin{cases} (I + A) \times G(K, A^2) & \text{if } N = 2K \\ I + (A + A^2) \times G(K, A^2) & \text{if } N = 2K + 1 \end{cases}$$

The number of matrix multiplications (MM) is $\approx 2 \log_2 N$

Ternary Decomposition

$$G(N, A) = \begin{cases} (I + A + A^2) \times G(K, A^3) & \text{if } N = 3K \\ I + (A + A^2 + A^3) \times G(K, A^3) & \text{if } N = 3K + 1 \\ I + A \times (A + A^2 + A^3) \times G(K, A^3) & \text{if } N = 3K + 2 \end{cases}$$

The number of MM is between $3 \log_3 N \approx 1.89 \log_2 N$ and $4 \log_3 N \approx 2.52 \log_2 N$

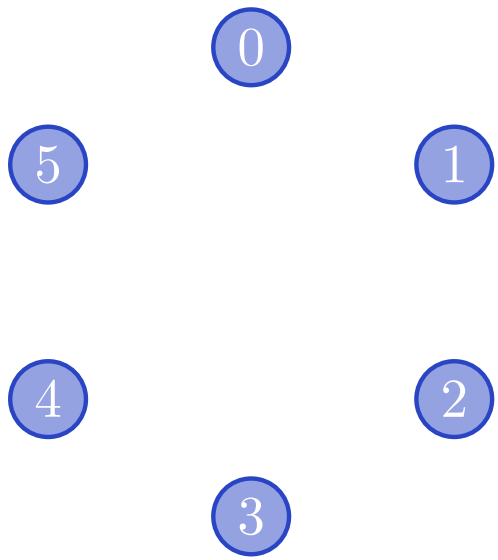
Hybrid Decomposition

$$G(N,A) = \begin{cases} (I + A + A^2) \times G(K, A^3) & \text{if } N = 3K \\ I + (A + A^2 + A^3) \times G(K, A^3) & \text{if } N = 3K + 1 \\ (I + A) \times G(3K + 1, A^2) & \text{if } N = 6K + 2 \\ I + (A + A^2) \times G(3K + 2, A^2) & \text{if } N = 6K + 5 \end{cases}$$

The number of MM is between $3 \log_3 N \approx 1.89 \log_2 N$ and $2 \log_2 N$

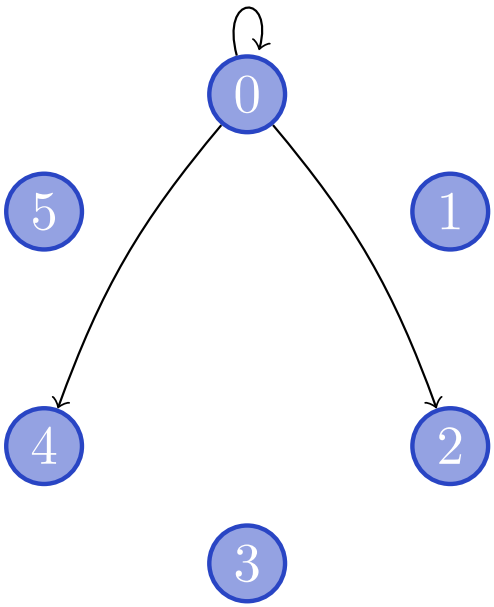
Average Complexity of the Hybrid Approach

$$G(N, A) = \begin{cases} (I + A + A^2) \times G(K, A^3) & \text{if } N = 3K \\ I + (A + A^2 + A^3) \times G(K, A^3) & \text{if } N = 3K + 1 \\ (I + A) \times G(3K + 1, A^2) & \text{if } N = 6K + 2 \\ I + (A + A^2) \times G(3K + 2, A^2) & \text{if } N = 6K + 5 \end{cases}$$



Average Complexity of the Hybrid Approach

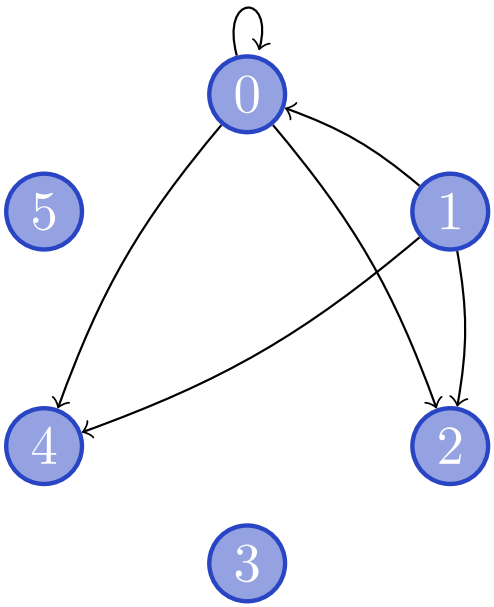
$$G(N,A) = \begin{cases} (I + A + A^2) \times G(K, A^3) & \text{if } N = 3K \\ I + (A + A^2 + A^3) \times G(K, A^3) & \text{if } N = 3K+1 \\ (I + A) \times G(3K+1, A^2) & \text{if } N = 6K+2 \\ I + (A + A^2) \times G(3K+2, A^2) & \text{if } N = 6K+5 \end{cases}$$



$$\begin{pmatrix} 1/3 & 0 & 1/3 & 0 & 1/3 & 0 \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \end{pmatrix}$$

Average Complexity of the Hybrid Approach

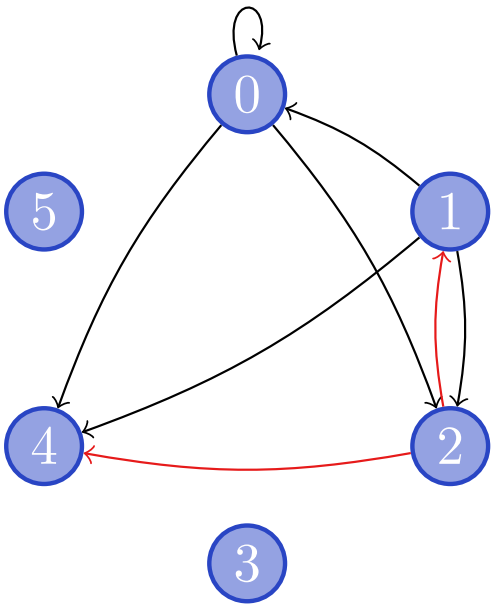
$$G(N, A) = \begin{cases} (I + A + A^2) \times G(K, A^3) & \text{if } N = 3K \\ I + (A + A^2 + A^3) \times G(K, A^3) & \text{if } N = 3K + 1 \\ (I + A) \times G(3K + 1, A^2) & \text{if } N = 6K + 2 \\ I + (A + A^2) \times G(3K + 2, A^2) & \text{if } N = 6K + 5 \end{cases}$$



$$\begin{pmatrix} 1/3 & 0 & 1/3 & 0 & 1/3 & 0 \\ 1/3 & 0 & 1/3 & 0 & 1/3 & 0 \\ & & & & & \\ & & & & & \\ & & & & & \\ & & & & & \end{pmatrix}$$

Average Complexity of the Hybrid Approach

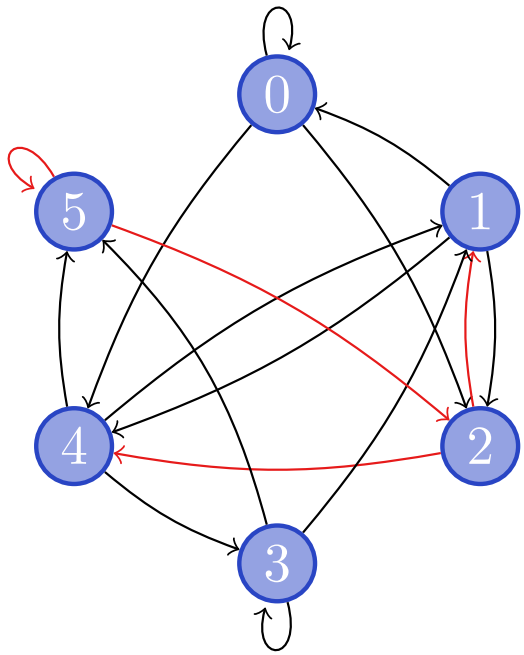
$$G(N, A) = \begin{cases} (I + A + A^2) \times G(K, A^3) & \text{if } N = 3K \\ I + (A + A^2 + A^3) \times G(K, A^3) & \text{if } N = 3K + 1 \\ (I + A) \times G(3K + 1, A^2) & \text{if } N = 6K + 2 \\ I + (A + A^2) \times G(3K + 2, A^2) & \text{if } N = 6K + 5 \end{cases}$$



$$\begin{pmatrix} 1/3 & 0 & 1/3 & 0 & 1/3 & 0 \\ 1/3 & 0 & 1/3 & 0 & 1/3 & 0 \\ 0 & 1/2 & 0 & 0 & 1/2 & 0 \\ & & & & & \\ & & & & & \\ & & & & & \end{pmatrix}$$

Average Complexity of the Hybrid Approach

$$G(N,A) = \begin{cases} (I + A + A^2) \times G(K, A^3) & \text{if } N = 3K \\ I + (A + A^2 + A^3) \times G(K, A^3) & \text{if } N = 3K+1 \\ (I + A) \times G(3K+1, A^2) & \text{if } N = 6K+2 \\ I + (A + A^2) \times G(3K+2, A^2) & \text{if } N = 6K+5 \end{cases}$$



$$\begin{pmatrix} 1/3 & 0 & 1/3 & 0 & 1/3 & 0 \\ 1/3 & 0 & 1/3 & 0 & 1/3 & 0 \\ 0 & 1/2 & 0 & 0 & 1/2 & 0 \\ 0 & 1/3 & 0 & 1/3 & 0 & 1/3 \\ 0 & 1/3 & 0 & 1/3 & 0 & 1/3 \\ 0 & 0 & 1/2 & 0 & 0 & 1/2 \end{pmatrix}$$

Stationary probabilities: $p_\infty = (1/10 \;\; 1/5 \;\; 1/5 \;\; 1/10 \;\; 1/5 \;\; 1/5)$

Average base: $\beta = 2^{2/5}3^{3/5} \approx 2.550849$

Average number of MM: $(3p_3 + 2p_2)\log_\beta 2 \approx 1.92 \log_2 N$

Fast Exponentiation

- Generic: given $g \in (G, \times)$ and $n \geq 0$, compute g^n
- Elliptic curve scalar multiplication: given $P \in E(\mathbb{K})$ and $k \geq 0$, compute $[k]P = P + P + \cdots + P$ (k times)
- Multi-scalar multiplication: given $k_1, k_2, P, Q \in E(\mathbb{K})$, compute $[k_1]P + [k_2]Q$

Scalar Multiplication Algorithms

Double-and-Add: $k = \sum_{i=0}^{n-1} k_i 2^i$, with $k_i \in \{0, 1\}$

$$314159 = 1\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 1.$$

$n - 1$ doublings, $n/2$ additions on average

NAF, CSD: $k_i \in \{\bar{1}, 0, 1\}$

$$\mathsf{NAF}_2(314159) = 1\ 0\ 1\ 0\ \bar{1}\ 0\ 1\ 0\ \bar{1}\ 0\ \bar{1}\ 0\ 1\ 0\ \bar{1}\ 0\ 0\ 0\ \bar{1}$$

n doublings, $n/3$ additions on average

NAF_w, Window Methods: $|k_i| < 2^{w-1}$ (process w bits at a time)

$$\mathsf{NAF}_3(314159) = 1\ 0\ 0\ 0\ 3\ 0\ 0\ 1\ 0\ 0\ 3\ 0\ 0\ 0\ 3\ 0\ 0\ 0\ \bar{1}$$

n doublings, $n/(w+1)$ additions on average

Double-Base Scalar Multiplication

The *double-base chain* approach:

$$k = \sum_{i=0}^{m-1} k_i \, 2^{a_i} 3^{b_i}, \text{ where } k_i \in \{-1, 1\} \text{ and } (a_i, b_i) \searrow$$

$$314159 = 2^4 3^9 - 2^0 3^6 - 3^3 - 3^2 - 3 - 1$$
$$[314159]P = 3(3(3(3^3(2^4 3^3 P - P) - P) - P) - P) - P$$

Double-Base Scalar Multiplication

The *double-base chain* approach:

$$k = \sum_{i=0}^{m-1} k_i \, 2^{a_i} 3^{b_i}, \text{ where } k_i \in \{-1, 1\} \text{ and } (a_i, b_i) \searrow$$

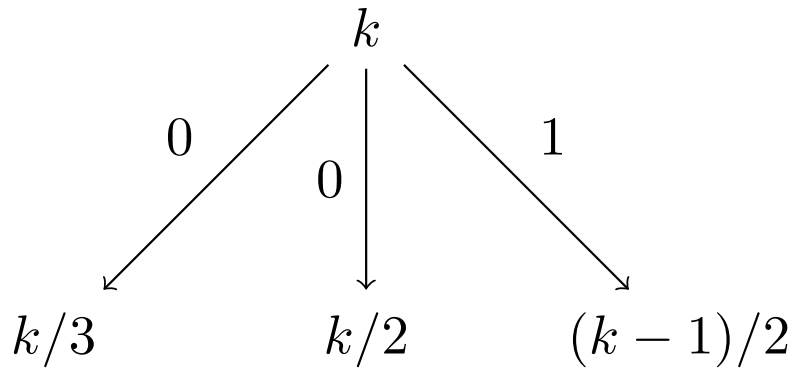
$$314159 = 2^4 3^9 - 2^0 3^6 - 3^3 - 3^2 - 3 - 1$$
$$[314159]P = 3(3(3(3^3(2^4 3^3 P - P) - P) - P) - P) - P$$

Yao/Meloni's approach:

$$k = \sum_{i=0}^{m-1} D_i \, 2^i, \text{ where } D_i = \sum_j d_j 3^j P \text{ with } d_j \in \{-1, 0, 1\}$$

$$314159 = 2^4 3^9 + 2^8 3^1 - 1$$
$$D_0 = -P, \quad D_4 = 3^9 P, \quad D_8 = 3P$$
$$[314159]P = 2^4(2^4 D_8 + D_4) + D_0$$

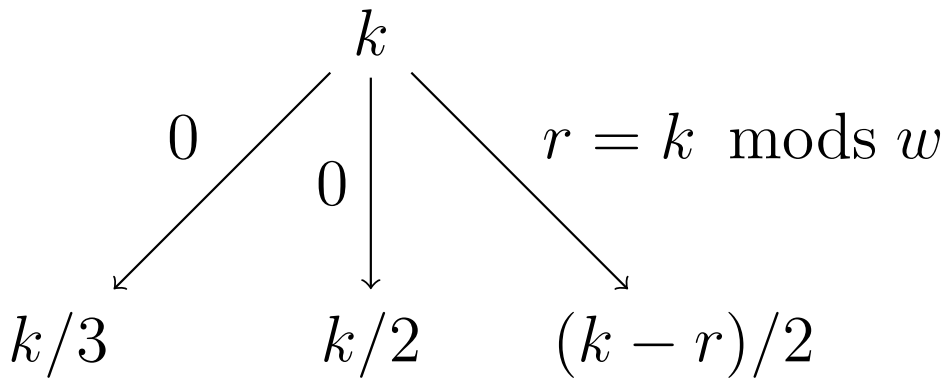
Hybrid Binary-Ternary Form (HBTF)



$$\texttt{hbtf} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$
$$\texttt{base} = \begin{bmatrix} 2 & 2 & 3 & 2 & 3 & 3 & 3 & 2 \end{bmatrix}$$

$$727 = 2^3 3^4 + 2^1 3^3 + 2^0 3^0$$

Window Hybrid Binary-Ternary Form (w-HBTF)



$$\begin{aligned} 12\text{-hbtf} &= [5 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad \bar{5}] \\ \texttt{base} &= [2 \quad 3 \quad 2 \quad 2 \quad 3 \quad 2 \quad 2] \end{aligned}$$

$$727 = 5 \cdot 2^4 3^2 + 2^2 3^1 - 5$$

$$\begin{aligned} 18\text{-hbtf} &= [5 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 7] \\ \texttt{base} &= [2 \quad 3 \quad 3 \quad 2 \quad 2 \quad 2 \quad 2] \end{aligned}$$

$$727 = 5 \cdot 2^4 3^2 + 7$$

Average complexity of w-HTBF

	w-NAF	6-HBTF	12HBTF	18-HBTF	24HBTF	36-HBTF
avg base	2	2.38	2.29	2.51	2.23	2.40
avg #2	$n+1$	$0.46n$	$0.56n$	$0.63n$	$0.34n$	$0.43n$
avg #3	0	$0.34n$	$0.28n$	$0.42n$	$0.24n$	$0.36n$
avg #dig	$n/(w+1)$	$0.23n$	$0.19n$	$0.17n$	$0.16n$	$0.14n$
Pre	$2^{w-2}-1$	0	1	2	3	5

Practical complexity depends on the relative cost between a cube (triple) and a combined square + multiply (double + add)

Comments on Double-Base Chains

- The w-HBTF generate double-base chains from right to left
- The greedy approach can be adapted to compute left-to-right double-base chains
- None of these algorithms give a chain of minimal length

Chain Partitions

A *(strictly) chain partition* is a partition of the form

$$n = a_1 + a_2 + \cdots + a_k$$

into (distinct) positive integers such that $a_k | a_{k-1} | \ldots | a_2 | a_1$.

$$\begin{aligned} 873 &= 512 + 256 + 64 + 32 + 8 + 1 \\ &= 720 + 120 + 24 + 6 + 2 + 1 \\ &= 696 + 174 + 3 \end{aligned}$$

[Erdös-Loxton 1979]

- $\#$ partitions of this type: $p(n) \geq \log_2 n$ for $n \geq 6$
- $\#$ partitions of this type whose smallest part is 1: $p_1(n) \geq \frac{1}{2} \log_2 n$ for $n \geq 27$ and $n - 1$ not a prime
- $P(x) = \sum_{1 \leq n \leq x} p(n) \approx cx^\rho$, where c is an unknown constant and ρ is the unique root of $\zeta(s) - 2$, where ζ is the Riemann zeta function.

Strictly Chained (p, q)-ary Partitions

Strictly chained (p, q)-ary partitions are chain partitions with distinct parts of the form $p^a q^b$, where $p, q \geq 2$ and $(p, q) = 1$.

Notations:

- $\Omega(U)$: The set of all strictly chained (p, q)-ary partitions of U
- $\Omega^*(U)$: The subset of partitions $\omega \in \Omega(U)$ with no part 1
- $W(U) = \#\Omega(U)$
- $W^*(U) = \#\Omega^*(U)$

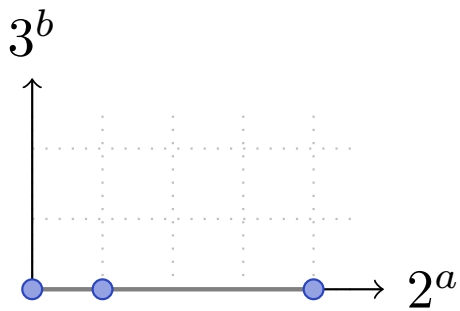
Special cases of interest:

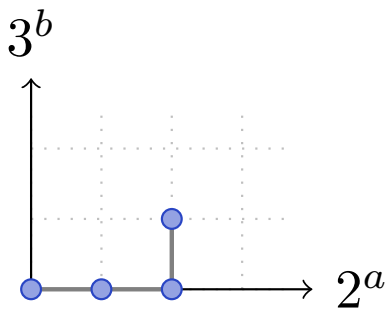
- $\min(p, q) = 2$
- $(p, q) = (2, 3)$

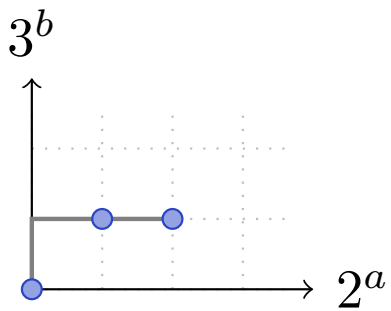
Graphic Representation and Encoding

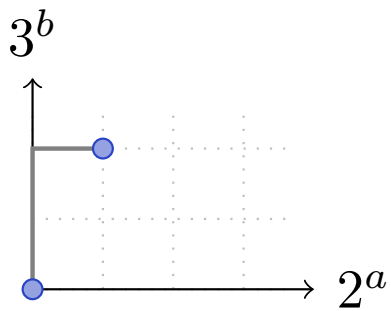
Example with $(p, q) = (2, 3)$.

$$\Omega(19) = \{(16, 2, 1), (12, 4, 2, 1), (12, 6, 1), (18, 1)\}$$





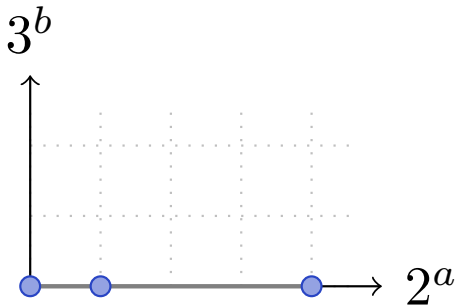




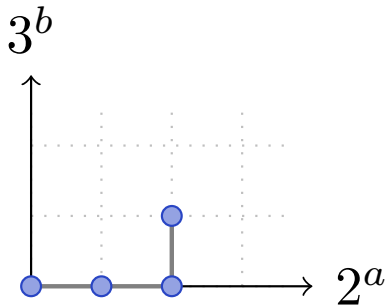
Graphic Representation and Encoding

Example with $(p, q) = (2, 3)$.

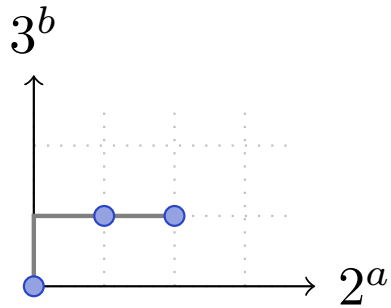
$$\Omega(19) = \{(16, 2, 1), (12, 4, 2, 1), (12, 6, 1), (18, 1)\}$$



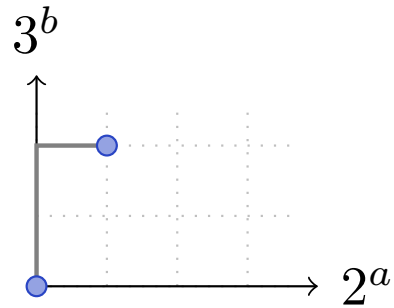
11003



1133



3013



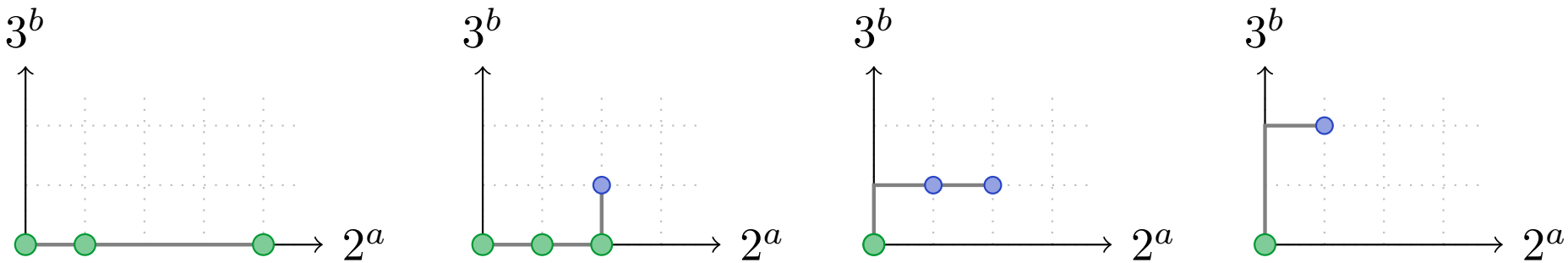
3203

The couples of exponents (a, b) form a chain in $\mathbb{N}^2$. They can be encoded with words on $\{0,1,2,3\}^*$. (Conventions: words end with '3', we go North before going East)

Graphic Representation and Encoding

Example with $(p, q) = (2, 3)$.

$$\Omega(19) = \{(16, 2, 1), (12, 4, 2, 1), (12, 6, 1), (18, 1)\}$$



If $\min(p, q) = 2$, the *binary amount* of a partition is equal to the sum of all its binary parts (● parts) or 0 if none.

Complete Generation

Lemma: (+ denotes union of disjoint sets)

$$\Omega(U) = \Omega^*(U) + {}^1\Omega^*(U-1), \qquad \Omega^*(U) = {}^p\Omega(U/p) \cup {}^q\Omega(U/q)$$

Complete Generation

Lemma: (+ denotes union of disjoint sets)

$$\Omega(U) = \Omega^*(U) + {}^1\Omega^*(U-1), \qquad \Omega^*(U) = {}^p\Omega(U/p) \cup {}^q\Omega(U/q)$$

Formula for $(p,q) = (2,3)$

$$\begin{aligned}
\Omega(3U) &= {}^3\Omega(U) + {}^1\Omega(3U-1) \\
\Omega(6U-1) &= {}^{12}\Omega(3U-1) \\
\Omega(6U+1) &= {}^{13}\Omega(2U) + {}^{11}\Omega(6U-1) \\
\Omega(6U+2) &= {}^2\Omega(3U+1) \\
\Omega(6U+4) &= {}^{13}\Omega(2U+1) + {}^2\Omega(3U+2)
\end{aligned}$$

Examples

$\Omega(217) = \{$ 3000133, 30001003, 322033, 3220003, 3200013, 10011013, 1001333, 10013003 $\}$

$\Omega(95) = \{$ 1111103 $\}$

$\Omega(6143) = \{$ 11111111111103 $\}$

$W(3 \cdot 2^a - 1) = 1$

$\Omega(575) = \{$ 1111110003, 111111033 $\}$

$\Omega(959) = \{$ 1111110113, 1111110303 $\}$

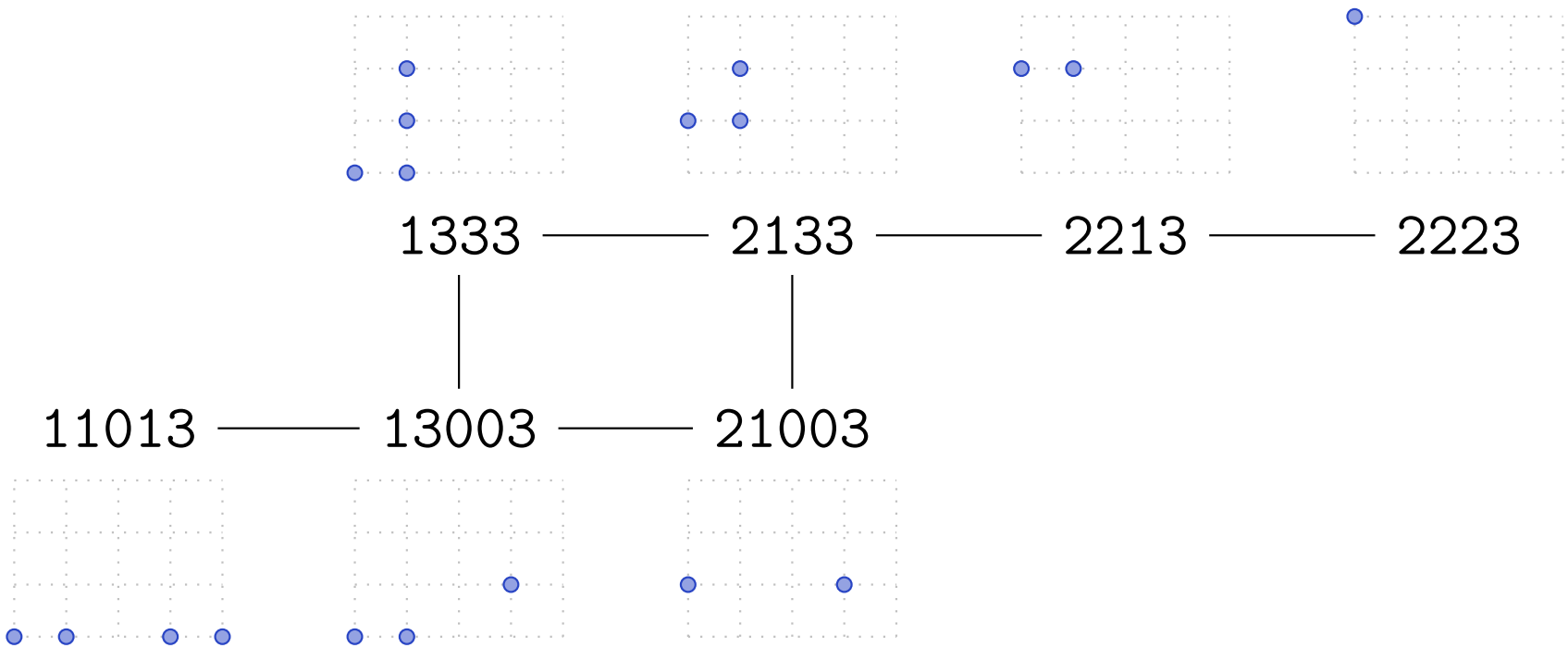
$W(9 \cdot 2^a - 1) = W(15 \cdot 2^a - 1) = 2$

Transitions

$1 + 2 = 3$ $\qquad$ $4 = 3 + 1$ (and generalizations)

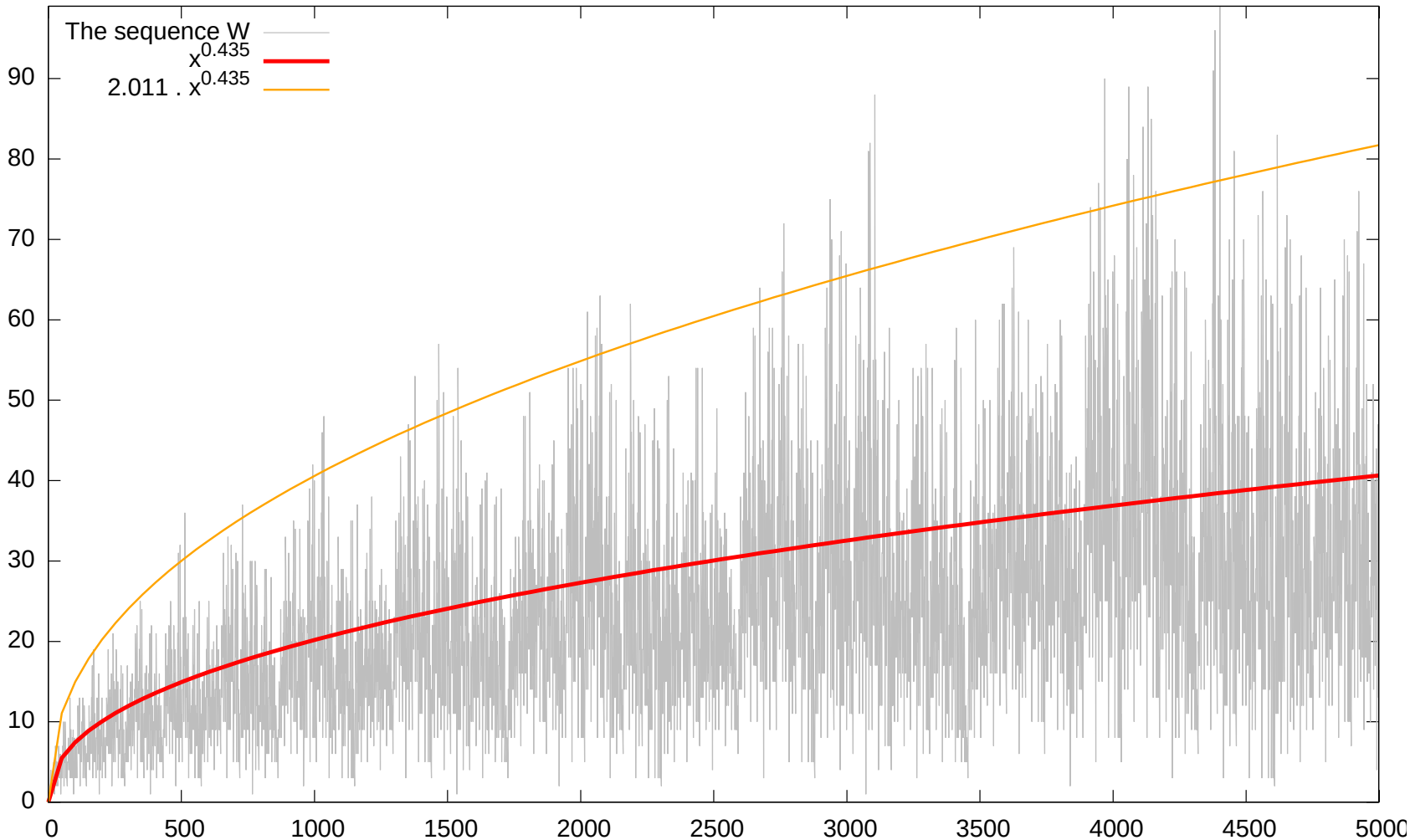
The transition graph is symmetric and connected

Example: $G(27)$ for $(p, q) = (2, 3)$



The sequence W

For any pair (p, q), the sequence W behaves rather irregularly



Shortest Partitions

Our formula can be adapted to compute the length $\sigma(U)$ of a shortest unsigned double-base chain for U

Size of U	greedy		shortest	
(in bits)	$+$	$+/-$	$+$	$+/-$
64	26.09	18.55	17.22	–
128	54.52	34.88	33.27	–
160	72.21	44.96	40.85	–
256	119.26	75.78	64.35	–

Average values for $10,000$ random integers

Numerical experiments suggest $\sigma(U) \approx \log_2(U)/4$

Double-Base Representations of Minimal Length

Smallest $n > 0$ requiring m parts

m	$+$	$+/-$
2	5	5
3	23	103
4	431	4,985
5	18,431	641,687
6	3,448,733	326,552,783
7	1,441,896,119	–
8	–	–

How far is the greedy from optimal in the signed case?

Thank you!

http://www.lirmm.fr/~imbert

Laurent.Imbert@lirmm.fr