β-expansions of minimal weight

Wolfgang Steiner
(joint work with Christiane Frougny)

LIAFA (CNRS, Université Paris 7)

LIAFA, October 5, 2007

Diffie-Hellman scheme

The Diffie-Hellman encryption scheme allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel.

party	secret (integers)	public
A	m_A, r_A	P, $P_A = m_A P$, $r_A P$
B	m_B, r_B	P, $P_B = m_B P$, $r_B P$

A message is coded by an element x of a group (e.g. elliptic curve). For sending the message to B, it is encoded by

$$y = x + r_A P_B.$$

A sends $r_A P$ and y to B, who recovers x by

$$x = y - m_B r_A P = x + r_A m_B P - m_B r_A P.$$

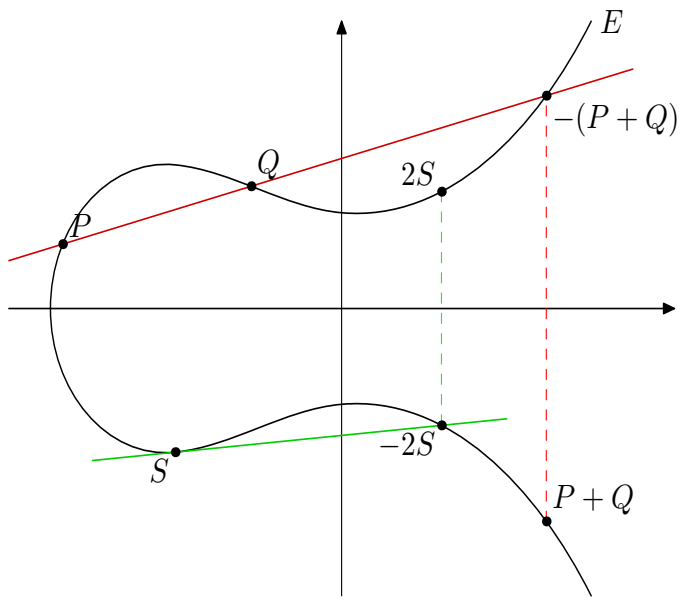
The security of this system is based on the assumption that r_A is very hard to find given $(P, r_A P)$ (Discrete Logarithm Problem).

Elliptic curves

An equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with coefficients in a field K defines an elliptic curve over K. The set of solutions (plus a point at "infinity") carries a group law by the secant-tangent-rule.



Addition is costly, subtraction is similar to addition.

Double-and-add algorithm

The Diffie-Hellman scheme is based on the computation of (large) scalar multiples of group elements. It is therefore interesting to find algorithms for the fast computation of multiples.
One simple way to compute mP is the double-and-add algorithm (Horner's scheme). Write m in base 2,

$$m = \sum_{k=1}^{n} x_k 2^{n-k} = x_1 2^{n-1} + \cdots + x_{n-1} 2^1 + x_n 2^0 = x_1 \cdots x_{n-1} x_n \text{.} ,$$

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

$$mP = 2(\cdots 2(2(2x_1 P + x_2 P) + x_3 P) + \cdots) + x_n P.$$

Weight

In the case of elliptic curve cryptosystems, the additional property that addition and subtraction can be computed by the same formula can be used to speed up this algorithm: Writing

$$m = \sum_{k=1}^{n} x_k 2^{n-k}$$

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

$$h(x_1 \cdots x_n) = \sum_{k=1}^{n} |x_k|$$

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

Representations of minimal weight

For speeding up the computation of multiples, we can use representations of integers which minimize the weight function h.

The weight of a representation can be reduced by replacing blocks of the form $01\cdots11$ by $10\cdots0\bar{1}$ (where $\bar{1} = -1$)

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

One instance of a minimal weight representation is the Non-Adjacent-Form (NAF):
Every integer m can be represented uniquely in the form

$$m = \sum_{k=1}^{n} x_k 2^{n-k} = x_1 \cdots x_n. \quad \text{with} \quad x_k \in \{0, \pm 1\}$$

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

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): $x_1 \cdots x_n \in \{0, \pm 1\}^*$ is a representation of minimal weight (in base 2) if and only if contains none of the factors

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

Joint digit expansions: Solinas; Grabner, Heuberger, Prodinger

Redundancy automaton

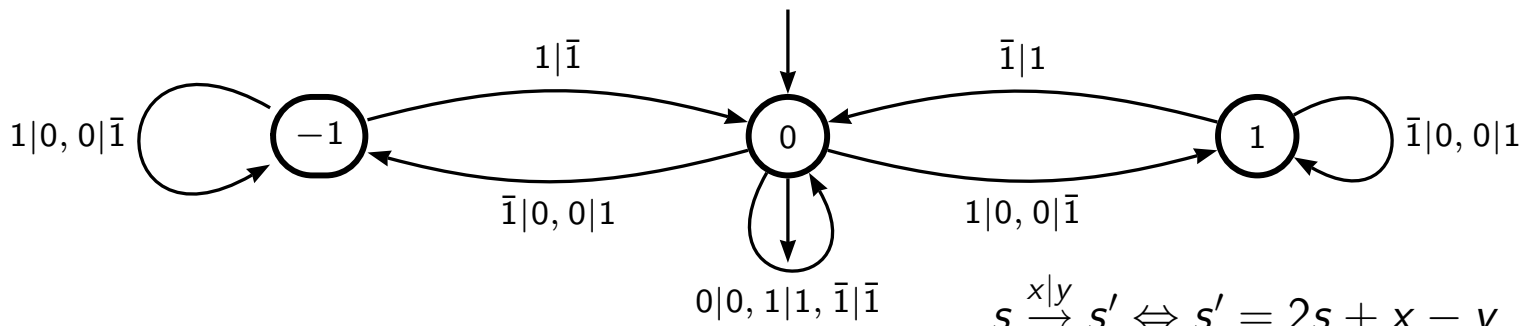
To find different representations of the same number, suppose that $x_1 \cdots x_n\cdot = y_1 \cdots y_n\cdot$, and set $s_0 = 0$,

$$s_k = x_1 \cdots x_k\cdot - y_1 \cdots y_k\cdot = \cdot y_{k+1} \cdots y_n - \cdot x_{k+1} \cdots x_n,$$
$$\text{i.e., } s_{k+1} = x_1 \cdots x_k x_{k+1}\cdot - y_1 \cdots y_k y_{k+1}\cdot = 2s_k + x_{k+1} - y_{k+1}.$$

Then $|s_k| < 2$ and there exists a path

$$s_0 = 0 \overset{x_1|y_1}{\to} s_1 \overset{x_2|y_2}{\to} s_2 \ \cdots \ s_{n-1} \overset{x_n|y_n}{\to} s_n = 0$$

in the redundancy automaton (transducer)



$s \overset{x|y}{\to} s' \Leftrightarrow s' = 2s + x - y,\ |s'| < 2$

Redundancy automaton

To find different representations of the same number, suppose that $x_1 \cdots x_n\boldsymbol{.} = y_1 \cdots y_n\boldsymbol{.}$, and set $s_0 = 0$,

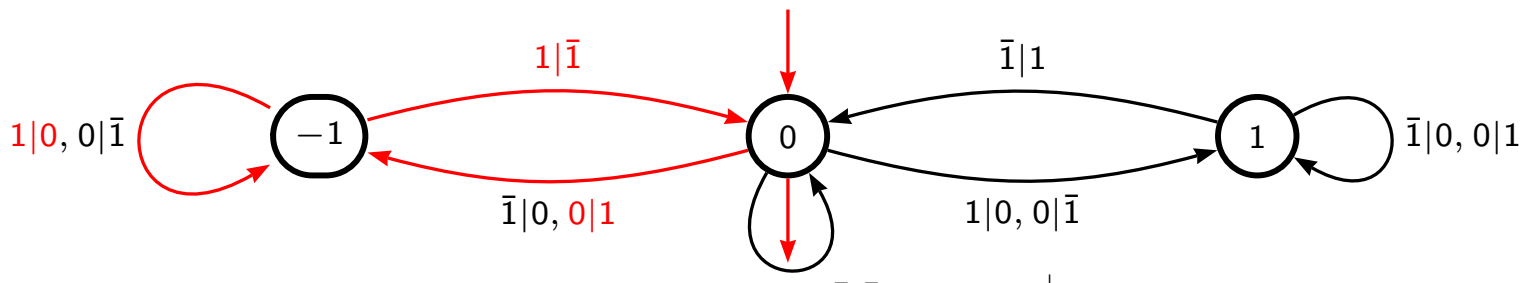
$$s_k = x_1 \cdots x_k\boldsymbol{.} - y_1 \cdots y_k\boldsymbol{.} = \boldsymbol{.}y_{k+1} \cdots y_n - \boldsymbol{.}x_{k+1} \cdots x_n,$$

$$\text{i.e., } s_{k+1} = x_1 \cdots x_k x_{k+1}\boldsymbol{.} - y_1 \cdots y_k y_{k+1}\boldsymbol{.} = 2s_k + x_{k+1} - y_{k+1}.$$

Then $|s_k| < 2$ and there exists a path

$$s_0 = 0 \overset{x_1|y_1}{\to} s_1 \overset{x_2|y_2}{\to} s_2 \ \cdots \ s_{n-1} \overset{x_n|y_n}{\to} s_n = 0$$

in the redundancy automaton (transducer)



$01 \cdots 11\boldsymbol{.} = 10 \cdots 0\bar{1}\boldsymbol{.}$

$s \overset{x|y}{\to} s' \Leftrightarrow s' = 2s + x - y,\ |s'| < 2$

Heavy words

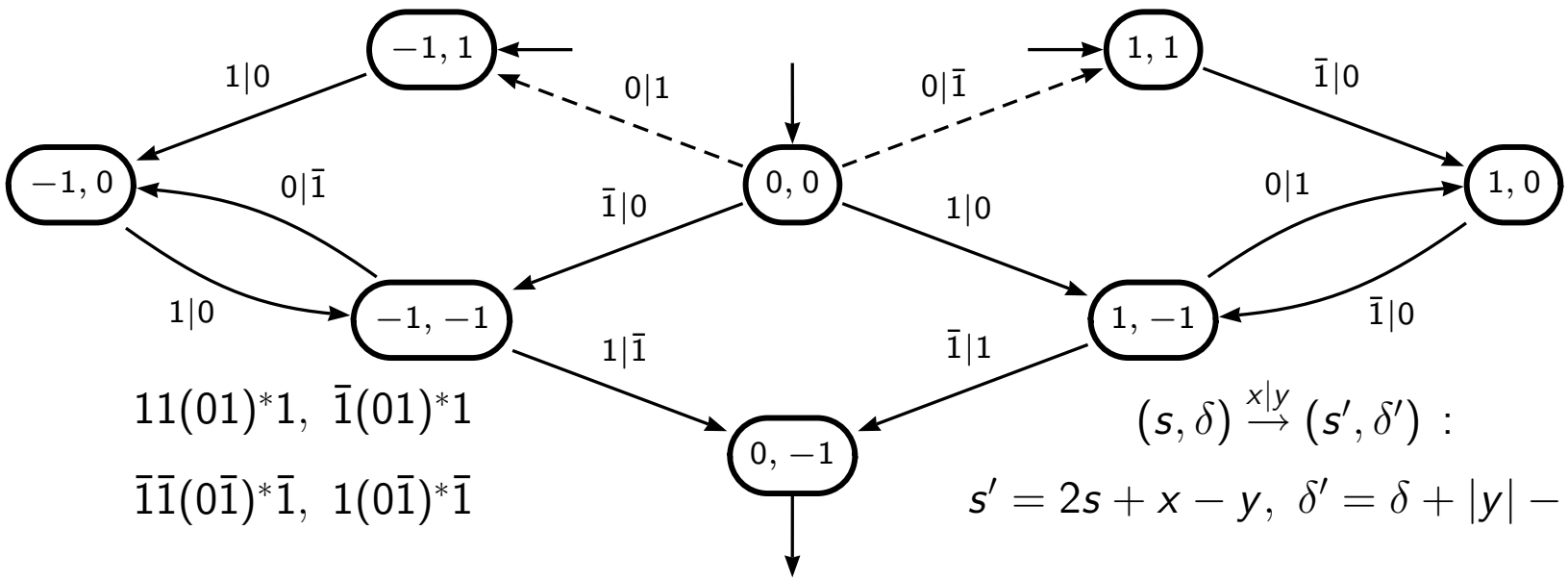
$x_1 \cdots x_n \in \{0, \pm 1\}^*$ is heavy if it is not minimal in weight, i.e., if there exists $y_0 y_1 \cdots y_n \in \{0, \pm 1\}^*$ with

$$x_1 \cdots x_n \bullet = y_0 y_1 \cdots y_n \bullet \quad \text{and} \quad h(y_0 \cdots y_n) < h(x_1 \cdots x_n)$$

If $x_1 \cdots x_{n-1}$ and $x_2 \cdots x_n$ are not heavy, then x is strictly heavy.

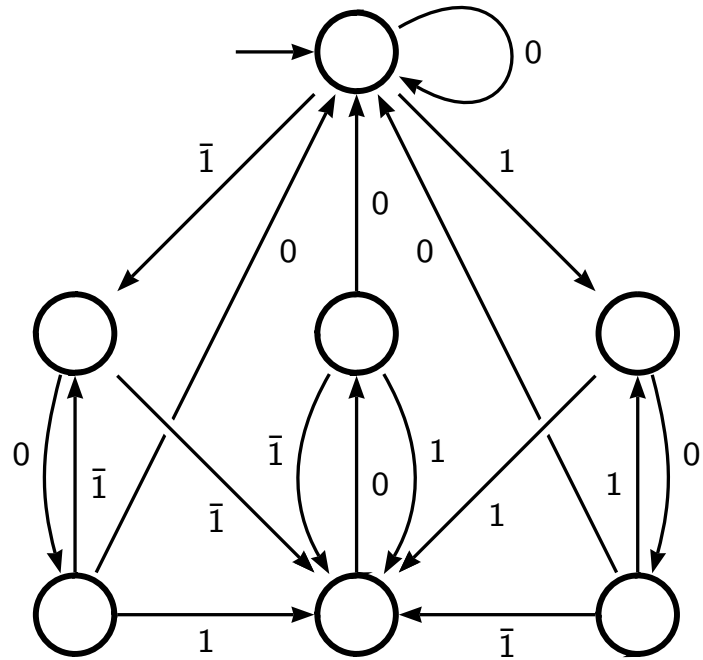
Theorem (cf. Heuberger 2004)

The strictly heavy words (in base 2) are inputs of the transducer



Theorem

All expansions of minimal weight (in base 2) are recognized by the following automaton, where all states are terminal.



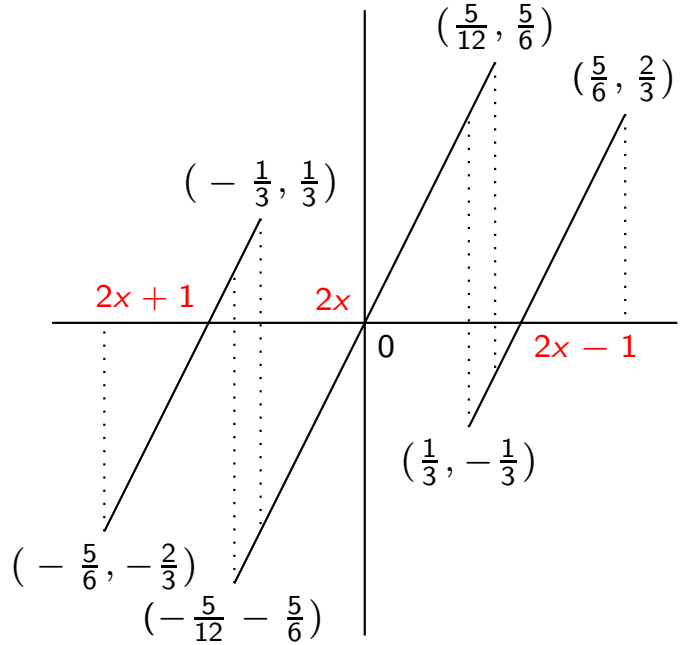
Theorem

For $x \in [-5/6, 5/6)$ with finite binary expansion, all expansions of minimal weight are given by the following branching transformation.

$T : [-5/6, 5/6) \to [-5/6, 5/6)$,
$T(x) = 2x - d(x)$ with

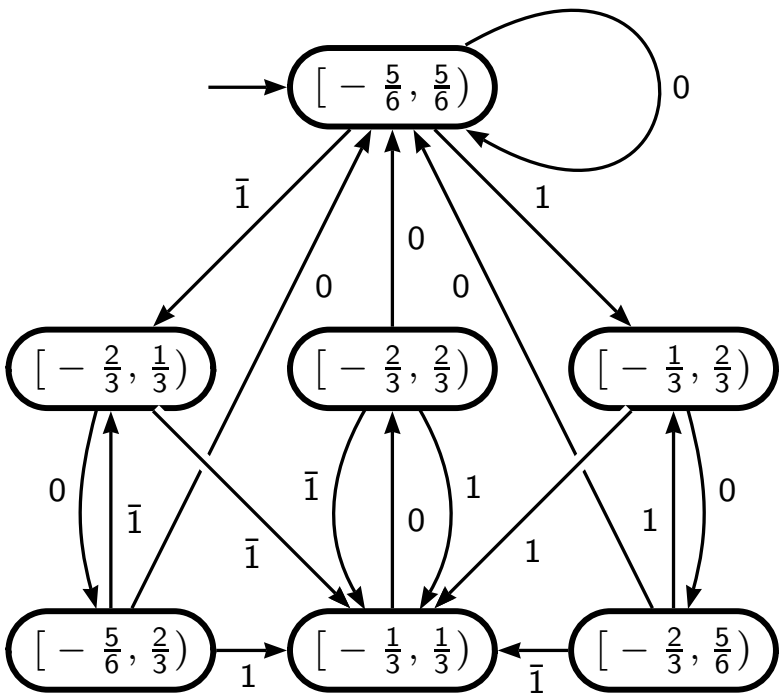
$$d(x) = \begin{cases} -1 & \text{if } x \in [-\frac{5}{6}, -\frac{5}{12}) \\ -1 \text{ or } 0 & \text{if } x \in [-\frac{5}{12}, -\frac{1}{3}) \\ 0 & \text{if } x \in [-\frac{1}{3}, \frac{1}{3}) \\ 0 \text{ or } 1 & \text{if } x \in [\frac{1}{3}, \frac{5}{12}) \\ 1 & \text{if } x \in [\frac{5}{12},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

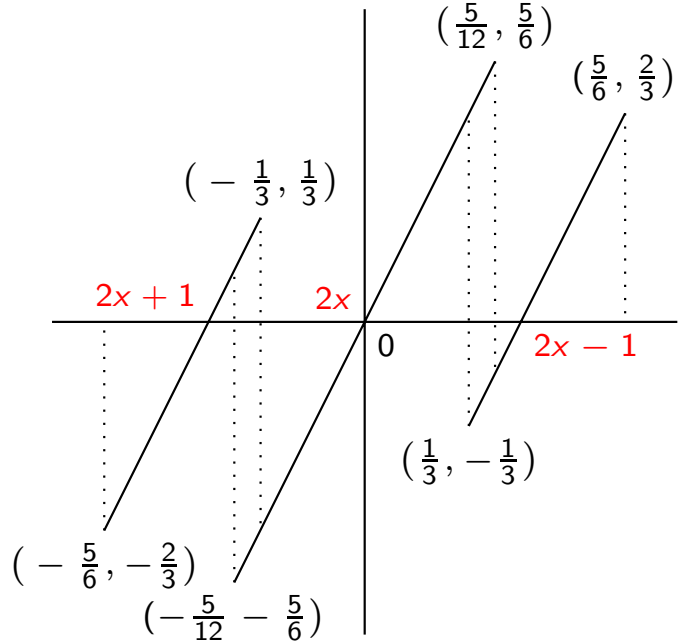
$x = .d(x)d(T(x))d(T^2(x))\cdots$



Theorem

All expansions of minimal weight (in base 2) are recognized by the following automaton, where all states are terminal.
For $x \in [-5/6, 5/6)$ with finite binary expansion, all expansions of minimal weight are given by the following branching transformation.





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

Greedy β-expansions: Every $x \in \mathbb{R}^+$ has a unique expansion

$$x = \sum_{k \in \mathbb{Z}} x_k \beta^{-k} = \cdots x_{-1} x_0 . x_1 x_2 \cdots$$

with $x_k \in \{0, 1\}$ and $x_k x_{k+1} = 0$, which does not terminate with $(10)^\omega = 101010 \cdots$.

$$\beta^2 = \beta + 1, \ 100. = 011., \ 1. = .11$$

Greedy β-expansions are not minimal in weight for $x_k \in \{0, \pm 1\}$:

$$0101001. = 10\bar{1}1001. = 1000\bar{1}01. = 10000\bar{1}0.$$

β-expansions of minimal weight

$x_1 \cdots x_n \in \{0, \pm 1\}^*$ is β-heavy if it is not minimal in weight, i.e., if there exists $y_\ell \cdots y_r \in \{0, \pm 1\}^*$ with

$$\cdot x_1 \cdots x_n = y_\ell \cdots y_0 \cdot y_1 \cdots y_r \quad \text{and} \quad h(y_\ell \cdots y_r) < h(x_1 \cdots x_n).$$

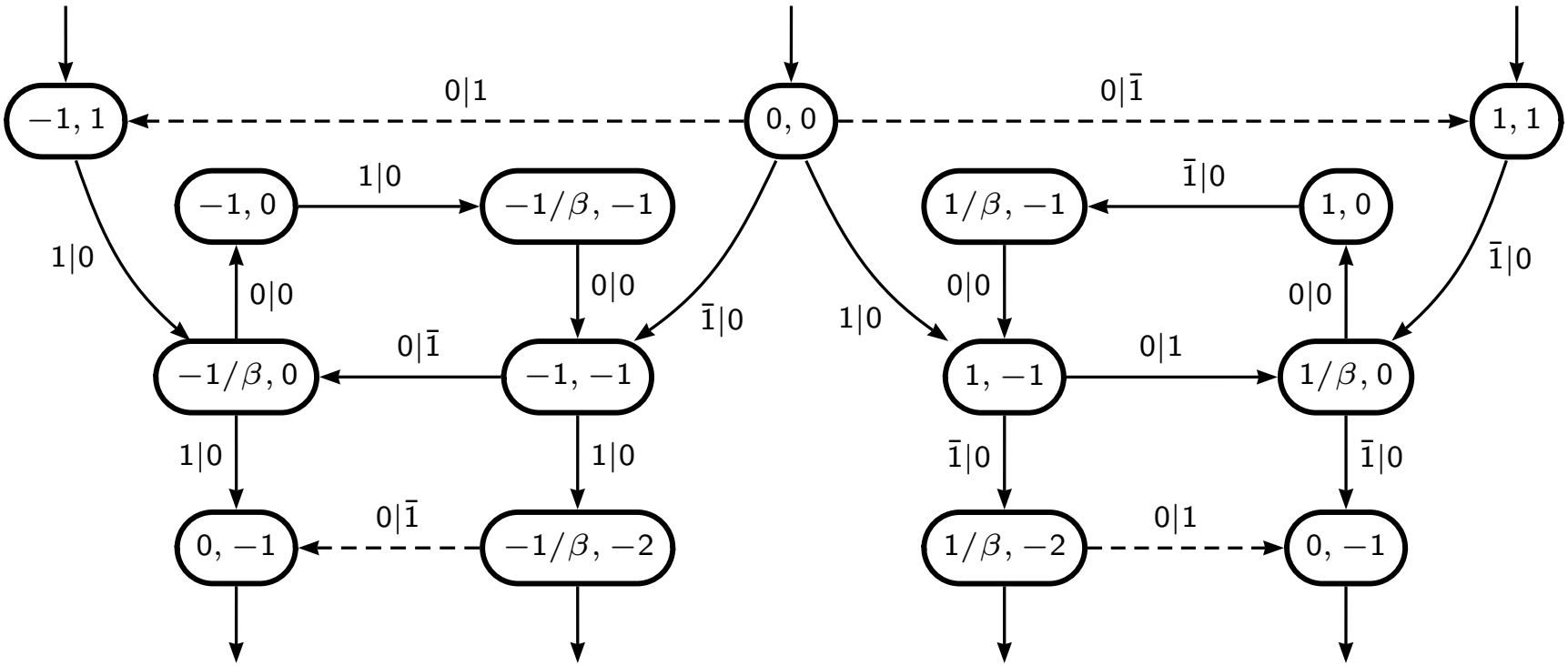
If $x_1 \cdots x_{n-1}$ and $x_2 \cdots x_n$ are not β-heavy, $x_1 \cdots x_n$ is strictly β-heavy.

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

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

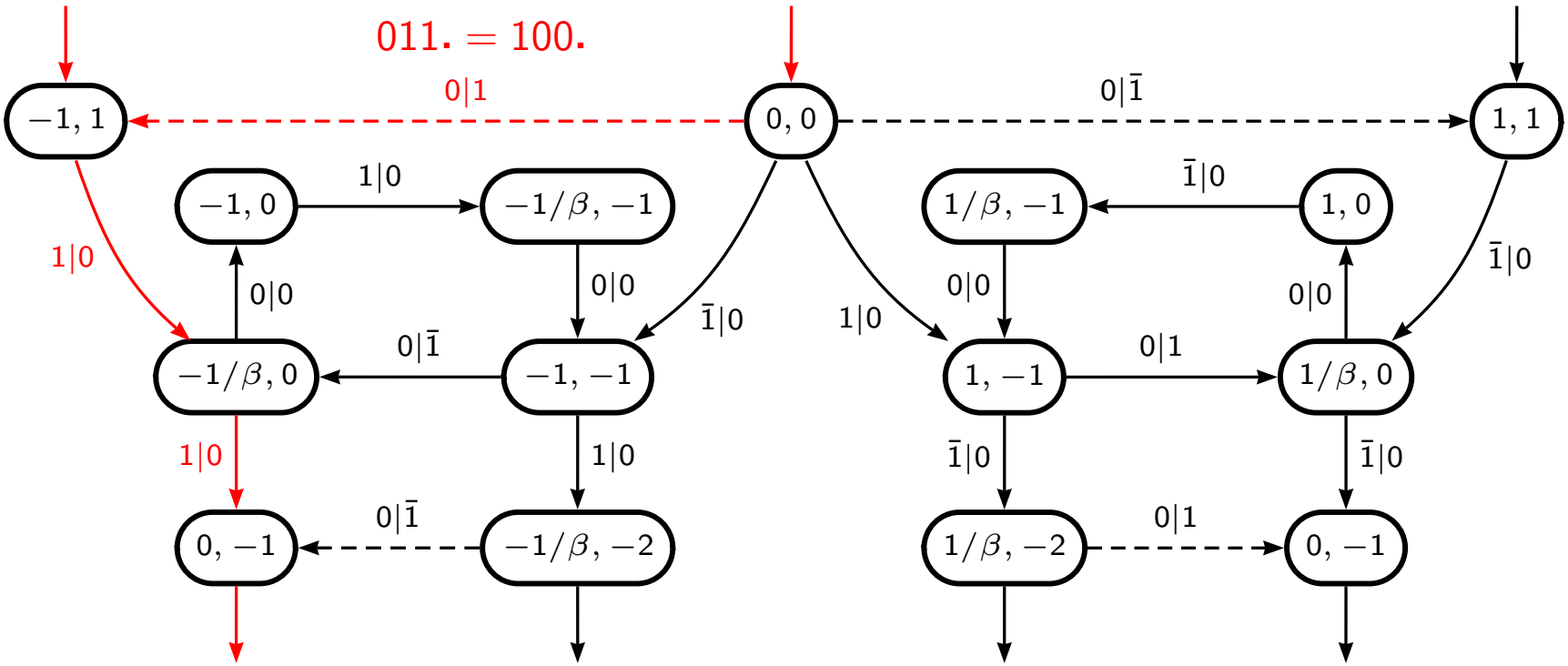
If $\cdots \epsilon_{-1}\epsilon_0\epsilon_1 \cdots$ does not contain any of these factors, then $\cdots \epsilon_{-1}\epsilon_0 \cdot \epsilon_1 \cdots$ is a signed β-expansion of minimal weight.

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 $(0,-1)$).



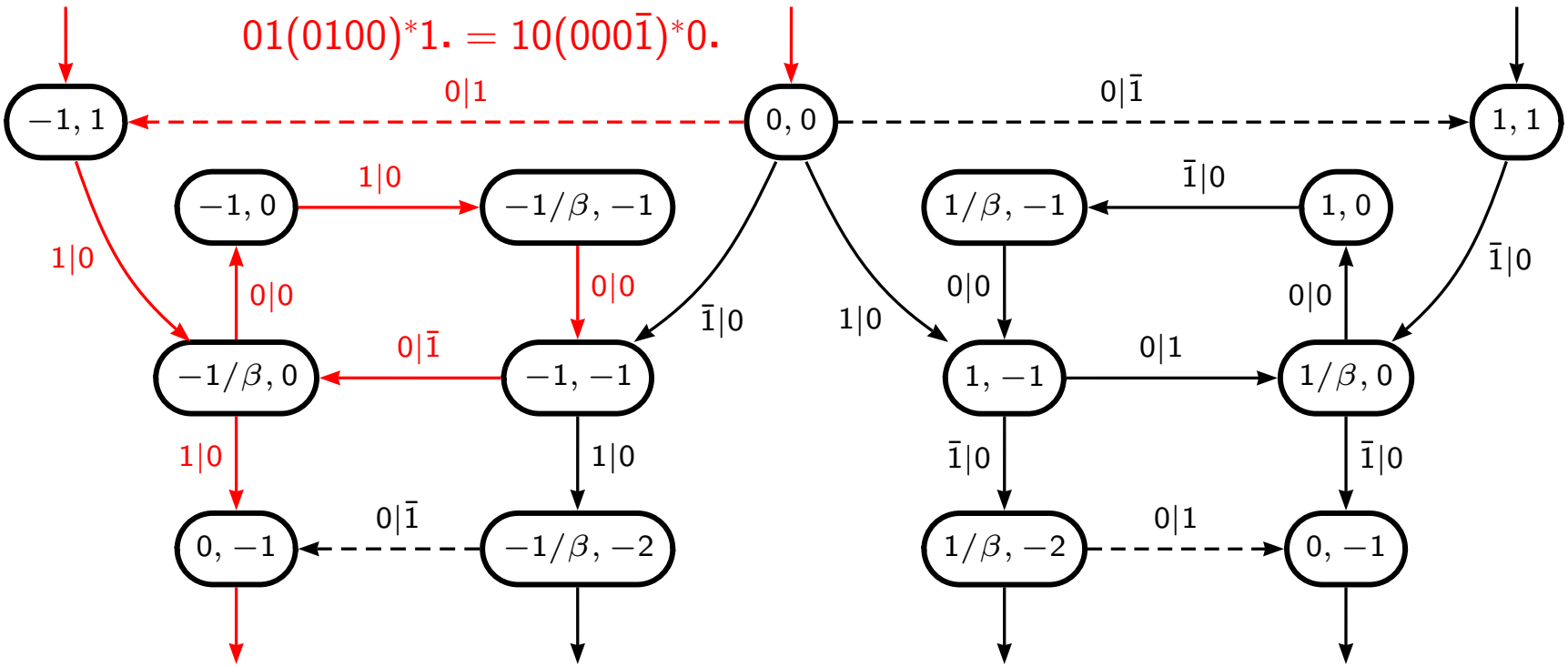
$$(s,\delta) \xrightarrow{x|y} (s',\delta') : \; s' = \beta s + x - y, \; \delta' = \delta + |y| - |x|$$

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 $(0,-1)$).



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

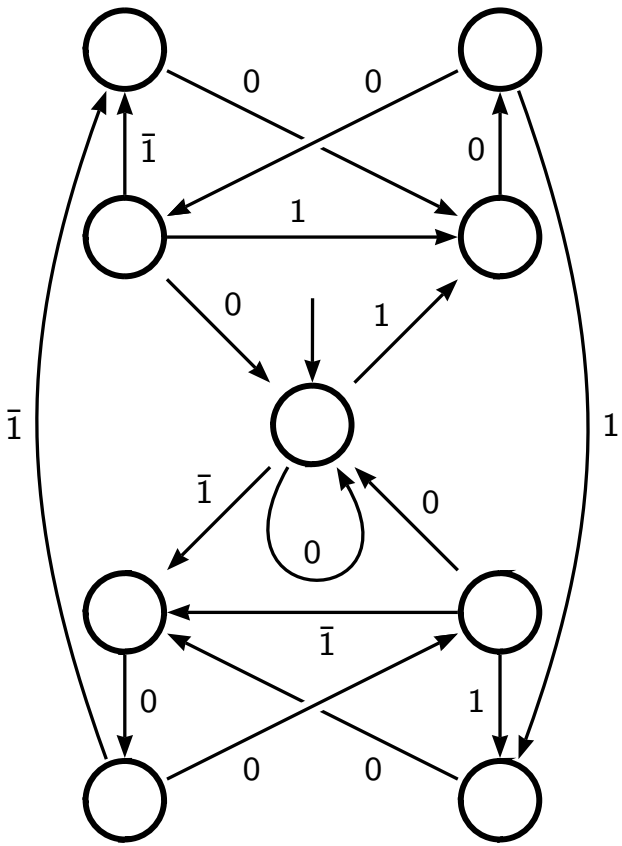
The strictly β-heavy words are the inputs of the following transducer. The outputs are corresponding lighter words (if the path is completed by dashed arrows such that it runs from $(0,0)$ to $(0,-1)$).

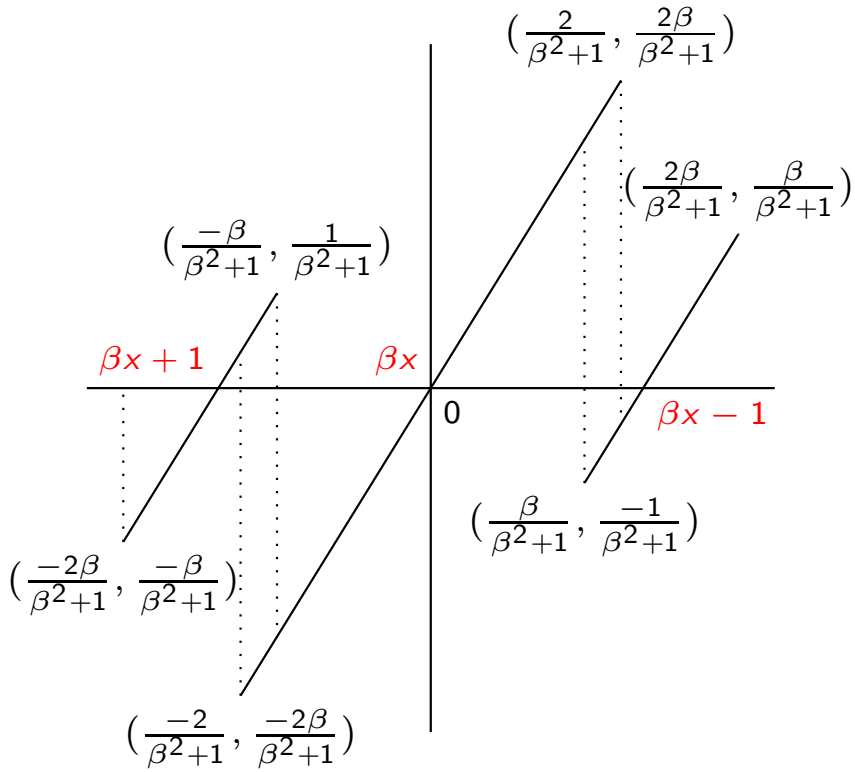


$$(s,\delta) \xrightarrow{x|y} (s',\delta') : \ s' = \beta s + x - y, \ \delta' = \delta + |y| - |x|$$

Theorem

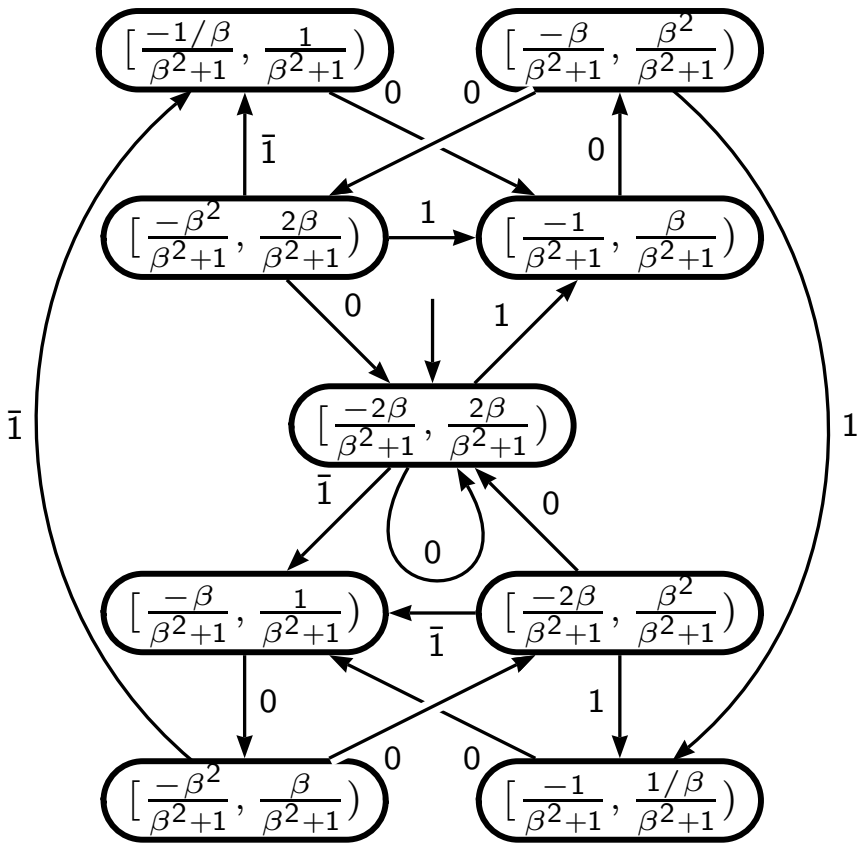
For $\beta = \frac{1+\sqrt{5}}{2}$, all signed β-expansions of minimal weight are given by the following automaton, where all states are terminal, and by the following branching transformation.

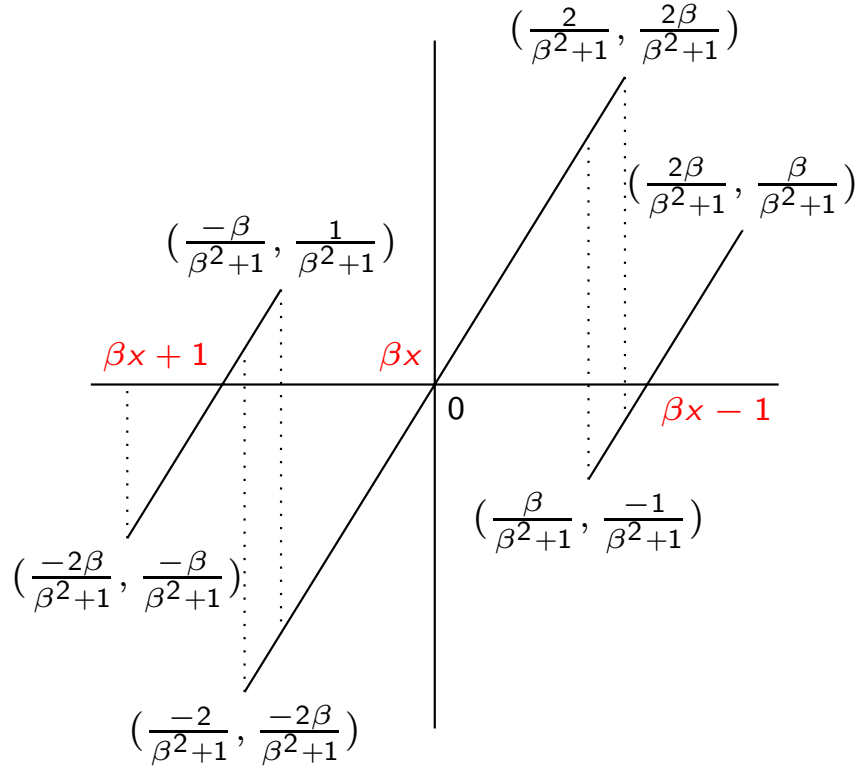




Theorem

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.





possible "NAF"s: exclude factors $11, 1\bar{1}, 101, 100\bar{1}$ and their opposites, or $11, 1\bar{1}, 101, 1001$

Fibonacci numeration system

Let $F_0 = 1$, $F_1 = 2$, $F_k = F_{k-1} + F_{k-2}$.
Then every integer $N \geq 0$ has a unique F-expansion

$$N = \sum_{k=1}^{n} x_k F_{n-k} = \langle x_1 \cdots x_n \rangle_F$$

with $x_k \in \{0, 1\}$ and $x_k x_{k+1} = 0$.

$x_1 \cdots x_n \in \{0, \pm 1\}^*$ is F-heavy if there exists $y_\ell \cdots y_n \in \{0, \pm 1\}^*$ such that $\langle x_1 \cdots x_n \rangle_F = \langle y_\ell \cdots y_n \rangle_F$ and $h(y_\ell \cdots y_n) < h(x_1 \cdots x_n)$.

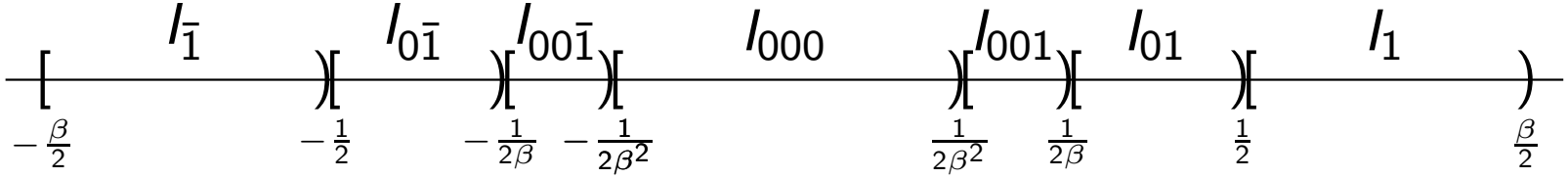
$\langle \cdots 1\bar{1}0 \cdots \rangle_F = \langle \cdots 001 \cdots \rangle_F$, but $\langle \cdots 1\bar{1} \rangle_F = \langle \cdots 01 \rangle_F$.

Theorem

The F-heavy words are exactly the β-heavy words for $\beta = \frac{1+\sqrt{5}}{2}$, i.e. a word is a signed F-expansion of minimal weight if and only if it is a signed β-expansion of minimal weight.

Markov chain of digits

Let $T(x) = \beta x - \lfloor x + 1/2 \rfloor$, and intervals I_j as follows

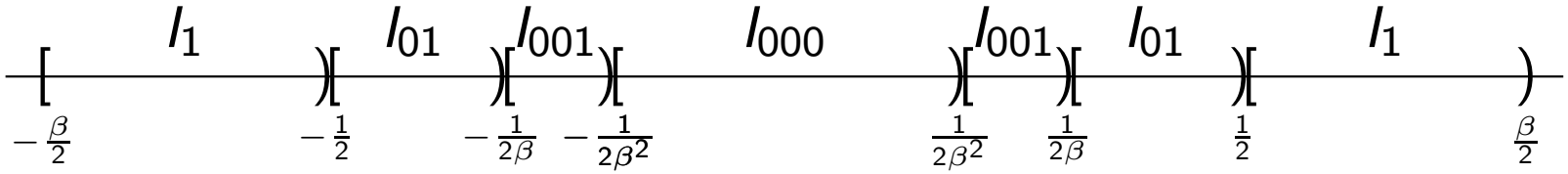


The sequence of random variables $(X_k)_{k \geq 0}$ defined by

$$\begin{aligned}
&\Pr[X_0 = j_0, \ldots, X_k = j_k] \\
&= \lambda(\{x \in [-\beta/2, \beta/2) : x \in I_{j_0}, T(x) \in I_{j_1}, \ldots, T^k(x) \in I_{j_k}\})/\beta \\
&= \lambda(I_{j_0} \cap T^{-1}(I_{j_1}) \cap \cdots \cap T^{-k}(I_{j_k}))/\beta
\end{aligned}$$

(where λ denotes the Lebesgue measure) is a Markov chain since the image of every I_j is a union of I_i's ($T(I_1) = I_{000} \cup I_{001}$) and $T(x)$ is affine on each I_j.

Put together I_1 and $I_{\bar{1}}$, I_{01} and $I_{0\bar{1}}$, I_{001} and $I_{00\bar{1}}$:



Then the matrix of transition probabilites is

$$(\Pr[X_k = j \mid X_{k-1} = i])_{i,j\in\{000,001,01,1\}} = \begin{pmatrix} 1/\beta & 1/\beta^2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 2/\beta^2 & 1/\beta^3 & 0 & 0 \end{pmatrix}$$

The stationary distribution vector is $(2/5, 1/5, 1/5, 1/5)$. Therefore

$$\Pr[X_k = 1] = \lambda(\{x \in [-\beta/2, \beta/2) : T^k(x) \in I_1) \to 1/5,$$

i.e., the expected number of non-zero digits in a signed β-expansion of minimal weight of length n is $n/5 + \mathcal{O}(1)$.
(cf. greedy β-expansions $n/(\beta^2+1)$, base 2 minimal expansions $n/3$)

Weight of integer expansions

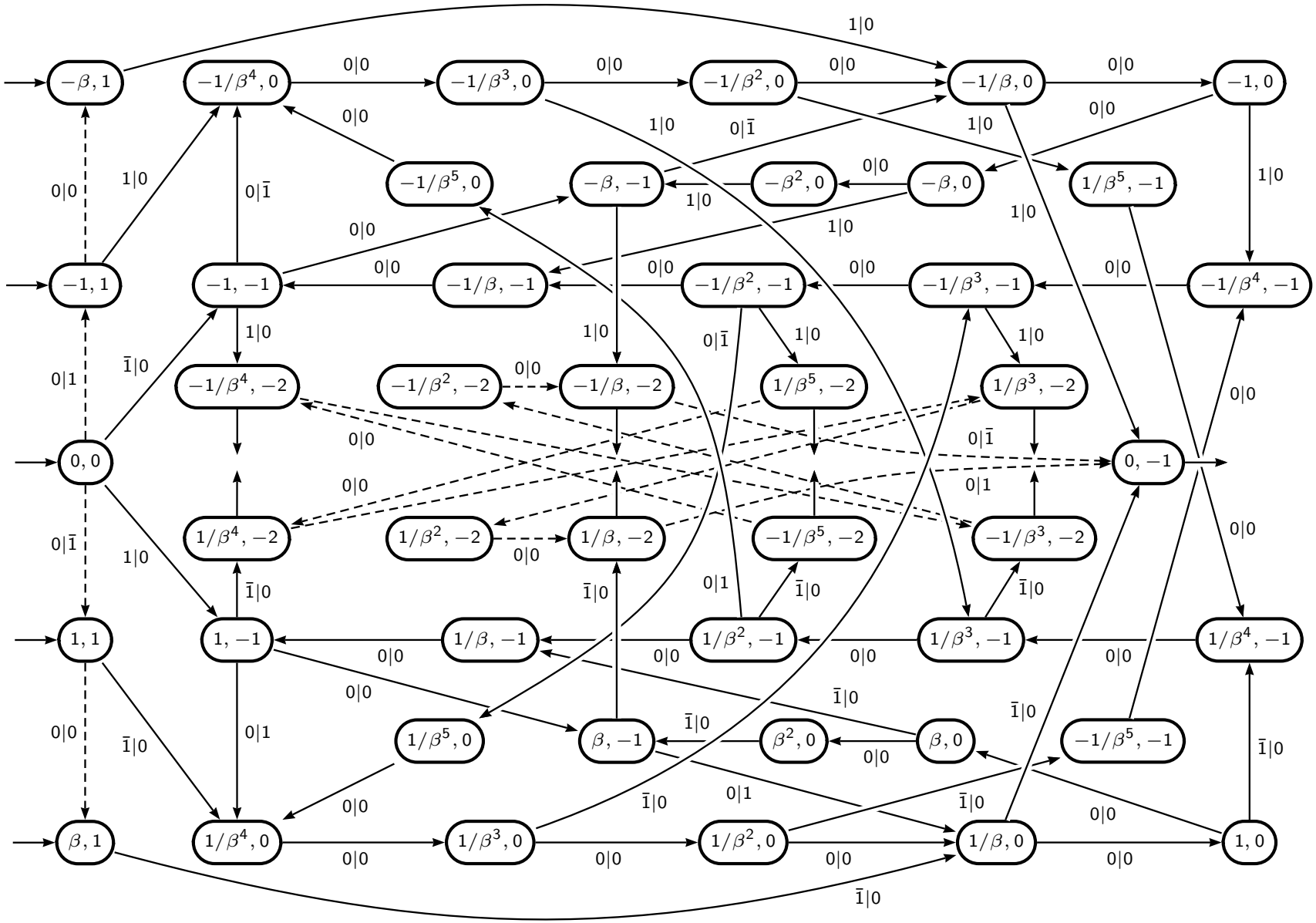
$N = \sum_{k=0}^{L} x_k U_k$, U_k sequence of increasing integers,
$x_L \cdots x_1 x_0$ expansion of minimal weight

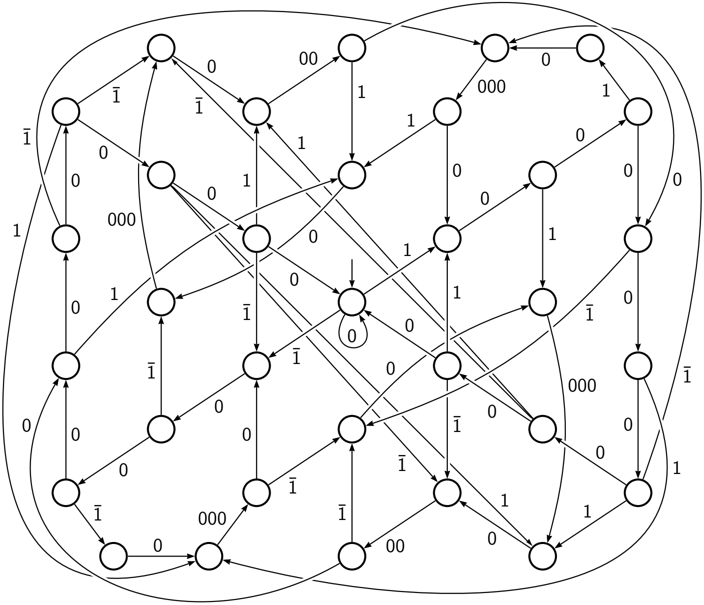
$$U_k = \Theta(\beta^k) \Rightarrow L \sim \log_\beta N$$

U_k	x_k	β	expected weight of $x_L \cdots x_1 x_0$
2^k	$\{0, 1\}$	2	$(\log_2 N)/2$
2^k	$\{0, \pm 1\}$	2	$(\log_2 N)/3$
F_k	$\{0, 1\}$	$\frac{1+\sqrt{5}}{2}$	$(\log_\beta N)/(\beta^2+1) \approx 0.398 \log_2 N$
F_k	$\{0, \pm 1\}$	$\frac{1+\sqrt{5}}{2}$	$(\log_\beta N)/5 \approx 0.288 \log_2 N$
$*$	$\{0, \pm 1\}$	$\beta^3 = \beta + 1$	$(\log_\beta N)/(7+2\beta^2) \approx 0.235 \log_2 N$

$*$: $U_{k+3} = U_{k+1} + U_k$, $\beta \approx 1.325$ is the smallest Pisot number,
$7 + 2\beta^2 \approx 10.51$

β-heavy words, $\beta^3 = \beta + 1$





“NAF”s: exclude factors $10^k1, 10^k\bar{1}, 0 \leq k \leq 5$ and either 10^61 or $10^6\bar{1}$

General case, condition (D)

(D): $\beta > 1$ and $P(\beta) = 0$ for some polynomial
$P(X) = X^d - b_1 X^{d-1} - \cdots - b_d \in \mathbb{Z}[X]$ with $b_1 > \sum_{j=2}^{d} |b_j|$

If β satisfies (D), then β is a Pisot number.

Proposition (Akiyama, Rao, St. 2004)

Let β satisfy (D), and $x_1 \cdots x_n \in \mathbb{Z}^*$ such that $|.x_1 \cdots x_n| < 1$. Then there exists a word $y_0 \cdots y_m \in \{-\lfloor\beta\rfloor, \ldots, \lfloor\beta\rfloor\}^*$ such that $y_0.y_1 \cdots y_m = .x_1 \cdots x_n$ and $\sum_{j=0}^{m} |y_j| \leq \sum_{j=1}^{n} |x_j|$.

Theorem

If β satisfies (D), then the set of signed β-expansions of minimal weight is recognized by a finite automaton.