A Polynomial Time Constructible Hitting Set for Restricted 1-Branching Programs of Width 3

Jiří Šíma and Stanislav Žák

Institute of Computer Science AS CR, v.v.i.
P. O. Box 5, 182 07 Prague 8,
Czech Republic

sima|stan@cs.cas.cz

Motivation:

– the issue of this paper was pointed out to us by Pavel Pudlák

– a polynomial-time construction of a so-called hitting set for general branching programs implies BPP=P

– this construction is unknown even for read-once branching programs of width 3

Given $n \in N$

a branching program P
on the set of variables $X_n = \{x_1, \ldots, x_n\}$

is a multigraph $G = (V, E)$

– directed, acyclic, one source
– out-degree = 2
– sinks labeled by 0, 1
– the inner nodes labeled by variables $\in X_n$
– the outgoing edges labeled by 0, 1

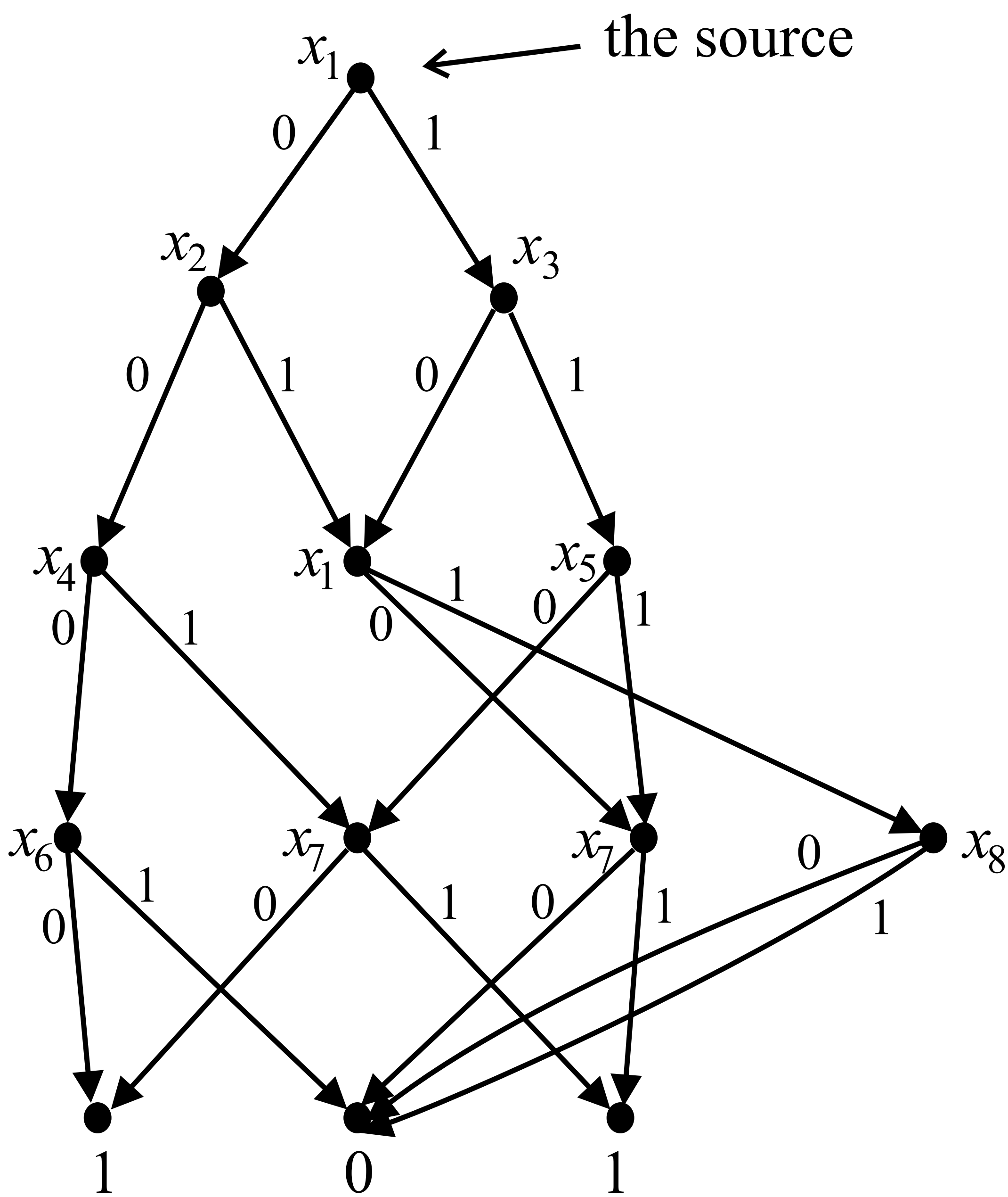
P computes $f_P : \{0,1\}^n \to \{0,1\}$

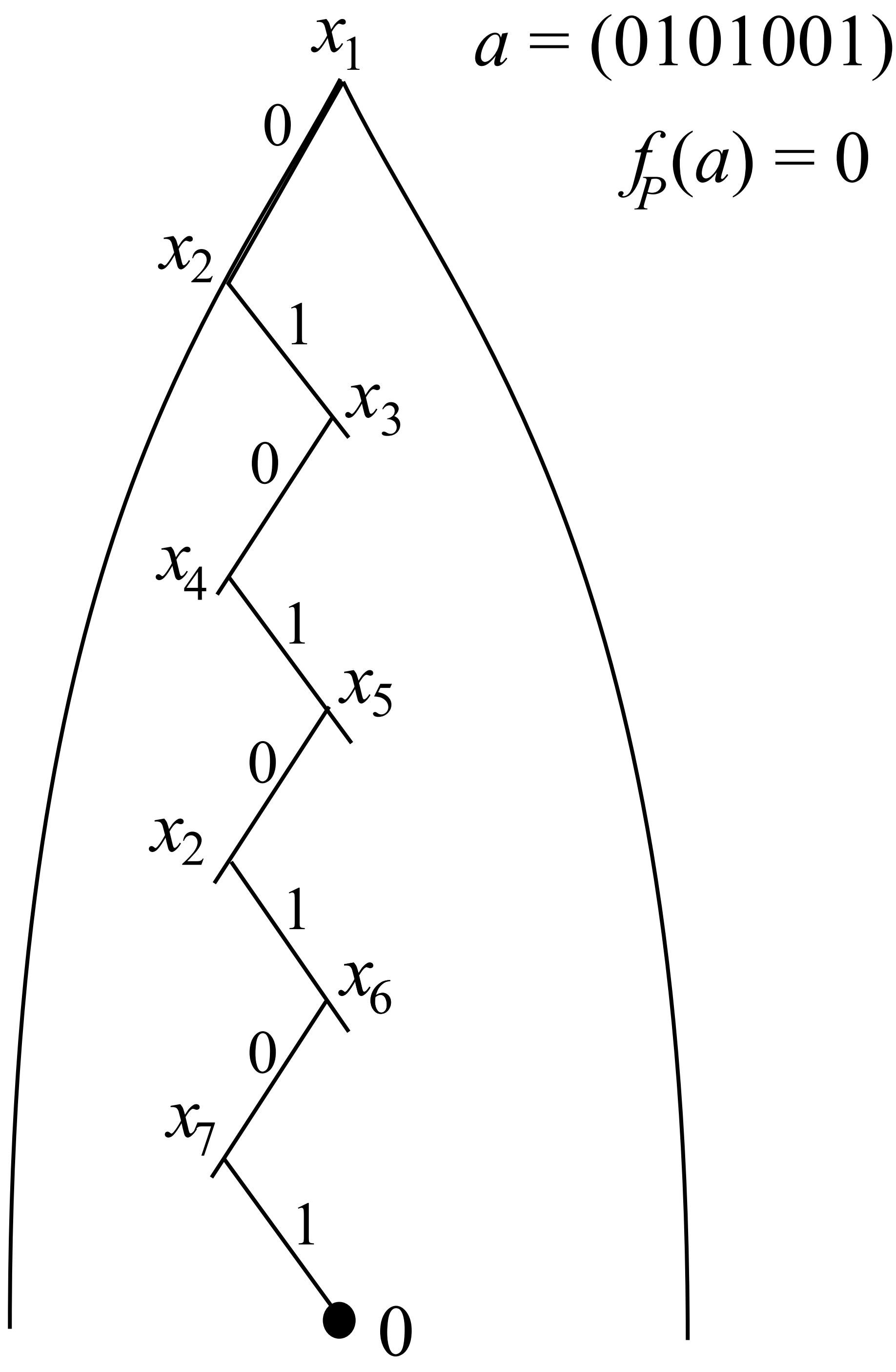
for $a \in \{0,1\}^n$

$comp(a)$ starts in the source
and ends in one of sinks

in the inner node labeled by x_i
$comp(a)$ follows the edge labeled by a_i

$f_P(a) = P(a) =_{df}$ the label of the reached sink


the source
x_1
0
1
x_2
x_3
0
1
0
1
x_4
x_1
x_5
0
1
0
1
0
1
x_6
x_7
x_7
x_8
0
1
0
1
0
1
0
1
1
0
1

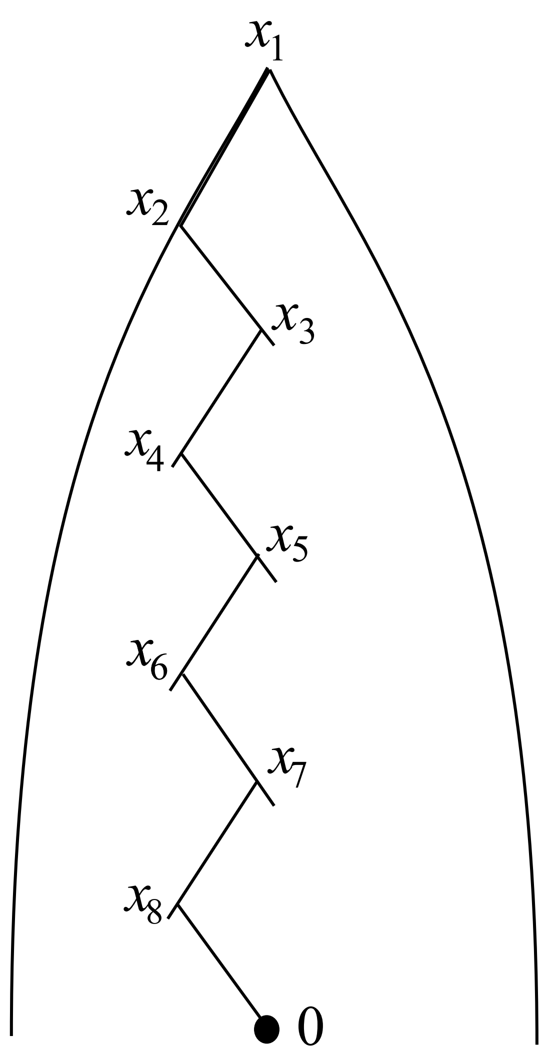

x_1
$a = (0101001)$
$f_P(a) = 0$
0
x_2
1
x_3
0
x_4
1
x_5
0
x_2
1
x_6
0
x_7
1
0

– each Boolean function
is computable by a branching program

– the complexity of a function f is given by the size of minimal b. p. computing f

– the space complexity of f is at least logarithm of b. p. complexity of f

A read-once branching program



On each path from the source to a sink each variable is tested at most once.

In the last 3 decades many superpolynomial lower bounds concerning read-once b. p.'s were proven.

P is **a leveled b. p.**

$\Longleftrightarrow$

- each node belongs to a level
- edges lead from level k to level $k+1$ only
- the source creates level 0
- the last level is composed of sinks

---

the depth of $P =_{df}$ the number of levels -1

the width of $P =_{df}$ the maximum number of nodes on one level

---

Normalized width-d branching program

$v_1^k, \ldots, v_d^k$ = nodes on level k

$M(v_i^k)$ = the number of inputs reaching v_i^k

(of course $\bigcup_{i=1}^{d} M(v_i^k) = \{0,1\}^n$).

$p_i^k =_{df} \frac{|M(v_i^k)|}{2^n}$

P **is normalized** iff

$1 > p_1^k \geq p_2^k \ldots \geq p_d^k > 0$

for every $k \geq \log_2 d$

Lemma:

Any width d 1-branching program
can be normalized.

Normalized 1$-$ b. p.'s of width 3

$p_1^k + p_2^k + p_3^k = 1$

$1 > p_1^k \geq p_2^k \geq p_3^k > 0$

$p_1^k > \frac{1}{3}, \quad p_2^k < \frac{1}{2}, \quad p_3^k < \frac{1}{3}$

for each k, $2 \leq k \leq d_P$

(d_P is the last level of P)

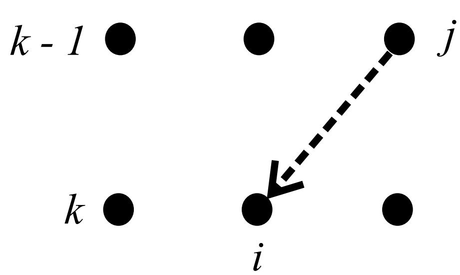
$m_P =_{df}$ the last level m of P
such that $p_3^m \geq \frac{1}{12}$

Notation

for k, $\quad 1 \leq k \leq d_P$

for $i, j \quad 1 \leq i, j \leq 3$

$t_{ij}^k \in \left\{0, \frac{1}{2}, 1\right\}$



$t_{ij}^k = 0, \frac{1}{2}, 1$
$\Downarrow$
$0, 1, 2,$ edge(s)

Lemma

For every level $k = m_P + 1, \ldots, d_P$ it holds

i) $t^k_{31} = 0$

ii) $p^{k-1}_2 \geq \frac{1}{6} \Rightarrow t^k_{32} = 0$

iii) $p^k_2 < \frac{1}{6} \Rightarrow t^k_{11} = 1$

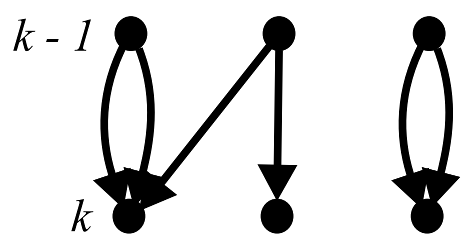
iv) $p^{k-1}_2 \geq \frac{1}{6}$ and $p^k_2 < \frac{1}{6} \Rightarrow t^k_{22} \leq \frac{1}{2}$

Let P be a normalized $1-$ b. p. of width 3.

P is *simple*

iff

below $m_P\, P$ does not contain transition such that $t^k_{11} = t^k_{33} = 1$ and $t^k_{12} = t^k_{12} = \frac{1}{2}$.



(Below m_P there are transitions of 39 possible types)

Definition

Given $n \in N$.

$M \subseteq \{0,1\}^n$ is an ε-hitting
set for a class C of b.p.'s over X_n

iff

$\forall P \in C \quad |P^{-1}(1)|/2^n \geq \varepsilon$

$\exists a \in M$

$P(a) = 1$

Theorem

M^3 is a $\frac{191}{192}$ - hitting set

for the class of *simple*

normalized read-once b.p.

of width 3.

Alon, Godreich, Håstad, Peralta (1992)

$\exists \mathcal{A} \subseteq \{0,1\}^n, \quad |\mathcal{A}|$ polynomial

$\forall r \leq \log_2 n$

$\forall\, i_1, \ldots, i_r$ indices, $1 \leq i_1 < i_2 \ldots < i_r \leq n$

$\{a_{i_1} \ldots a_{i_r} | a \in \mathcal{A}\} = \{0,1\}^r$

$c \in N$

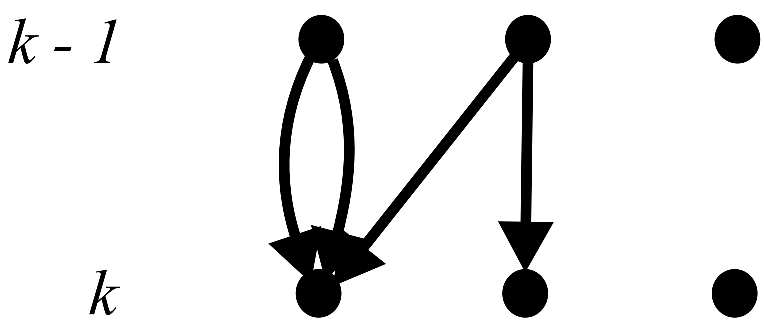
$M^c =_{df} \{m \in \{0,1\}^n | \exists a \in \mathcal{A}$
$Hamm.dist.(a,m) \leq c\}$

$|M^c|$ is polynomial

Definition

By a **special transition** $(k-1, k)$
we mean the transition with

$$p_2^{k-1} \geq \frac{1}{6}$$



$$p_2^{k} < \frac{1}{6}$$

Let $c \geq 0, 0 < \delta < \frac{1}{2}$

A normaliz. width 3 P is
(c, δ) – restricted

iff

$m_P = d_P$

or

below m_P there is m' s.t.

$p_2^{m'-1} \geq \delta$

and with at most c special
transitions below (m').

Theorem

M^{c+3} is a $\left(1-\frac{\delta}{8}\right)$-hitting

set for the class of (c, δ)

restricted normalized read one

b. p. of width 3.

Some points of the proof

By contradiction.

We suppose

$\exists P$ b. p. (c, δ)-restricted s.t.

$\left|\frac{P^{-1}(0)}{2^n}\right| \leq \frac{\delta}{8}$ and

$P(a) = 0$ for every $a \in M^{c+3}$.

Then there is a b. p. P

$(0, \delta)$-restricted

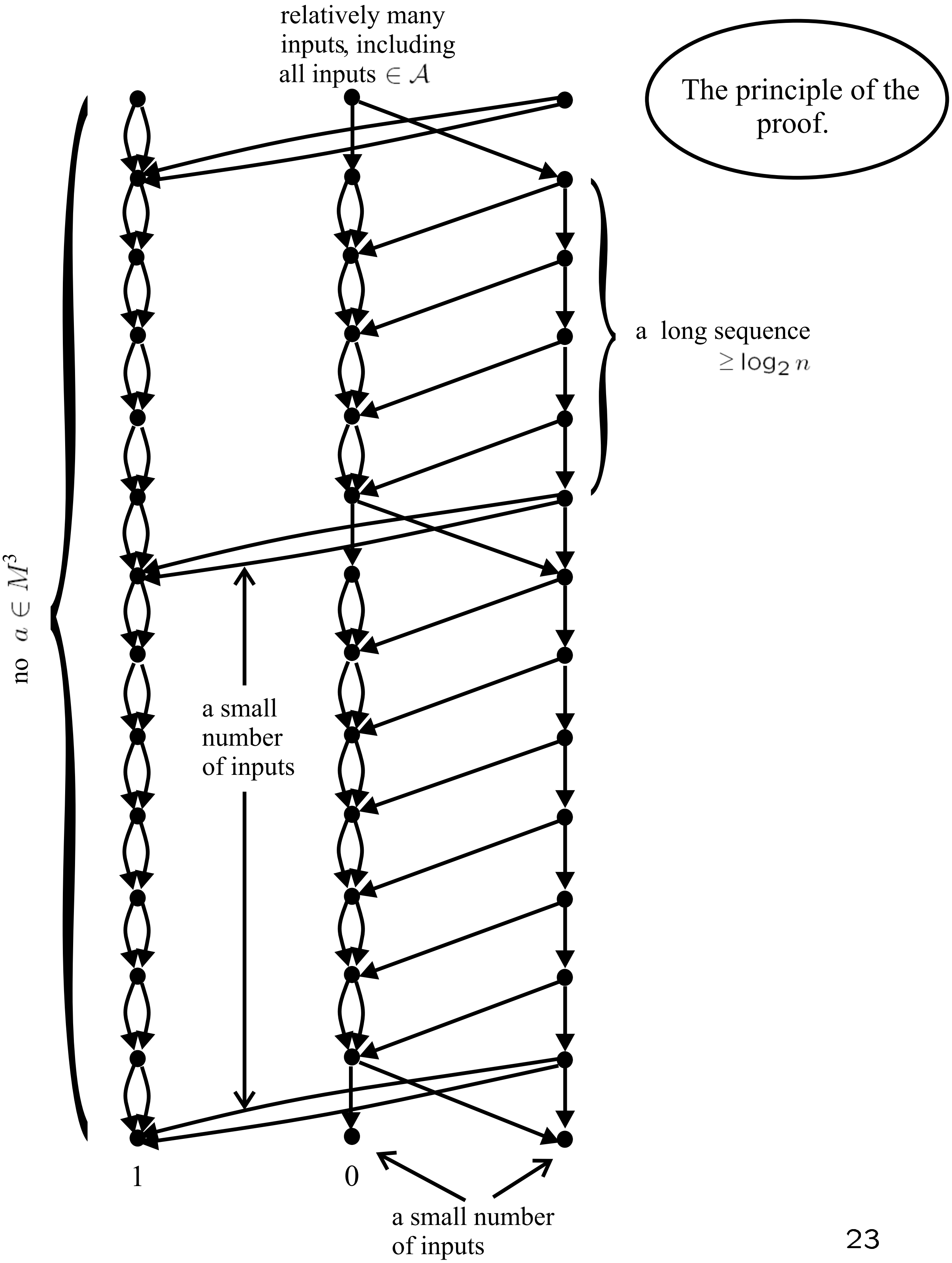
with small $P^{-1}(0)$ and

such that $P(a) = 0$ for every $a \in M^3$.

Moreover for $k \geq m_P$

$t^k_{11} = 1, \quad t^k_{12} = 0, \quad t^k_{22} \geq \frac{1}{2}, \quad t^k_{13} \in \{0, 1\}$

typical transitions


relatively many
inputs, including
all inputs $\in \mathcal{A}$
The principle of the proof.
a long sequence
$\geq \log_2 n$
no $a \in M^3$
a small
number
of inputs
1
0
a small number
of inputs