

Minimal weight expansions in Pisot numeration systems

Wolfgang Steiner

(joint work with Christiane Frougny and Peter J. Grabner)

Macquarie University, October 28, 2011

Double-and-add algorithm

For many applications, e.g. in elliptic curve cryptography, one has to compute (large) scalar multiples of group elements.

A simple way to compute mP is the **double-and-add algorithm** (Horner's scheme). Write $m \in \mathbb{N}$ in base 2,

$$\begin{aligned} m &= \sum_{k=0}^n x_k 2^k = x_n 2^n + x_{n-1} 2^{n-1} + \cdots + x_1 2^1 + x_0 2^0 \\ &= \langle x_n x_{n-1} \cdots x_0 \rangle_2, \end{aligned}$$

with $x_k \in \{0, 1\}$, and compute

$$mP = 2(\cdots 2(2(2x_n P + x_{n-1} P) + x_{n-2} P) + \cdots) + x_0 P.$$

Double-and-add algorithm

For many applications, e.g. in elliptic curve cryptography, one has to compute (large) scalar multiples of group elements.

A simple way to compute mP is the **double-and-add algorithm** (Horner's scheme). Write $m \in \mathbb{N}$ in base 2,

$$\begin{aligned} m &= \sum_{k=0}^n x_k 2^k = x_n 2^n + x_{n-1} 2^{n-1} + \cdots + x_1 2^1 + x_0 2^0 \\ &= \langle x_n x_{n-1} \cdots x_0 \rangle_2, \end{aligned}$$

with $x_k \in \{0, 1\}$, and compute

$$mP = 2(\cdots 2(2(2x_n P + x_{n-1} P) + x_{n-2} P) + \cdots) + x_0 P.$$

n duplications, $\sum_{k=0}^{n-1} x_k$ additions (in average $n/2$)

Signed expansions

In the case of elliptic curve cryptosystems, addition and subtraction are computed by the same formula. Writing

$$m = \sum_{k=0}^n x_k 2^k$$

with $x_k \in \{0, \pm 1\}$, yields mP with n duplications and

$$w(x_{n-1} \cdots x_0) = \sum_{k=0}^{n-1} |x_k|$$

additions/subtractions. w is called the absolute sum of digits or Hamming weight (if $x_k \in \{0, \pm 1\}$).

Representations of minimal weight

Taking digits in $\{0, \pm 1\}$ instead of $\{0, 1\}$ allows replacing blocks of the form $01 \cdots 11$ by $10 \cdots 0\bar{1}$ (where $\bar{1} = -1$), reducing the weight:

$$\langle 01^n \rangle_2 = 2^{n-1} + \cdots + 2 + 1 = 2^n - 1 = \langle 10^{n-1}\bar{1} \rangle_2$$

Representations of minimal weight

Taking digits in $\{0, \pm 1\}$ instead of $\{0, 1\}$ allows replacing blocks of the form $01 \cdots 11$ by $10 \cdots 0\bar{1}$ (where $\bar{1} = -1$), reducing the weight:

$$\langle 01^n \rangle_2 = 2^{n-1} + \cdots + 2 + 1 = 2^n - 1 = \langle 10^{n-1}\bar{1} \rangle_2$$

Instances of **minimal weight** representations are given by the **Non-Adjacent Form (NAF)**:

Every integer m can be represented uniquely as

$$m = \langle x_n x_{n-1} \cdots x_0 \rangle_2 \quad \text{with} \quad x_k \in \{0, \pm 1\}$$

and $x_k x_{k+1} = 0$ for all k , i.e., no two adjacent digits are non-zero.

Representations of minimal weight

Taking digits in $\{0, \pm 1\}$ instead of $\{0, 1\}$ allows replacing blocks of the form $01 \cdots 11$ by $10 \cdots 0\bar{1}$ (where $\bar{1} = -1$), reducing the weight:

$$\langle 01^n \rangle_2 = 2^{n-1} + \cdots + 2 + 1 = 2^n - 1 = \langle 10^{n-1}\bar{1} \rangle_2$$

Instances of **minimal weight** representations are given by the **Non-Adjacent Form (NAF)**:

Every integer m can be represented uniquely as

$$m = \langle x_n x_{n-1} \cdots x_0 \rangle_2 \quad \text{with} \quad x_k \in \{0, \pm 1\}$$

and $x_k x_{k+1} = 0$ for all k , i.e., no two adjacent digits are non-zero.

In average, $w(x_{n-1} \cdots x_0) \approx n/3$.

Applications of the NAF:

- ▶ Efficient arithmetic operations (Reitwiesner 1960)
- ▶ Coding Theory
- ▶ Elliptic Curve Cryptography (Morain and Olivos 1990)

Applications of the NAF:

- ▶ Efficient arithmetic operations (Reitwiesner 1960)
- ▶ Coding Theory
- ▶ Elliptic Curve Cryptography (Morain and Olivos 1990)

Other representations of minimal weight (Heuberger 2004):

$x_n x_{n-1} \cdots x_0 \in \{0, \pm 1\}^*$ is a representation of minimal weight (in base 2) if and only if contains no factor of the form

$$11(01)^*1, 1(0\bar{1})^*\bar{1}, \bar{1}\bar{1}(0\bar{1})^*\bar{1}, \bar{1}(01)^*1.$$

Fibonacci numeration system

Let $F_0 = 1$, $F_1 = 2$, $F_k = F_{k-1} + F_{k-2}$ for $k \geq 2$.

Theorem (Heuberger 2004)

“NAF”: Every $m \in \mathbb{Z}$ can be written as

$$m = \sum_{k=0}^n x_k F_k = \langle x_n x_{n-1} \cdots x_0 \rangle_F, \quad x_k \in \{0, \pm 1\},$$

with an F -expansion of minimal weight $x_n \cdots x_0$ avoiding

11 , $1\bar{1}$, $10\bar{1}$, 101 , 1001 , $\bar{1}\bar{1}$, $\bar{1}1$, $\bar{1}01$, $\bar{1}0\bar{1}$, $\bar{1}00\bar{1}$.

Fibonacci numeration system

Let $F_0 = 1$, $F_1 = 2$, $F_k = F_{k-1} + F_{k-2}$ for $k \geq 2$.

Theorem (Heuberger 2004)

“NAF”: Every $m \in \mathbb{Z}$ can be written as

$$m = \sum_{k=0}^n x_k F_k = \langle x_n x_{n-1} \cdots x_0 \rangle_F, \quad x_k \in \{0, \pm 1\},$$

with an F -expansion of minimal weight $x_n \cdots x_0$ avoiding

11 , $1\bar{1}$, $10\bar{1}$, 101 , 1001 , $\bar{1}\bar{1}$, $\bar{1}1$, $\bar{1}01$, $\bar{1}0\bar{1}$, $\bar{1}00\bar{1}$.

Theorem (Frougny–St 2008)

$x_n x_{n-1} \cdots x_0 \in \{0, \pm 1\}^*$ is an F -expansion of minimal weight if and only if it contains no factor of the form

$1(0100)^*1$, $1(0100)^*0101$, $1(00\bar{1}0)^*\bar{1}$, $1(00\bar{1}0)^*0\bar{1}$,
 $\bar{1}(0\bar{1}00)^*\bar{1}$, $\bar{1}(0\bar{1}00)^*0\bar{1}0\bar{1}$, $\bar{1}(0010)^*1$, or $\bar{1}(0010)^*01$.

Fibonacci numeration system

Let $F_0 = 1$, $F_1 = 2$, $F_k = F_{k-1} + F_{k-2}$ for $k \geq 2$.

Theorem (Heuberger 2004)

“NAF”: Every $m \in \mathbb{Z}$ can be written as

$$m = \sum_{k=0}^n x_k F_k = \langle x_n x_{n-1} \cdots x_0 \rangle_F, \quad x_k \in \{0, \pm 1\},$$

with an F -expansion of minimal weight $x_n \cdots x_0$ avoiding

11, $1\bar{1}$, $10\bar{1}$, 101, 1001, $\bar{1}\bar{1}$, $\bar{1}1$, $\bar{1}01$, $\bar{1}0\bar{1}$, $\bar{1}00\bar{1}$.

Theorem (Frougny–St 2008)

$x_n x_{n-1} \cdots x_0 \in \{0, \pm 1\}^*$ is an F -expansion of minimal weight if and only if it contains no factor of the form

$$1(0100)^*1, 1(0100)^*0101, 1(00\bar{1}0)^*\bar{1}, 1(00\bar{1}0)^*0\bar{1}, \\ \bar{1}(0\bar{1}00)^*\bar{1}, \bar{1}(0\bar{1}00)^*0\bar{1}0\bar{1}, \bar{1}(0010)^*1, \text{ or } \bar{1}(0010)^*01.$$

In average, $w(x_n \cdots x_0) \approx n/5$; $n \approx \log_{(1+\sqrt{5})/2} m \approx 1.44 \log_2 m$.

Fibonacci-and-add (Meloni 2007)

For $m = \sum_{k=0}^n x_k F_k$, $x_k \in \{0, \pm 1\}$, set $(Q_0, R_0) = (x_n P, x_n P)$ and

$$(Q_k, R_k) = (Q_{k-1} + R_{k-1} + x_{n-k} P, Q_{k-1} + x_{n-k} P)$$

for $1 \leq k \leq n$. Then

$$(Q_k, R_k) = \left(\sum_{j=0}^k x_{n-j} F_{k-j} P, \sum_{j=0}^k x_{n-j} F_{k-1-j} P \right),$$

with $F_{-1} = 1$, thus $Q_n = \sum_{j=0}^n x_{n-j} F_{n-j} P = mP$.

Fibonacci-and-add (Meloni 2007)

For $m = \sum_{k=0}^n x_k F_k$, $x_k \in \{0, \pm 1\}$, set $(Q_0, R_0) = (x_n P, x_n P)$ and

$$(Q_k, R_k) = (Q_{k-1} + R_{k-1} + x_{n-k} P, Q_{k-1} + x_{n-k} P)$$

for $1 \leq k \leq n$. Then

$$(Q_k, R_k) = \left(\sum_{j=0}^k x_{n-j} F_{k-j} P, \sum_{j=0}^k x_{n-j} F_{k-1-j} P \right),$$

with $F_{-1} = 1$, thus $Q_n = \sum_{j=0}^n x_{n-j} F_{n-j} P = mP$.

$n \approx 1.44 \log_2 m$ additions $Q_{k-1} + R_{k-1}$, $1 \leq k \leq n$,

$2 w(x_{n-1} \cdots x_0) \approx 0.576 \log_2 m$ additions/subtractions of P .

Fibonacci-and-add (Meloni 2007)

For $m = \sum_{k=0}^n x_k F_k$, $x_k \in \{0, \pm 1\}$, set $(Q_0, R_0) = (x_n P, x_n P)$ and

$$(Q_k, R_k) = (Q_{k-1} + R_{k-1} + x_{n-k} P, Q_{k-1} + x_{n-k} P)$$

for $1 \leq k \leq n$. Then

$$(Q_k, R_k) = \left(\sum_{j=0}^k x_{n-j} F_{k-j} P, \sum_{j=0}^k x_{n-j} F_{k-1-j} P \right),$$

with $F_{-1} = 1$, thus $Q_n = \sum_{j=0}^n x_{n-j} F_{n-j} P = mP$.

$n \approx 1.44 \log_2 m$ additions $Q_{k-1} + R_{k-1}$, $1 \leq k \leq n$,

$2 w(x_{n-1} \cdots x_0) \approx 0.576 \log_2 m$ additions/subtractions of P .

Other algorithm:

Calculate first $F_k P$, $0 \leq k \leq n$, then $mP = \sum_{k=0}^n x_k (F_k P)$.

Fibonacci-and-add (Meloni 2007)

For $m = \sum_{k=0}^n x_k F_k$, $x_k \in \{0, \pm 1\}$, set $(Q_0, R_0) = (x_n P, x_n P)$ and

$$(Q_k, R_k) = (Q_{k-1} + R_{k-1} + x_{n-k} P, Q_{k-1} + x_{n-k} P)$$

for $1 \leq k \leq n$. Then

$$(Q_k, R_k) = \left(\sum_{j=0}^k x_{n-j} F_{k-j} P, \sum_{j=0}^k x_{n-j} F_{k-1-j} P \right),$$

with $F_{-1} = 1$, thus $Q_n = \sum_{j=0}^n x_{n-j} F_{n-j} P = mP$.

$n \approx 1.44 \log_2 m$ additions $Q_{k-1} + R_{k-1}$, $1 \leq k \leq n$,

$2 w(x_{n-1} \cdots x_0) \approx 0.576 \log_2 m$ additions/subtractions of P .

Other algorithm:

Calculate first $F_k P$, $0 \leq k \leq n$, then $mP = \sum_{k=0}^n x_k (F_k P)$.

$n \approx 1.44 \log_2 m$ additions $F_{k-1} P + F_{k-2} P$, $1 \leq k \leq n$,

$w(x_n \cdots x_1) \approx 0.288 \log_2 m$ additions/subtractions of $F_k P$.

Weight of expansions

$m = \sum_{k=0}^n x_k U_k$, U_k sequence of increasing integers,
 $x_n x_{n-1} \cdots x_0$ U -expansion of minimal weight

$$U_k = \Theta(\beta^k) \Rightarrow n \sim \log_{\beta} m$$

U_k	x_k	n	expected weight $w(x_n \cdots x_0)$
2^k	$\{0, 1\}$	$\log_2 m$	$(\log_2 m)/2$
2^k	$\{0, \pm 1\}$	$\log_2 m$	$(\log_2 m)/3$
F_k	$\{0, 1\}$	$1.44 \log_2 m$	$2 (\log_{(1+\sqrt{5})/2} m) / (5 + \sqrt{5}) \approx 0.398 \log_2 m$
F_k	$\{0, \pm 1\}$	$1.44 \log_2 m$	$(\log_{(1+\sqrt{5})/2} m) / 5 \approx 0.288 \log_2 m$
S_k	$\{0, \pm 1\}$	$2.46 \log_2 m$	$(\log_{\beta} m) / (7 + 2\beta^2) \approx 0.235 \log_2 m$

$S_0 = 1$, $S_1 = 2$, $S_2 = 3$, $S_3 = 4$, $S_{k+3} = S_{k+1} + S_k$ for $k \geq 1$,
 $\beta \approx 1.325$ ($\beta^3 = \beta + 1$) is the smallest Pisot number

Redundancy automaton (in base 2)

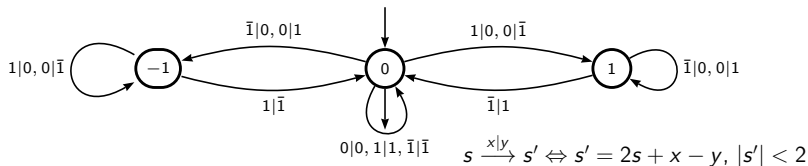
To find different representations of the same number, suppose that $\langle x_n \cdots x_0 \rangle_2 = \langle y_n \cdots y_0 \rangle_2$, and set $s_0 = 0$,

$$\begin{aligned} s_k &= \langle x_n \cdots x_{n-k+1} \rangle_2 - \langle y_n \cdots y_{n-k+1} \rangle_2 \\ &= \frac{\langle y_{n-k} \cdots y_0 \rangle_2 - \langle x_{n-k} \cdots x_0 \rangle_2}{2^{n-k+1}}. \end{aligned}$$

Then $s_{k+1} = 2s_k + x_{n-k} - y_{n-k}$, $|s_k| < 2$, and there exists a path

$$s_0 = 0 \xrightarrow{x_n|y_n} s_1 \xrightarrow{x_{n-1}|y_{n-1}} s_2 \cdots s_n \xrightarrow{x_0|y_0} s_{n+1} = 0$$

in the **redundancy automaton** (transducer)



Heavy words

$x_n x_{n-1} \cdots x_0 \in \{0, \pm 1\}^*$ is **heavy** if it is not a minimal weight representation of the corresponding number $\langle x_n \cdots x_0 \rangle_2$,

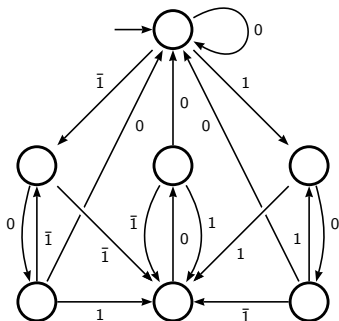
i.e., if there exists $y_{n+1} y_n \cdots y_0 \in \{0, \pm 1\}^*$ with

$$\langle x_n \cdots x_0 \rangle_2 = \langle y_{n+1} y_n \cdots y_0 \rangle_2 \text{ and } w(y_{n+1} \cdots y_0) < w(x_n \cdots x_0).$$

If $x_n \cdots x_0$ is heavy, but $x_{n-1} \cdots x_0$ and $x_n \cdots x_1$ are not heavy, then $x_n \cdots x_0$ is called **strictly heavy**.

Theorem

The set of expansions of minimal weight (in base 2) is recognised by the following automaton, where all states are terminal.



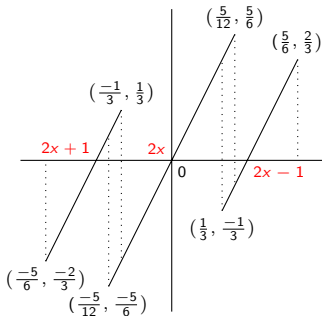
Theorem

For $x \in \left[-\frac{5}{6}, \frac{5}{6}\right) \cap \mathbb{Z}\left[\frac{1}{2}\right]$, all expansions of minimal weight are given by the following branching transformation.

$T : \left[-\frac{5}{6}, \frac{5}{6}\right) \rightarrow \left[-\frac{5}{6}, \frac{5}{6}\right)$, $x \mapsto 2x - d(x)$ with

$$d(x) = \begin{cases} -1 & \text{if } x \in \left[-\frac{5}{6}, -\frac{5}{12}\right) \\ -1 \text{ or } 0 & \text{if } x \in \left[-\frac{5}{12}, -\frac{1}{3}\right) \\ 0 & \text{if } x \in \left[-\frac{1}{3}, \frac{1}{3}\right) \\ 0 \text{ or } 1 & \text{if } x \in \left[\frac{1}{3}, \frac{5}{12}\right) \\ 1 & \text{if } x \in \left[\frac{5}{12}, \frac{5}{6}\right) \end{cases}$$

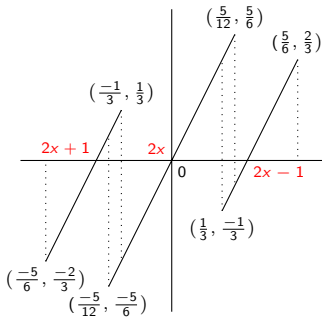
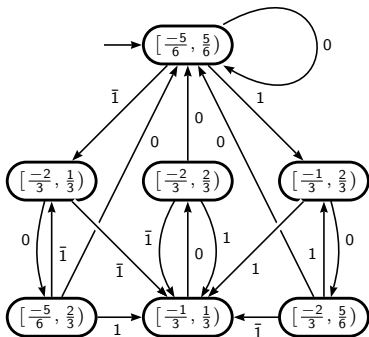
$$x = \frac{d(x)}{2^1} + \frac{d(T(x))}{2^2} + \frac{d(T^2(x))}{2^3} + \dots$$



Theorem

The set of expansions of minimal weight (in base 2) is recognised by the following automaton, where all states are terminal.

For $x \in [-\frac{5}{6}, \frac{5}{6}) \cap \mathbb{Z}[\frac{1}{2}]$, all expansions of minimal weight are given by the following branching transformation.



β -expansions, $\beta = \frac{1+\sqrt{5}}{2}$

Every $\xi \in \mathbb{R}$ can be written as

$$\xi = \sum_{k=-\infty}^n x_k \beta^k = \langle x_n \cdots x_0 \cdot x_{-1} x_{-2} \cdots \rangle_{\beta}$$

with $x_k \in \{0, \pm 1\}$.

A word $x_n x_{n-1} \cdots x_0 \in \{0, \pm 1\}^*$ is β -heavy if

$$\langle x_n \cdots x_0 \cdot \rangle_{\beta} = \langle y_l \cdots y_0 \cdot y_{-1} \cdots y_r \rangle_{\beta} \text{ and } w(y_l \cdots y_r) < w(x_n \cdots x_0)$$

for some $y_l \cdots y_r \in \{0, \pm 1\}^*$. If $x_n x_{n-1} \cdots x_0$ is β -heavy, $x_{n-1} \cdots x_0$ and $x_n \cdots x_1$ are not β -heavy, then $x_n \cdots x_0$ is **strictly β -heavy**.

β -expansions, $\beta = \frac{1+\sqrt{5}}{2}$

Every $\xi \in \mathbb{R}$ can be written as

$$\xi = \sum_{k=-\infty}^n x_k \beta^k = \langle x_n \cdots x_0 \cdot x_{-1} x_{-2} \cdots \rangle_{\beta}$$

with $x_k \in \{0, \pm 1\}$.

A word $x_n x_{n-1} \cdots x_0 \in \{0, \pm 1\}^*$ is β -heavy if

$$\langle x_n \cdots x_0 \cdot \rangle_{\beta} = \langle y_\ell \cdots y_0 \cdot y_{-1} \cdots y_r \rangle_{\beta} \text{ and } w(y_\ell \cdots y_r) < w(x_n \cdots x_0)$$

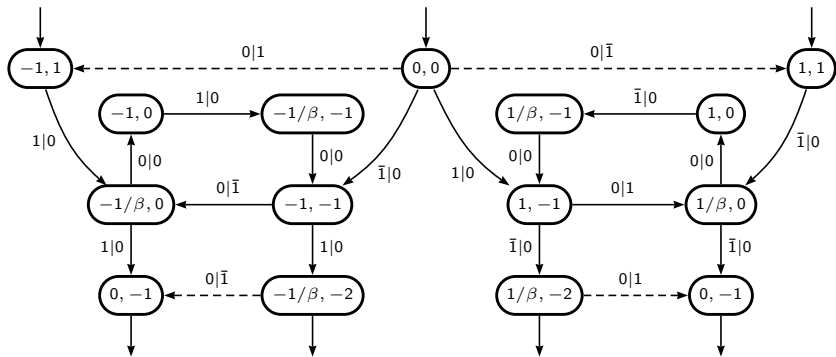
for some $y_\ell \cdots y_r \in \{0, \pm 1\}^*$. If $x_n x_{n-1} \cdots x_0$ is β -heavy, $x_{n-1} \cdots x_0$ and $x_n \cdots x_1$ are not β -heavy, then $x_n \cdots x_0$ is **strictly β -heavy**.

Theorem

If $\beta = \frac{1+\sqrt{5}}{2}$, then the set of strictly β -heavy words is

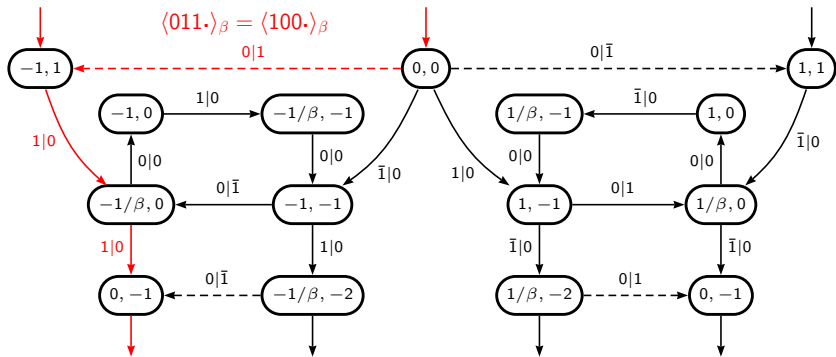
$$\begin{aligned} &1(0100)^*1 \cup 1(0100)^*0101 \cup 1(00\bar{1}0)^*\bar{1} \cup 1(00\bar{1}0)^*0\bar{1} \\ &\cup \bar{1}(0\bar{1}00)^*\bar{1} \cup \bar{1}(0\bar{1}00)^*0\bar{1}0\bar{1} \cup \bar{1}(0010)^*1 \cup \bar{1}(0010)^*01. \end{aligned}$$

The strictly β -heavy words are the inputs of the following transducer. The outputs are corresponding lighter words (if the path is completed by dashed arrows such that it runs from $(0, 0)$ to $(0, -1)$).



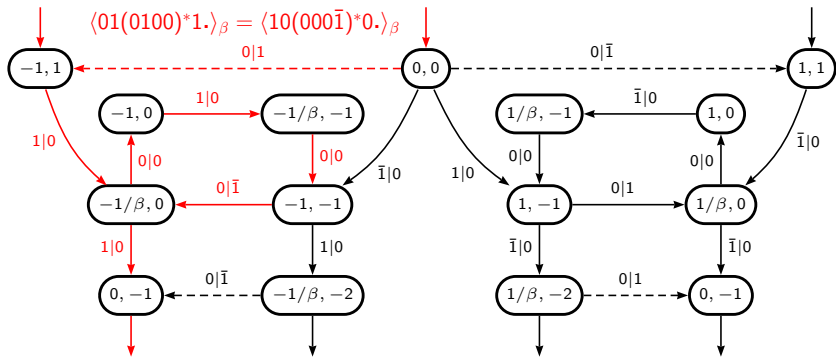
$$(s, \delta) \xrightarrow{x|y} (s', \delta') : s' = \beta s + x - y, \delta' = \delta + |y| - |x|$$

The strictly β -heavy words are the inputs of the following transducer. The outputs are corresponding lighter words (if the path is completed by dashed arrows such that it runs from $(0, 0)$ to $(0, -1)$).



$$(s, \delta) \xrightarrow{x|y} (s', \delta') : s' = \beta s + x - y, \delta' = \delta + |y| - |x|$$

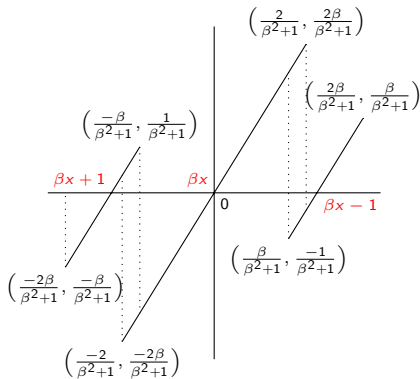
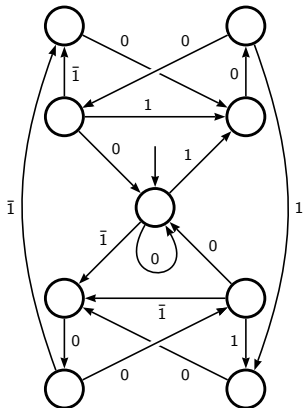
The strictly β -heavy words are the inputs of the following transducer. The outputs are corresponding lighter words (if the path is completed by dashed arrows such that it runs from $(0, 0)$ to $(0, -1)$).



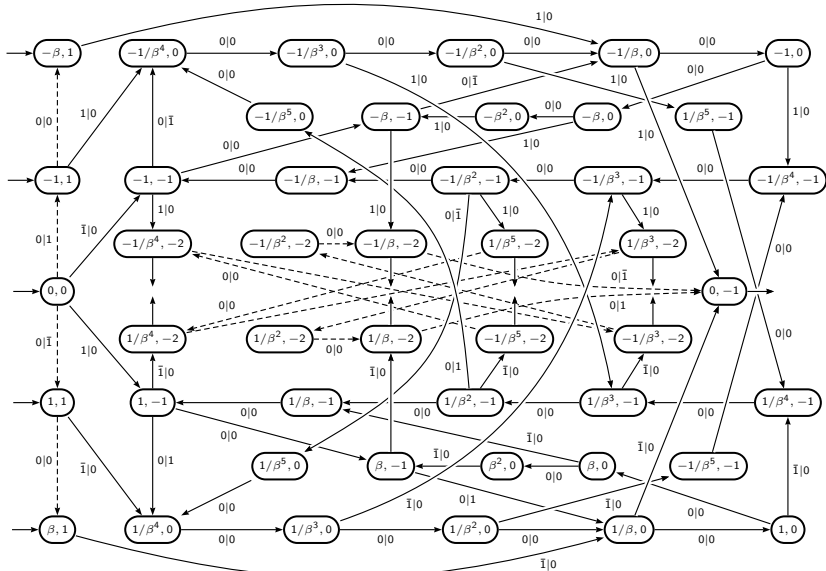
$$(s, \delta) \xrightarrow{x|y} (s', \delta') : s' = \beta s + x - y, \delta' = \delta + |y| - |x|$$

Theorem

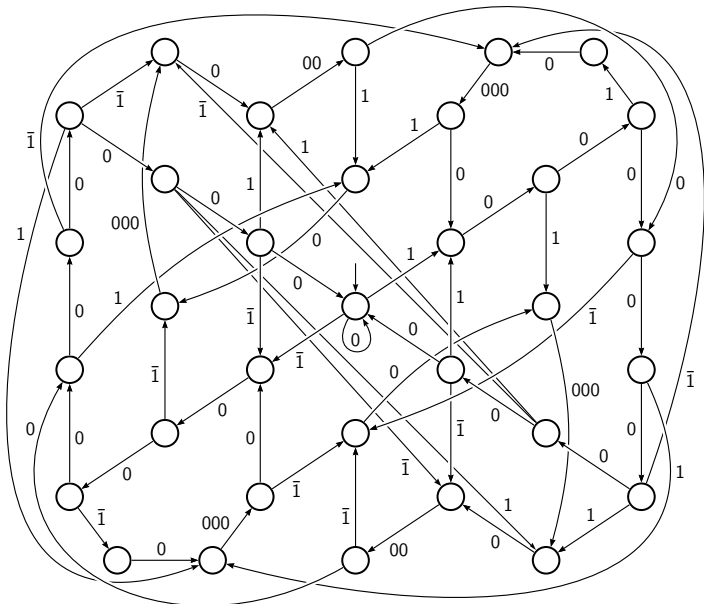
For $\beta = \frac{1+\sqrt{5}}{2}$, all signed β -expansions of minimal weight are given by the following automaton, where all states are terminal, and by the following branching transformation.



strictly (and some non-strictly) β -heavy words, $\beta^3 = \beta + 1$



β -expansions of minimal weight, $\beta^3 = \beta + 1$



“NAF”s: exclude factors $10^k 1, 10^k \bar{1}, 0 \leq k \leq 5$, and either $10^6 1$ or $10^6 \bar{1}$

General Pisot numeration systems

Theorem (Frougny–St 2008)

If β is a Pisot number, then the set of β -expansions of minimal weight is recognised by a finite automaton.

Theorem (Grabner–St 2011)

Let $U = (U_k)_{k \geq 0}$ be a strictly increasing sequence of integers with $U_0 = 1$, satisfying eventually a linear recurrence with characteristic polynomial equal to the minimal polynomial of a Pisot number.

Then the set of U -expansions of minimal weight is recognised by a finite automaton.

General Pisot numeration systems

Theorem (Frougny–St 2008)

If β is a Pisot number, then the set of β -expansions of minimal weight is recognised by a finite automaton.

Theorem (Grabner–St 2011)

Let $U = (U_k)_{k \geq 0}$ be a strictly increasing sequence of integers with $U_0 = 1$, satisfying eventually a linear recurrence with characteristic polynomial equal to the minimal polynomial of a Pisot number.

Then the set of U -expansions of minimal weight is recognised by a finite automaton.

We can choose a set G_U of U -expansions of minimal weight such that G_U is a regular language and every integer has exactly one representation in G_U . There exists a transducer that takes exactly the U -expansions of minimal weight as input and outputs the U -expansion in G_U representing the same number. (The set of U -expansions of minimal weight representing m is the set of inputs of the transducer with the expansion of m in G_U as output.)

Number of minimal weight expansions

Let $f_U(m)$ be the number of minimal weight U -expansions of m .

Theorem (Grabner–St 2011)

We have

$$\sum_{|m| < N} f_U(m) = N^{\log_\beta \alpha} \Phi(\log_\beta N) + \mathcal{O}(N^\lambda),$$

where α is the dominant eigenvalue of the automaton recognising the set of U -expansions of minimal weight, Φ is a continuous periodic function of period 1, and $\lambda < \log_\beta \alpha$.

Number of minimal weight expansions

Let $f_U(m)$ be the number of minimal weight U -expansions of m .

Theorem (Grabner–St 2011)

We have

$$\sum_{|m| < N} f_U(m) = N^{\log_\beta \alpha} \Phi(\log_\beta N) + \mathcal{O}(N^\lambda),$$

where α is the dominant eigenvalue of the automaton recognising the set of U -expansions of minimal weight, Φ is a continuous periodic function of period 1, and $\lambda < \log_\beta \alpha$.

Theorem (Grabner–Heuberger 2006)

If $U_k = 2^k$, then $f_U(m)$ is bounded by $F_{\lfloor \log_4 |m| \rfloor + 1}$;

Number of minimal weight expansions

Let $f_U(m)$ be the number of minimal weight U -expansions of m .

Theorem (Grabner–St 2011)

We have

$$\sum_{|m| < N} f_U(m) = N^{\log_\beta \alpha} \Phi(\log_\beta N) + \mathcal{O}(N^\lambda),$$

where α is the dominant eigenvalue of the automaton recognising the set of U -expansions of minimal weight, Φ is a continuous periodic function of period 1, and $\lambda < \log_\beta \alpha$.

Theorem (Grabner–Heuberger 2006)

If $U_k = 2^k$, then $f_U(m)$ is bounded by $F_{\lfloor \log_4 |m| \rfloor + 1}$; $\alpha \approx 2.17$
($\alpha^3 = \alpha^2 + 3\alpha - 1$), $\sum_{|m| < N} f_U(m) = \Theta(N^{\log_2 \alpha}) \approx \Theta(N^{1.11775})$.

Number of minimal weight expansions

Let $f_U(m)$ be the number of minimal weight U -expansions of m .

Theorem (Grabner–St 2011)

We have

$$\sum_{|m| < N} f_U(m) = N^{\log_\beta \alpha} \Phi(\log_\beta N) + \mathcal{O}(N^\lambda),$$

where α is the dominant eigenvalue of the automaton recognising the set of U -expansions of minimal weight, Φ is a continuous periodic function of period 1, and $\lambda < \log_\beta \alpha$.

Theorem (Grabner–Heuberger 2006)

If $U_k = 2^k$, then $f_U(m)$ is bounded by $F_{\lfloor \log_4 |m| \rfloor + 1}$; $\alpha \approx 2.17$
($\alpha^3 = \alpha^2 + 3\alpha - 1$), $\sum_{|m| < N} f_U(m) = \Theta(N^{\log_2 \alpha}) \approx \Theta(N^{1.11775})$.

Theorem (Grabner–St 2011)

The number of minimal weight F -expansions of m with digits in $\{0, \pm 1\}$ is bounded by (approximately) $2^{\lfloor (\log_\beta |m|)/3 \rfloor}$, $\beta = \frac{1+\sqrt{5}}{2}$.
We have $\alpha \approx 1.74$ ($\alpha^5 = \alpha^4 + 2\alpha^2 + \alpha - 1$), $\log_\beta \alpha \approx 1.15188$.