Quelques systèmes de numération exotiques (et applications)

Laurent Imbert

ARITH – LIRMM, CNRS, Univ. Montpellier 2

Séminaire CACAO, Nancy, février 2008

The double-base number system

Every integer $n > 0$ can be written as

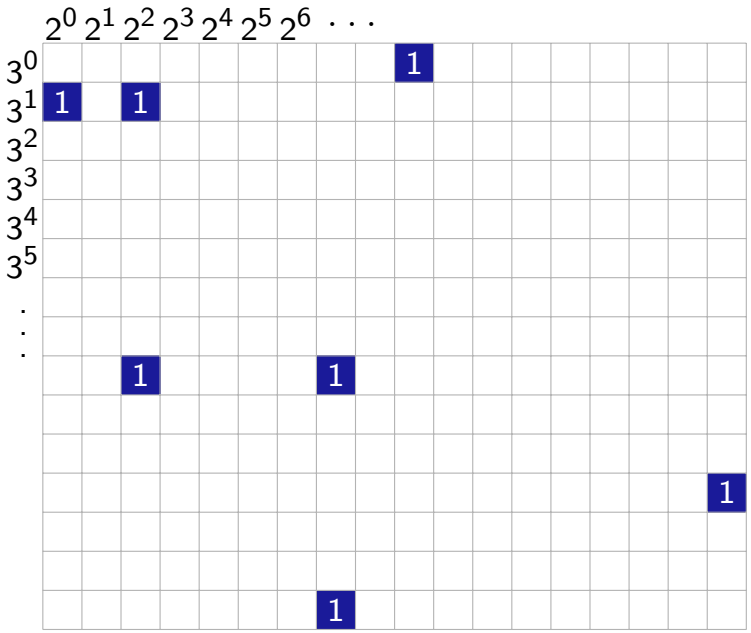
$$n = \sum_{i=0}^{m} 2^{a_i} 3^{b_i}, \ a_i, b_i \geq 0$$

The double-base number system

Every integer $n > 0$ can be written as

$$n = \sum_{i=0}^{m} 2^{a_i} 3^{b_i}, \ a_i, b_i \geq 0$$

Example: $n = 23832098195$



The double-base number system

Every integer $n > 0$ can be written as

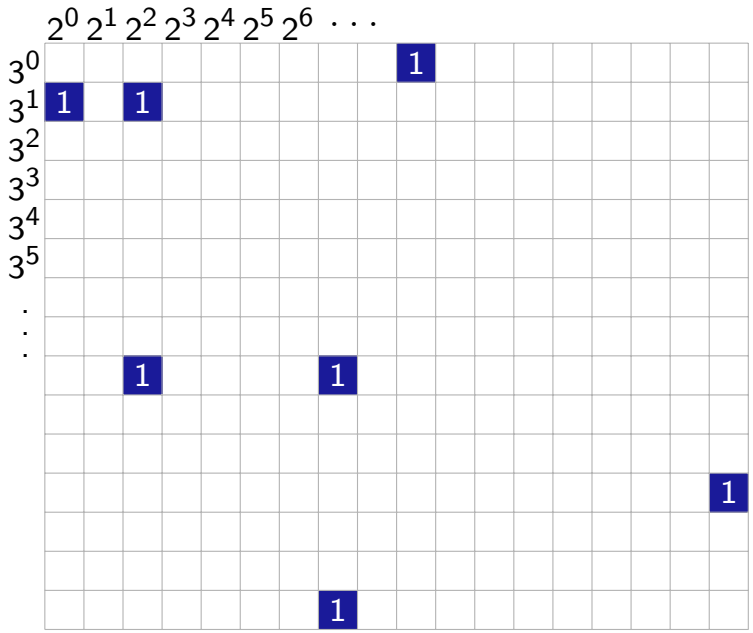
$$n = \sum_{i=0}^{m} 2^{a_i} 3^{b_i}, \ a_i, b_i \geq 0$$

Partition of n with distinct parts of the form $2^a 3^b$ ($\{2,3\}$-integers)

3-partition of n

$$n = p_0 + 3p_1 + 3^2 p_2 + \cdots + 3^m p_m$$

Example: $n = 23832098195$



Properties

Redundancy: # of representations of a given n

$$f(n) = \begin{cases} f(n-1) + f(n/3) & \text{if } n \equiv 0 \pmod 3, \\ f(n-1) & \text{otherwise.} \end{cases}$$

$f(3n) =$ number of partitions of $3n$ into powers of 3

1, 2, 3, 5, 7, 9, 12, 15, 18, 23, 28, 33, 40, 47, 54, 63, 72, 81, 93, ...

Sloane's on-line encyclopedia of integer sequences #A005704

Properties

Sparseness: # of parts (or length m of the expansion)

$$m \in O(\log n / \log \log n)$$

Numerical experiments show that the constant $\simeq 1$

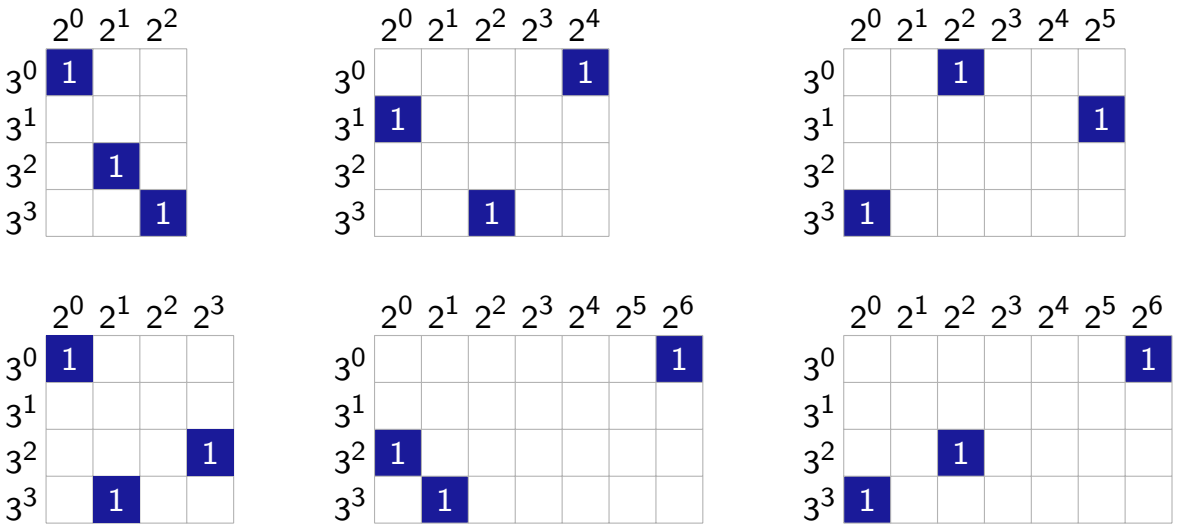
Smallest $n > 0$ requiring m terms:

m	unsigned DBNS	Binary	$\log n / \log \log n$
2	5	3	3.38
3	23	5	2.74
4	431	9	3.36
5	18 431	15	4.29
6	3 448 733	22	5.55
7	1 441 896 119	31	6.91
8	-	-	-

Canonic representations

Representation of minimal length (smallest partitions)

Example: $f(127) = 783$ among which 6 are canonic



Canonic representations are extremely difficult to compute!

Conversion: a greedy approach

Input: A positive integer n

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

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

Conversion: a greedy approach

Input: A positive integer n

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

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

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

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

Conversion: a greedy approach

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

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

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

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

Best default approximation of the form $2^a 3^b$

The problem: find $a, b \geq 0$ such that

$$2^a 3^b = \max\{2^c 3^d \leq n : (c, d) \in \mathbb{N}^2\}$$

Best default approximation of the form $2^a 3^b$

The problem: find $a, b \geq 0$ such that

$$2^a 3^b = \max\{2^c 3^d \leq n : (c, d) \in \mathbb{N}^2\}$$

Equivalently, find $a, b \geq 0$ such that, for all $c \neq a, d \neq b$

$$c \log 2 + d \log 3 < a \log 2 + b \log 3 \leq \log n$$

Best default approximation of the form $2^a 3^b$

The problem: find $a, b \geq 0$ such that

$$2^a 3^b = \max\{2^c 3^d \leq n : (c, d) \in \mathbb{N}^2\}$$

Equivalently, find $a, b \geq 0$ such that, for all $c \neq a, d \neq b$

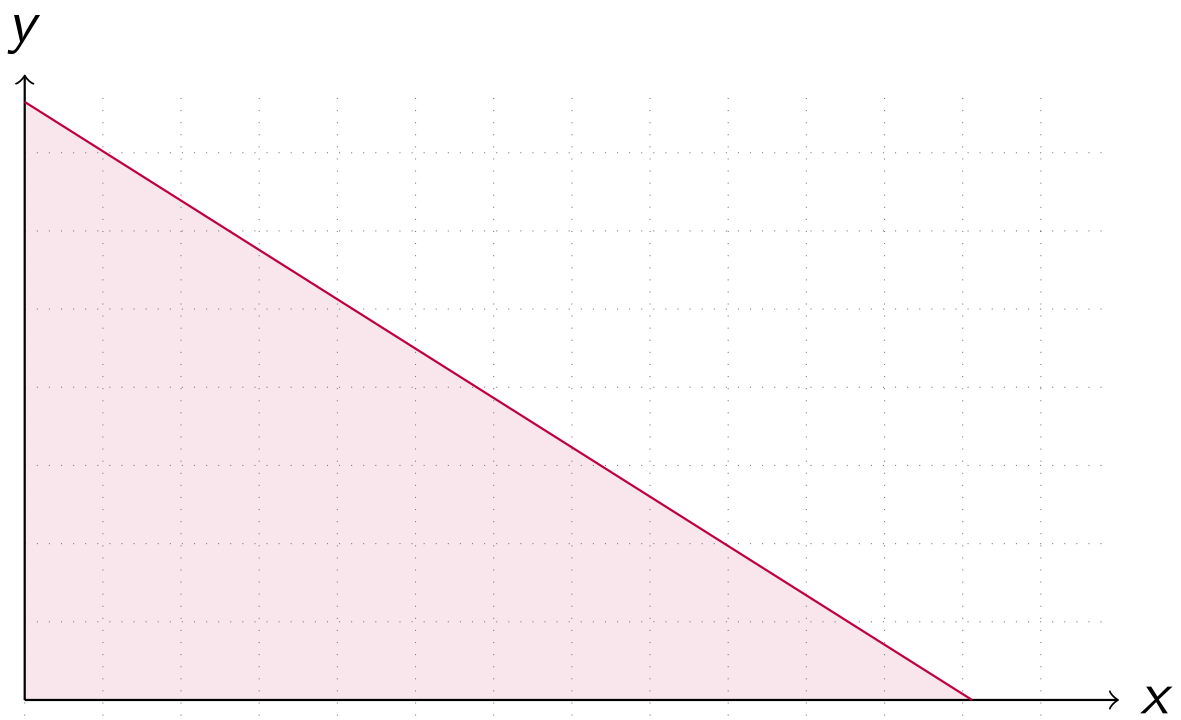
$$c \log 2 + d \log 3 < a \log 2 + b \log 3 \leq \log n$$

$$c \log_3 2 + d < a \log_3 2 + b \leq \log_3 n$$

Geometric interpretation

$c\alpha + d < a\alpha + b \leq \log_3 n \quad (\alpha = \log_3 2, \quad \{\} = \text{fractional part})$

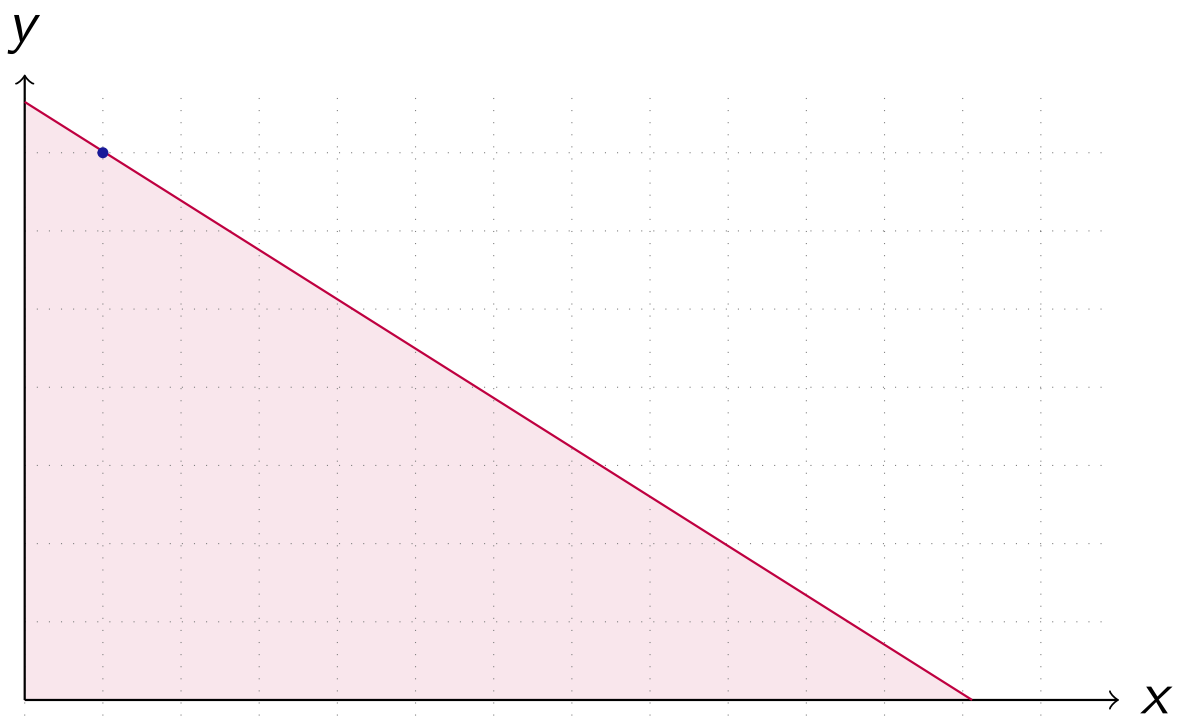
Solutions: points under the line of equation $y = -\alpha x + \log_3 n$



Geometric interpretation

$c\alpha + d < a\alpha + b \leq \log_3 n \quad (\alpha = \log_3 2, \quad \{\} = \text{fractional part})$

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



Best approx: (a, b) such that $\delta(a) = \min\{\delta(x) = \{-\alpha x + \log_3 n\}\}$

Continued fractions

- α irrational ; simple infinite CF: $\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}$
- Partial quotients: $a_0 = \lfloor \alpha \rfloor, \quad a_i \geq 1$

Continued fractions

- α irrational ; simple infinite CF: $\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}$
- Partial quotients: $a_0 = \lfloor \alpha \rfloor, \quad a_i \geq 1$
- Convergents: $p_n/q_n = [a_0, a_1, a_2, \ldots, a_n] \longrightarrow \alpha$

Continued fractions

- α irrational ; simple infinite CF: $\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}$
- Partial quotients: $a_0 = \lfloor \alpha \rfloor, \quad a_i \geq 1$
- Convergents: $p_n/q_n = [a_0, a_1, a_2, \ldots, a_n] \longrightarrow \alpha$
- $\left| \alpha - \dfrac{p_n}{q_n} \right| \leq \dfrac{1}{q_n^2}$

Continued fractions

- α irrational ; simple infinite CF: $\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}$
- Partial quotients: $a_0 = \lfloor \alpha \rfloor, \quad a_i \geq 1$
- Convergents: $p_n/q_n = [a_0, a_1, a_2, \ldots, a_n] \longrightarrow \alpha$
- $\left| \alpha - \dfrac{p_n}{q_n} \right| \leq \dfrac{1}{q_n^2}$
- $\dfrac{p_0}{q_0} = 0, \ \dfrac{p_1}{q_1} = 1, \ \ldots, \ \dfrac{p_{n+1}}{q_{n+1}} = \dfrac{a_{n+1}p_n + p_{n-1}}{a_{n+1}q_n + q_{n-1}}$

Continued fractions

- α irrational ; simple infinite CF: $\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}$
- Partial quotients: $a_0 = \lfloor \alpha \rfloor, \quad a_i \geq 1$
- Convergents: $p_n/q_n = [a_0, a_1, a_2, \ldots, a_n] \longrightarrow \alpha$
- $\left| \alpha - \dfrac{p_n}{q_n} \right| \leq \dfrac{1}{q_n^2}$
- $\dfrac{p_0}{q_0} = 0, \ \dfrac{p_1}{q_1} = 1, \ \ldots, \ \dfrac{p_{n+1}}{q_{n+1}} = \dfrac{a_{n+1}p_n + p_{n-1}}{a_{n+1}q_n + q_{n-1}}$
- even convergents $< \alpha <$ odd convergents

Ostrowski's number system for integers

Every integer N can be written uniquely in the form

$$N = \sum_{k=1}^{m} d_k q_{k-1},$$

where $0 \leq d_k \leq a_k$ $(d_1 \leq a_1 - 1)$ and $d_k = 0$ if $d_{k+1} = a_{k+1}$

Ostrowski's number system for integers

Every integer N can be written uniquely in the form

$$N = \sum_{k=1}^{m} d_k q_{k-1},$$

where $0 \leq d_k \leq a_k$ ($d_1 \leq a_1 - 1$) and $d_k = 0$ if $d_{k+1} = a_{k+1}$

Example 1: $\alpha = \log_3 2$ $\qquad 481 = 5q_7 + 3q_5 + q_3 + q_1$

$\log_3 2$	0	1	1	1	2	2	3	1	5	2	...
p_n	0	1	1	2	5	12	41	53	306	665	...
q_n	1	1	2	3	8	19	65	84	485	1054	...

Ostrowski's number system for integers

Every integer N can be written uniquely in the form

$$N = \sum_{k=1}^{m} d_k q_{k-1},$$

where $0 \leq d_k \leq a_k$ ($d_1 \leq a_1 - 1$) and $d_k = 0$ if $d_{k+1} = a_{k+1}$

Example 1: $\alpha = \log_3 2$ $\qquad 481 = 5q_7 + 3q_5 + q_3 + q_1$

$\log_3 2$	0	1	1	1	2	2	3	1	5	2	...
p_n	0	1	1	2	5	12	41	53	306	665	...
q_n	1	1	2	3	8	19	65	84	485	1054	...

Example 2: $\alpha = \dfrac{1+\sqrt{5}}{2} = [1, 1, 1, 1, \ldots]$ $\qquad 481 = F_{13} + F_{10} + F_6 + F_2$

(q_n): Fibonacci numbers $(1, 1, 2, 3, 5, 8, 13, \ldots)$, Zeckendorf repr.

Ostrowski's number system for reals

Every real number $-\alpha \leq \beta < 1 - \alpha$ can be written uniquely in the form

$$\beta = \sum_{k=1}^{+\infty} b_k \theta_{k-1}, \qquad (\theta_n)_n = (q_n\alpha - p_n)_n$$

where $0 \leq b_k \leq a_k$, $(b_1 \leq a_1 - 1)$, $b_k = 0$ if $b_{k+1} = a_{k+1}$ and $b_k \neq a_k$ for infinitely many even and odd integers

Example 3: $n = 26831$ $\qquad \beta = \{\log_3 n\} = 0.281994\ldots$

i	a_i	p_i	q_i	$\theta_i = q_i\alpha - p_i$
0	0	0	1	0.63093
1	1	1	1	−0.36907
2	1	1	2	0.26186
3	1	2	3	−0.10721
4	2	5	8	0.04744
5	2	12	19	−0.01234
6	3	41	65	0.01043

Ostrowski's number system for reals

Every real number $-\alpha \leq \beta < 1-\alpha$ can be written uniquely in the form

$$\beta = \sum_{k=1}^{+\infty} b_k \theta_{k-1}, \qquad (\theta_n)_n = (q_n\alpha - p_n)_n$$

where $0 \leq b_k \leq a_k$, $(b_1 \leq a_1 - 1)$, $b_k = 0$ if $b_{k+1} = a_{k+1}$ and $b_k \neq a_k$ for infinitely many even and odd integers

Example 3: $n = 26831$

$$\beta = \{\log_3 n\} = 0.281994\ldots$$

$$\beta = \theta_2 + 0.020135\ldots$$

i	a_i	p_i	q_i	$\theta_i = q_i\alpha - p_i$
0	0	0	1	0.63093
1	1	1	1	−0.36907
2	1	1	2	0.26186
3	1	2	3	−0.10721
4	2	5	8	0.04744
5	2	12	19	−0.01234
6	3	41	65	0.01043

Ostrowski's number system for reals

Every real number $-\alpha \leq \beta < 1 - \alpha$ can be written uniquely in the form

$$\beta = \sum_{k=1}^{+\infty} b_k \theta_{k-1}, \qquad (\theta_n)_n = (q_n\alpha - p_n)_n$$

where $0 \leq b_k \leq a_k$, $(b_1 \leq a_1 - 1)$, $b_k = 0$ if $b_{k+1} = a_{k+1}$ and $b_k \neq a_k$ for infinitely many even and odd integers

Example 3: $n = 26831$

i	a_i	p_i	q_i	$\theta_i = q_i\alpha - p_i$
0	0	0	1	0.63093
1	1	1	1	−0.36907
2	1	1	2	0.26186
3	1	2	3	−0.10721
4	2	5	8	0.04744
5	2	12	19	−0.01234
6	3	41	65	0.01043

$$\beta = \{\log_3 n\} = 0.281994\ldots$$

$$\beta = \theta_2 + 0.020135\ldots$$

$$\beta = \theta_2 + 2\theta_6 - 0.00073\ldots$$

Back to our problem

Compute the best approximation of n of the form $2^a 3^b$

with $0 \leq a < \log_2 n, \quad 0 \leq b < \log_3 n$

- $n = 26831, \qquad \log_3 n = 9.281994\ldots$
- $\{\log_3 n\} = \theta_2 + 2\theta_6 + \cdots$

Back to our problem

Compute the best approximation of n of the form $2^a 3^b$

with $0 \leq a < \log_2 n, \quad 0 \leq b < \log_3 n$

- $n = 26831, \qquad \log_3 n = 9.281994\ldots$
- $\{\log_3 n\} = \theta_2 + 2\theta_6 + \cdots$
- $\log_3 n = (q_2 + 2q_6 + \cdots)\alpha - (p_2 + 2p_6 + \cdots) + \lfloor \log_3 n \rfloor$

Back to our problem

Compute the best approximation of n of the form $2^a 3^b$

with $0 \leq a < \log_2 n, \quad 0 \leq b < \log_3 n$

- $\mathrm{n} = 26831, \qquad \log_3 n = 9.281994\ldots$
- $\{\log_3 n\} = \theta_2 + 2\theta_6 + \cdots$
- $\log_3 n = (q_2 + 2q_6 + \cdots)\alpha - (p_2 + 2p_6 + \cdots) + \lfloor \log_3 n \rfloor$
- $2^{q_2} 3^{\lfloor \log_3 n \rfloor - p_2} = 2^2 3^8 = 26244, \qquad \varepsilon = 587$

Back to our problem

Compute the best approximation of n of the form $2^a 3^b$

with $0 \leq a < \log_2 n, \quad 0 \leq b < \log_3 n$

- $n = 26831, \qquad \log_3 n = 9.281994\ldots$
- $\{\log_3 n\} = \theta_2 + 2\theta_6 + \cdots$
- $\log_3 n = (q_2 + 2q_6 + \cdots)\alpha - (p_2 + 2p_6 + \cdots) + \lfloor \log_3 n \rfloor$
- $2^{q_2} 3^{\lfloor \log_3 n \rfloor - p_2} = 2^2 3^8 = 26244, \qquad \varepsilon = 587$
- $q_2 + 2q_6 = 132 > \lfloor \log_2 n \rfloor = 14$

An algorithm for the best left approximation

Consider the sequence $(f_n)_n = |\theta_n|_n$

Input: Two irrationals $0 < \alpha < 1$ and $0 < \beta \leq 1$
Output: The infinite sequence $(k_n\alpha - l_n)_{n\geq 0} < \beta$

1: $(k_0, l_0) := (0, 0)$
2: *while* true *do*
3: Compute n_i, c_i, e_i such that $\beta - (k_i\alpha - l_i) = c_i f_{n_i} + f_{n_i+1} + e_i$
4: *if* n_i is even *then*
5: $(k_{i+1}, l_{i+1}) := (k_i + q_{n_i}, l_i + p_{n_i})$
6: *else*
7: $(k_{i+1}, l_{i+1}) := (k_i - c_i q_{n_i} + q_{n_i+1}, l_i - c_i p_{n_i} + p_{n_i+1})$

Complexity analysis

For all $i \geq 0$, $0 < k_i\alpha - l_i < k_{i+1}\alpha - l_{i+1} < \beta$

For all $i \geq 0$, $k_{i+1} \geq k_i + c_i q_{n_i-1}$

$$\frac{\left(\frac{1+\sqrt{5}}{2}\right)^m}{\sqrt{5}} - \frac{1}{2} < \sum_{i=0}^{m} c_i q_{n_i-1} < u_m < \lfloor \log_2 n \rfloor < u_{m+1},$$

Thus, there exists a constant $C > 0$ such that

$$m < C \log\log n$$

Example

$n = 23832098195, \qquad \lfloor \log_3 n \rfloor = 21, \qquad \{\log_3 n\} = 0.7495\ldots$

i	$\beta - (k_i\alpha - l_i)$	n_i	c_i	e_i	k_{i+1}	l_{i+1}	$k_{i+1}\alpha - l_{i+1}$	$2^k 3^{21-l}$
0	0.7495	1	1	0.1186	1	0	0.6309	20920706406
1	0.1186	4	2	0.0114	9	5	0.6784	22039921152
2	0.0712	4	1	0.0114	17	10	0.7258	23219011584
3	0.0237	5	1	0.0009	63	39	0.7486	–

Example

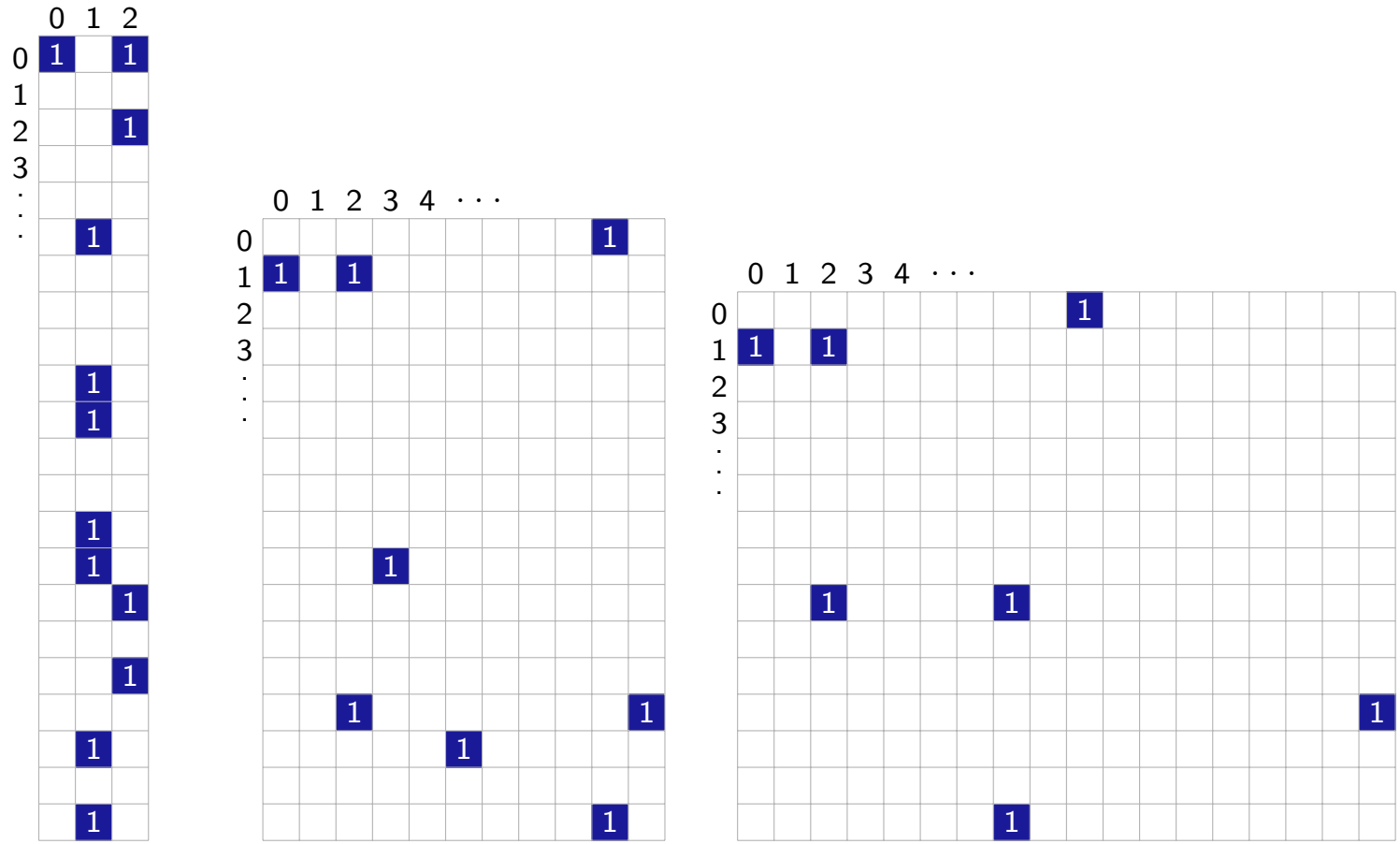
$n = 23832098195, \qquad \lfloor \log_3 n \rfloor = 21, \qquad \{\log_3 n\} = 0.7495\ldots$

i	$\beta - (k_i\alpha - l_i)$	n_i	c_i	e_i	k_{i+1}	l_{i+1}	$k_{i+1}\alpha - l_{i+1}$	$2^k 3^{21-l}$
0	0.7495	1	1	0.1186	1	0	0.6309	20920706406
1	0.1186	4	2	0.0114	9	5	0.6784	22039921152
2	0.0712	4	1	0.0114	17	10	0.7258	23219011584
3	0.0237	5	1	0.0009	63	39	0.7486	–

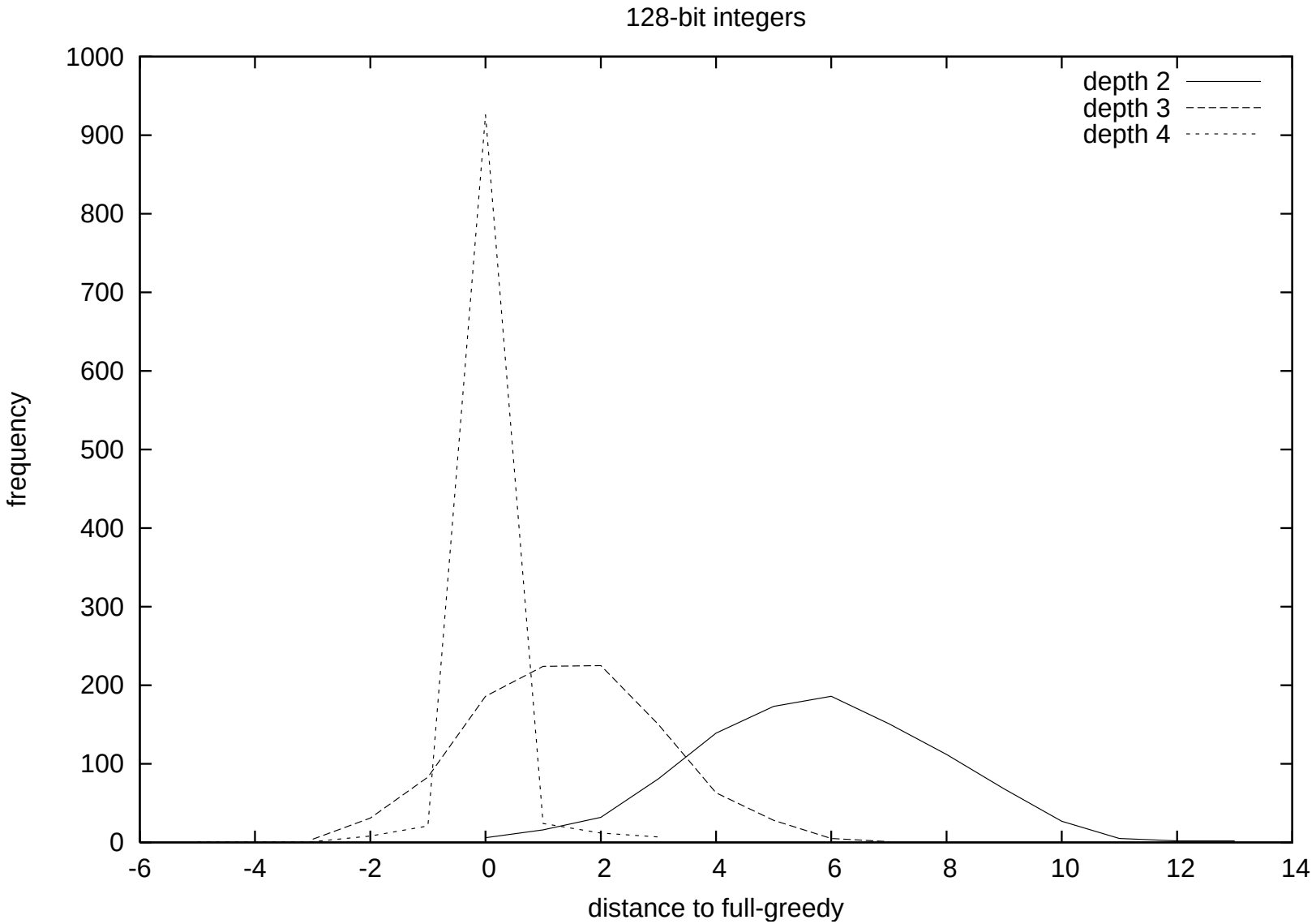
$n = 2^{17}3^{11} + 2^{7}3^{14} + 2^{7}3^{8} + 2^{2}3^{8} + 2^{9}3^{0} + 2^{2}3^{1} + 2^{0}3^{1}$

Approximate algorithms

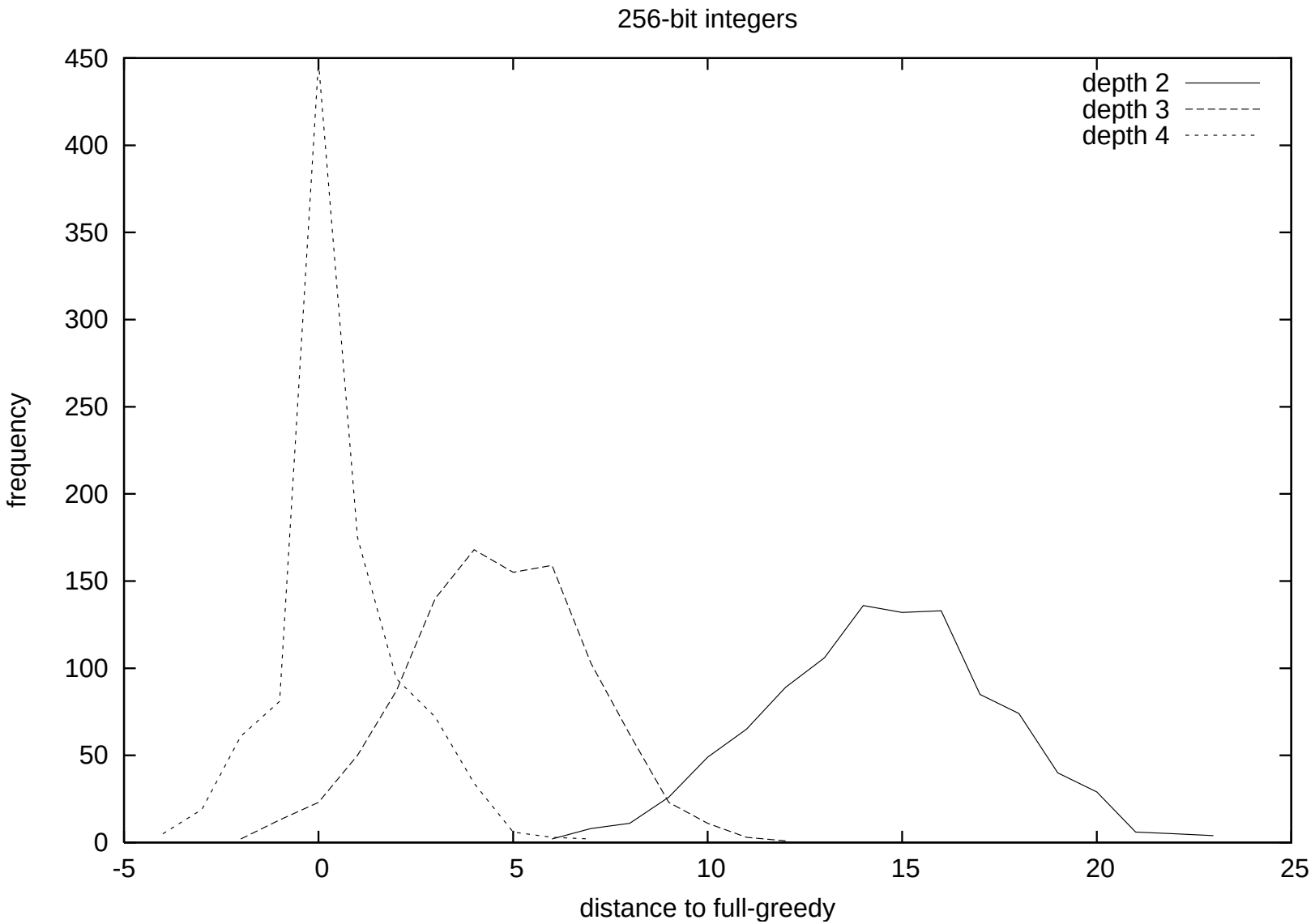
DBNS decompositions of $n = 23832098195$ at depths $1, 2, 3$



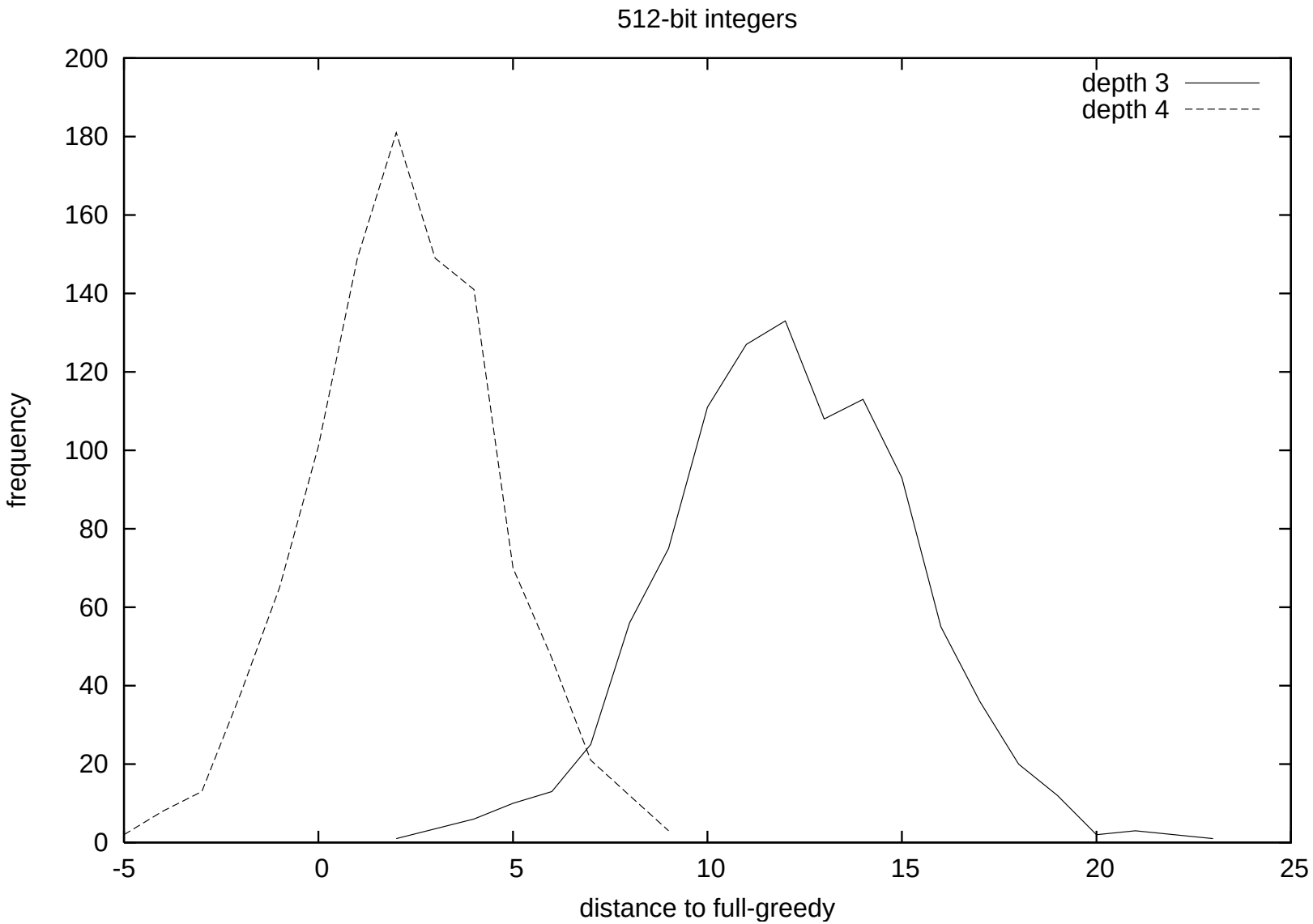
Length difference for 128-bit integers



Length difference for 256-bit integers



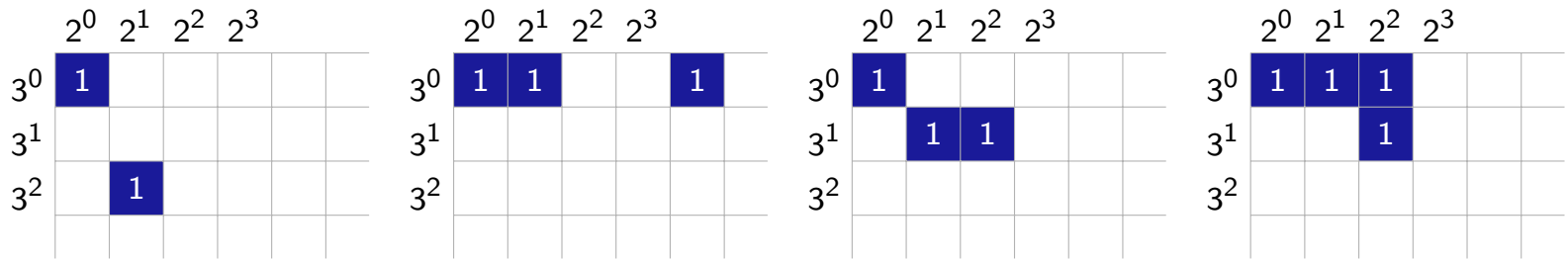
Length difference for 512-bit integers



$\{2,3\}$-partition chains

$$n = \sum_i 2^{a_i} 3^{b_i}, \qquad (a_i, b_i) \searrow$$

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



k-ary partitions: Euler

Chain partitions: Erdös, Loxton 79

Computing all $\{2,3\}$-partition chains

Basic relations:

$$\begin{aligned}
\Omega(n) &= \Omega^*(n) + {}^1\Omega^*(n-1) \\
\Omega^*(n) &= {}^2\Omega(n/2) \cup {}^3\Omega(n/3) \\
&= {}^2\big(\Omega(n/2) \setminus {}^3\Omega(n/6)\big) + {}^3\Omega(n/3) \\
\Omega(0) &= \{()\} \text{ ou } \Omega(1) = \{(1)\}
\end{aligned}$$

Computing all $\{2,3\}$-partition chains

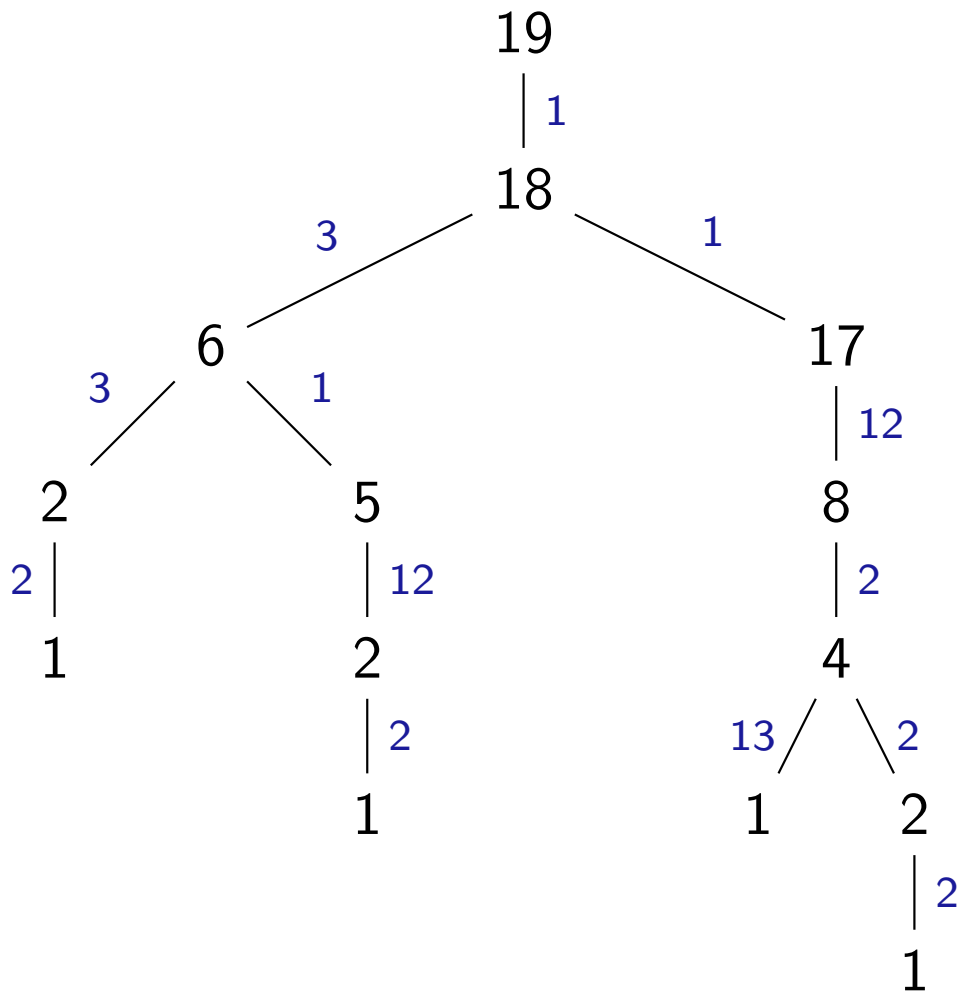
Basic relations:

$$\begin{aligned}
\Omega(n) &= \Omega^*(n) + {}^1\Omega^*(n-1) \\
\Omega^*(n) &= {}^2\Omega(n/2) \cup {}^3\Omega(n/3) \\
&= {}^2\big(\Omega(n/2) \setminus {}^3\Omega(n/6)\big) + {}^3\Omega(n/3) \\
\Omega(0) &= \{()\} \text{ ou } \Omega(1) = \{(1)\}
\end{aligned}$$

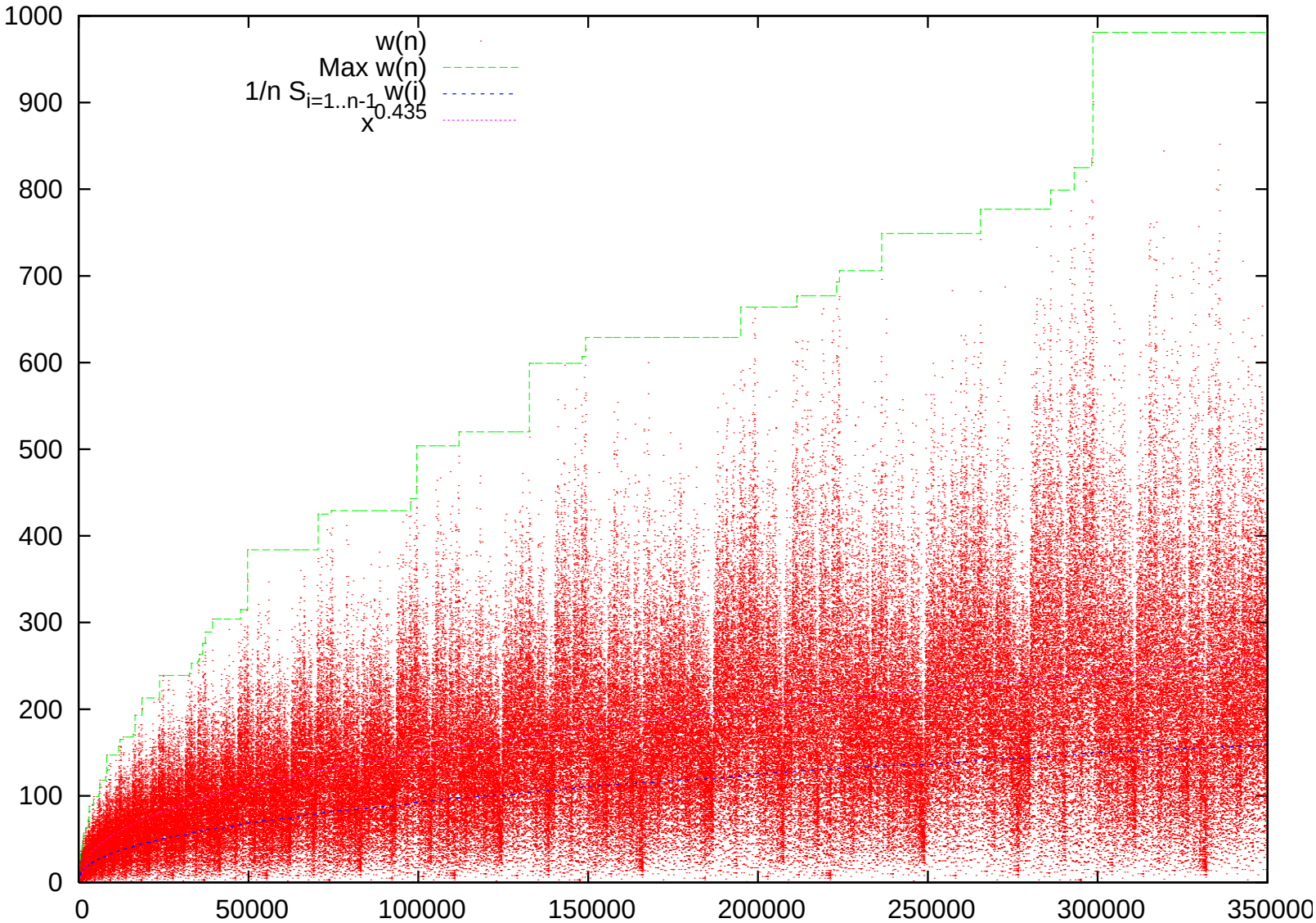
Better relations:

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

Representation of $\Omega(n)$ with a binary tree



Counting $\{2, 3\}$-partition chains



Generating $\{2,3\}$-partition chains at random

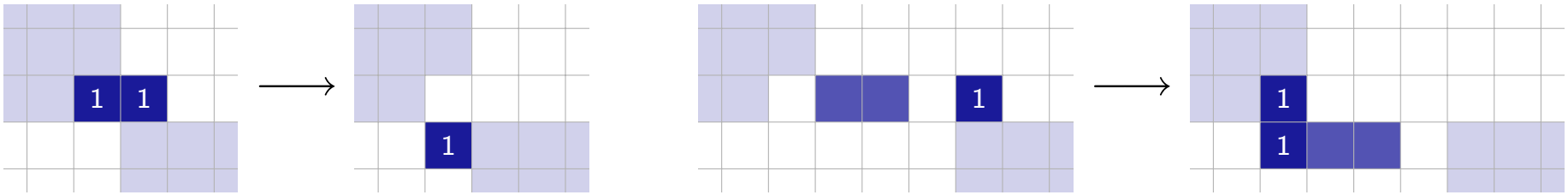
Transitions:

$$2+1=3$$

$$2(2^m-1+2^{m+1})=3(2^{m+1}-1)+1$$

b is fixed, *a* is maximal

going down



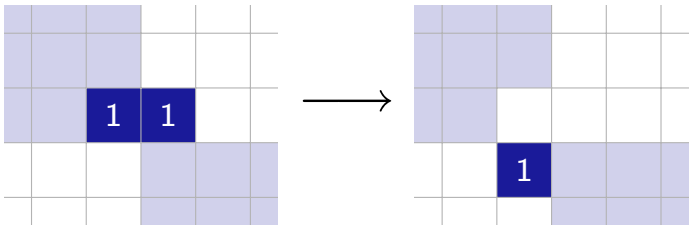
Generating $\{2, 3\}$-partition chains at random

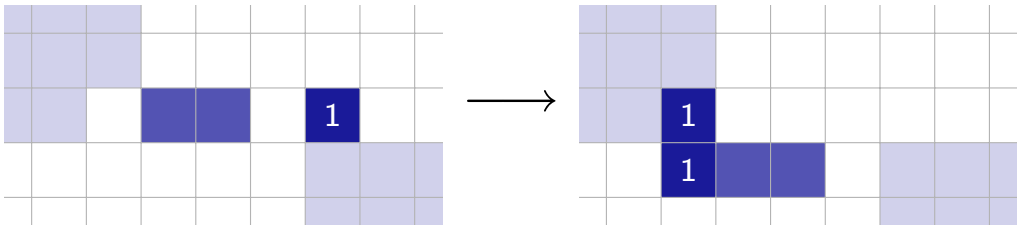
Transitions:

$$2 + 1 = 3$$

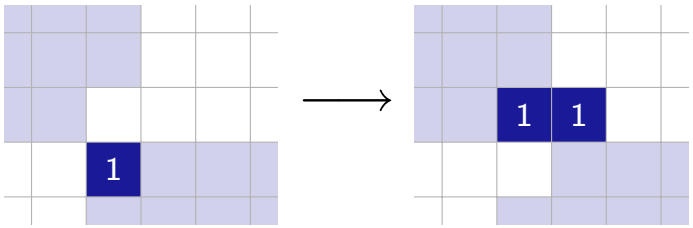
$$2(2^m - 1 + 2^{m+1}) = 3(2^{m+1} - 1) + 1$$

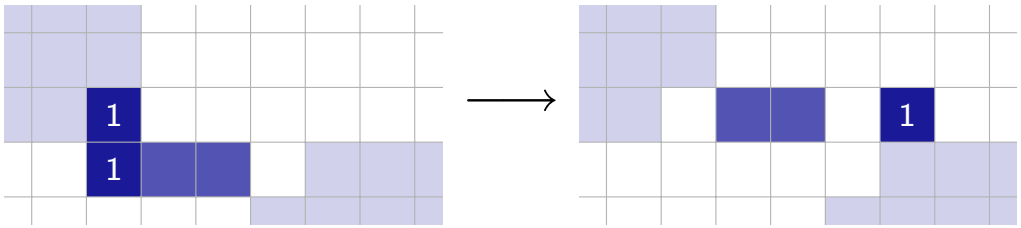
b is fixed, a is maximal — going down





b is fixed, a is minimal — going up





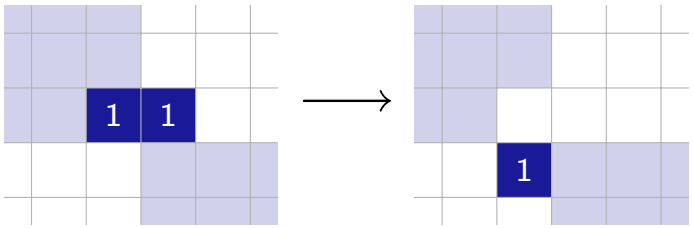
Generating $\{2,3\}$-partition chains at random

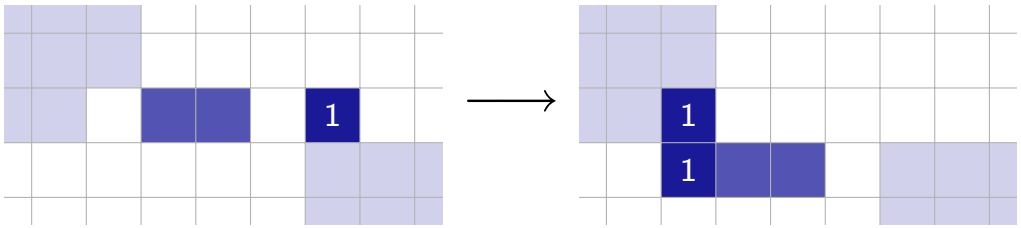
Transitions:

$$2+1=3$$

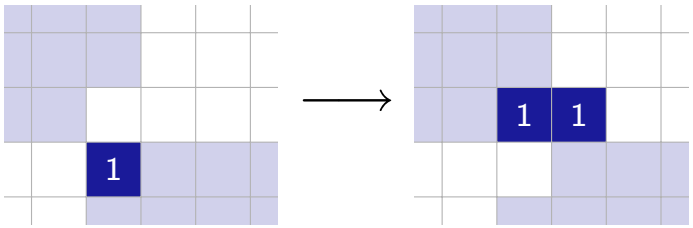
$$2(2^m-1+2^{m+1})=3(2^{m+1}-1)+1$$

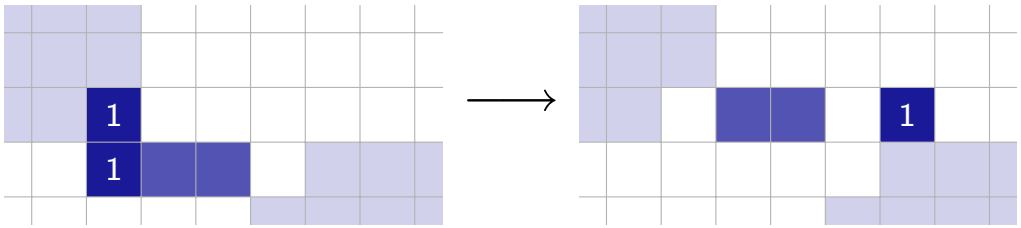
b is fixed, *a* is maximal — going down



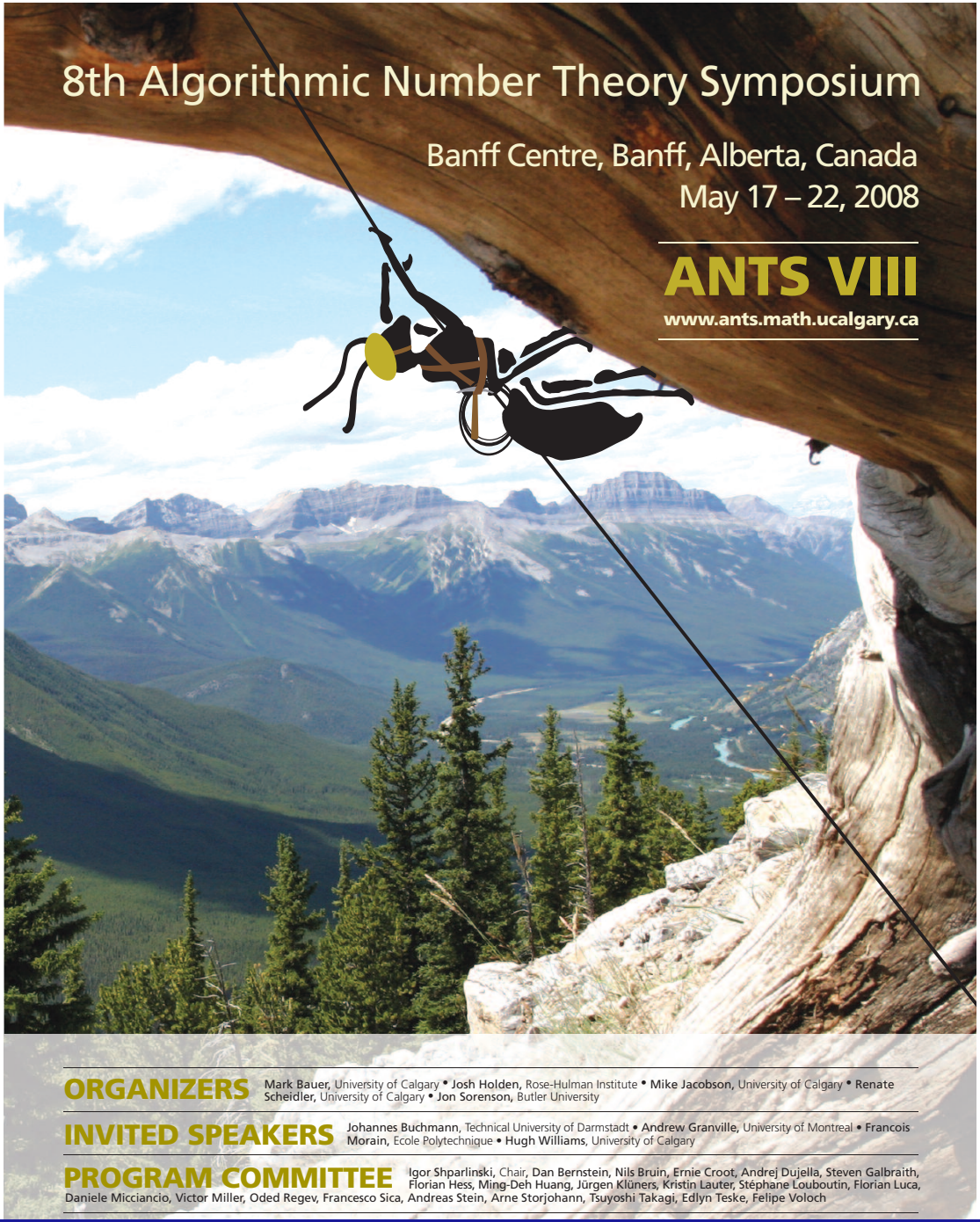


b is fixed, *a* is minimal — going up





Transition graph: symmetric & connected


8th Algorithmic Number Theory Symposium
Banff Centre, Banff, Alberta, Canada
May 17 – 22, 2008
ANTS VIII
www.ants.math.ucalgary.ca
ORGANIZERS
Mark Bauer, University of Calgary • Josh Holden, Rose-Hulman Institute • Mike Jacobson, University of Calgary • Renate Scheidler, University of Calgary • Jon Sorenson, Butler University
INVITED SPEAKERS
Johannes Buchmann, Technical University of Darmstadt • Andrew Granville, University of Montreal • Francois Morain, Ecole Polytechnique • Hugh Williams, University of Calgary
PROGRAM COMMITTEE
Igor Shparlinski, Chair, Dan Bernstein, Nils Bruin, Ernie Croot, Andrej Dujella, Steven Galbraith, Florian Hess, Ming-Deh Huang, Jürgen Klüners, Kristin Lauter, Stéphane Louboutin, Florian Luca, Daniele Micciancio, Victor Miller, Oded Regev, Francesco Sica, Andreas Stein, Arne Storjohann, Tsuyoshi Takagi, Edlyn Teske, Felipe Voloch