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

Jiří Šíma* and Stanislav Žák**

Institute of Computer Science, Academy of Sciences of the Czech Republic,
P. O. Box 5, 18207 Prague 8, Czech Republic, sima|stan@cs.cas.cz

Abstract. An important problem in complexity theory is to find polynomial time constructible hitting sets for Boolean functions in different standard models. This would have consequences for the relationship between deterministic and probabilistic computations in the respective models. Using the result by Alon, Goldreich, Håstad, and Peralta (1992) we provide a polynomial time constructible hitting set for restricted read-once branching programs of width 3. The restriction excludes only one from all patterns of level-to-level transitions in a normalized form of 3-width 1-branching programs. In fact, our technique works for a slightly more general class of such programs. Although this restriction seems to be relatively strong our proof reveals the core of difficulties and thus represents the first step for proving the result for less restricted models.

1 Introduction

An ε-hitting set for a class of Boolean functions of n variables is a set $M \subseteq \{0,1\}^n$ such that for every function f in the class, the following is satisfied: If a random input is accepted by f with probability at least ε, then there is also an input in M that is accepted by f. An efficiently constructible sequence of hitting sets for increasing n is a straightforward generalization of the hitting set generator introduced in [2].

For the class of Boolean functions of polynomial complexity in any reasonable model, it is easy to prove the existence of ε-hitting set of polynomial size, if $\varepsilon > 1/n^c$ for a constant c and n is the number of variables. The proof is nonconstructive, since it uses a counting argument. An important problem in complexity theory is to find polynomial time constructible hitting sets for functions of polynomial complexity in different standard models like circuits, formulas, branching programs etc. Such constructions would have consequences for the relationship between deterministic and probabilistic computations in the respective models.

Looking for polynomial time constructions of hitting sets for unrestricted models belongs to the hardest problems in computer science. Hence, restricted

* Research partially supported by project 1M0545 of The Ministry of Education of the Czech Republic.

** Research partially supported by the "Information Society" project 1ET100300517 and the Institutional Research Plan AV0Z10300504.

models are investigated. In this paper, we find a polynomial time constructible hitting set for restricted read-once branching programs of width 3 by using the result from [1]. The restriction excludes only one from all patterns of level-to-level transitions in a normalized form of 3-width 1-branching programs. In fact, our proof technique works for a slightly more general class of such programs which are defined by a rather technical restriction. Although this restriction seems to be relatively strong our proof reveals the crux of difficulties and thus represents the first step for proving the result for less restricted models.

The paper is organized as follows. After a brief review of basic definitions regarding branching programs in Section 2 (see [3] for more information), the main result concerning the hitting set for restricted 3-width 1-branching programs is presented in Section 3. The remaining two sections are devoted to the technical proof.

2 Normalized Width-*d* 1-Branching Programs

A *branching program* P_n on the set of input Boolean variables $X_n = \{x_1, \ldots, x_n\}$ is a directed acyclic multi-graph $G = (V, E)$ that has one *source* $s \in V$ of zero in-degree and, except for *sinks* of zero out-degree, all the *inner* (non-sink) nodes have out-degree 2. In addition, the inner nodes get labels from X_n and the sinks get labels from $\{0, 1\}$. For each inner node, one of the outgoing edges gets the label 0 and the other one gets the label 1. The branching program P_n computes Boolean function $P_n : \{0, 1\}^n \longrightarrow \{0, 1\}$ as follows. The computational path of P_n for an input $\mathbf{a} = (a_1, \ldots, a_n) \in \{0, 1\}^n$ starts at source s. At any inner node labeled by $x_i \in X_n$, input variable x_i is tested and this path continues with the outgoing edge labeled by a_i to the next node, which is repeated until the path reaches the sink whose label gives the output value $P_n(\mathbf{a})$. Denote by $P_n^{-1}(a) = \{\mathbf{a} \in \{0, 1\}^n \,|\, P_n(\mathbf{a}) = a\}$ the set of inputs for which P_n gives $a \in \{0, 1\}$. For inputs of arbitrary lengths, infinite families $\{P_n\}$ of branching programs, each P_n for one input length $n \geq 1$, are used.

A branching program P_n is called *read-once* (or shortly *1-branching* program) if every input variable from X_n is tested at most once along each computational path. Here we consider *leveled* branching programs in which each node belongs to a level and edges lead from level $k \geq 0$ only to the next level $k+1$. We assume that the source of P_n creates level 0 whereas the last level is composed of sinks. The number of levels decreased by 1 equals the *depth* of P_n which is the length of its longest path, and the maximum number of nodes on one level is called the *width* of P_n.

For a 1-branching program P_n of width d define a $d \times d$ *transition matrix* $\mathbf{T}_k$ on level $k \geq 1$ such that $t_{ij}^{(k)} \in \{0, \frac{1}{2}, 1\}$ is the half of the number of edges leading from node $v_j^{(k-1)}$ $(1 \leq j \leq d)$ on level $k-1$ of P_n to node $v_i^{(k)}$ $(1 \leq i \leq d)$ on level k. For example, $t_{ij}^{(k)} = 1$ implies there is a *double edge* from $v_j^{(k-1)}$ to $v_i^{(k)}$. Clearly, $\sum_{i=1}^{d} t_{ij}^{(k)} = 1$ since this sum equals the half of the out-degree of inner node $v_j^{(k-1)}$, and $2 \cdot \sum_{j=1}^{d} t_{ij}^{(k)}$ is the in-degree of node $v_i^{(k)}$. Denote by a column vector $\mathbf{p}^{(k)} = (p_1^{(k)}, \ldots, p_d^{(k)})^\mathsf{T}$ the *distribution* of inputs among d nodes on level k of P_n, that is $p_i^{(k)}$ is the probability that a random input is tested at node $v_i^{(k)}$ which equals the ratio of inputs from $M(v_i^{(k)}) \subseteq \{0,1\}^n$ that are tested at $v_i^{(k)}$ to all 2^n possible inputs. It follows $\bigcup_{i=1}^d M(v_i^{(k)}) = \{0,1\}^n$ and $\sum_{i=1}^d p_i^{(k)} = 1$ for every level $k \geq 0$.

Given the distribution $\mathbf{p}^{(k-1)}$ on level $k-1$, the distribution on the subsequent level k can be computed using transition matrix $\mathbf{T}_k$ as follows:

$$\mathbf{p}^{(k)} = \mathbf{T}_k \cdot \mathbf{p}^{(k-1)} \,. \tag{1}$$

It is because the ratio of inputs coming to node $v_i^{(k)}$ from previous-level nodes equals $p_i^{(k)} = \sum_{j=1}^d t_{ij}^{(k)} p_j^{(k-1)}$ since each of the two edges outgoing from node $v_j^{(k-1)}$ distributes exactly the half of the inputs tested at $v_j^{(k-1)}$.

We say that a 1-branching program P_n of width d is *normalized* if P_n does not contain the identity transition, that is $\mathbf{T}_k \neq \mathbf{I}$, and satisfies

$$1 > p_1^{(k)} \geq p_2^{(k)} \geq \cdots \geq p_d^{(k)} > 0 \tag{2}$$

for every $k \geq \log_2 d$.

Lemma 1. *Any width-d 1-branching program can be normalized.*

Proof. We can assume without loss of generality there are exactly d nodes on every level $k \geq \log_2 d$ of a width-d branching program since a node with in-degree at least 2 that belongs to level $k \geq \log_2 d$ with fewer than d nodes can possibly be split into two nodes with the same outgoing edges while the incoming edges being arbitrarily divided between these two new nodes.

The normalization proceeds by induction on level k starting with the initial distribution $\mathbf{p}^{(0)} = (1, 0, \ldots, 0)^\mathsf{T}$. Assume that the branching program has been normalized up to level $k-1$. Let $\pi : \{1, \ldots, d\} \longrightarrow \{1, \ldots, d\}$ be the permutation that meets the decreasing order of distribution on level k so that $p_{\pi(1)}^{(k)} \geq p_{\pi(2)}^{(k)} \geq \cdots \geq p_{\pi(d)}^{(k)}$. Now it suffices to sort the nodes on level k according to permutation π which gives rise to new transition matrices $\mathbf{T}'_k$ and $\mathbf{T}'_{k+1}$ by permuting the rows of $\mathbf{T}_k$ and the columns of $\mathbf{T}_{k+1}$, respectively, that is $t'^{(k)}_{ij} = t_{\pi(i)j}^{(k)}$ and $t'^{(k+1)}_{ij} = t_{i\pi(j)}^{(k+1)}$. Such node permutations do not change the function that is computed by the program. The same holds after we delete the identity transitions. $\square$

In the sequel, we confine ourselves to the families of normalized 1-branching programs $\{P_n\}$ of width 3. Any such program P_n satisfies $p_1^{(k)} + p_2^{(k)} + p_3^{(k)} = 1$ and $1 > p_1^{(k)} \geq p_2^{(k)} \geq p_3^{(k)} > 0$ which implies

$$p_1^{(k)} > \frac{1}{3} \,, \qquad p_2^{(k)} < \frac{1}{2} \,, \qquad p_3^{(k)} < \frac{1}{3} \tag{3}$$

for every level $2 \leq k \leq d_n$ where $d_n \leq n$ is the depth of P_n. In addition, denote by $m_n \leq d_n$ the last level of P_n such that $p_3^{(m_n)} \geq \frac{1}{12}$. Note that such m_n exists since $p_3^{(2)} = \frac{1}{4}$ due P_n is normalized. Then the following trivial observations follows:

Lemma 2. *For every level $k = m_n + 1, \ldots, d_n$ it holds*

(i) $t_{31}^{(k)} = 0$,
(ii) $p_2^{(k-1)} \geq \frac{1}{6}$ *implies* $t_{32}^{(k)} = 0$,
(iii) $p_2^{(k)} < \frac{1}{6}$ *implies* $t_{11}^{(k)} = 1$,
(iv) $p_2^{(k-1)} \geq \frac{1}{6}$ *and* $p_2^{(k)} < \frac{1}{6}$ *implies* $t_{22}^{(k)} \leq \frac{1}{2}$.

We say that a normalized 1-branching program P_n of width 3 is *simple* if P_n does not contain transition $\mathbf{T}_k$ such that $t_{11}^{(k)} = t_{33}^{(k)} = 1$ and $t_{12}^{(k)} = t_{22}^{(k)} = \frac{1}{2}$, below level m_n (i.e. $m_n < k \leq d_n$).

3 Main Result

Alon, Goldreich, Håstad, and Peralta [1] provided a polynomial time construction of a set $\mathcal{A}_n \subseteq \{0,1\}^n$ of Boolean vectors satisfying $\{a_{i_1} \ldots a_{i_r} \mid \mathbf{a} \in \mathcal{A}_n\} = \{0,1\}^r$ for any choice $1 \leq i_1 < i_2 < \cdots < i_r \leq n$ of $r \leq \log_2 n$ indices. We define $\mathcal{M}_n^c = \Omega_c(\mathcal{A}_n)$ and $\mathcal{M}^c = \bigcup_{n \geq 1} \mathcal{M}_n^c$ where $\Omega_c(A) = \{\mathbf{a}' \in \{0,1\}^n \mid (\exists \mathbf{a} \in A)\ \mathcal{H}(\mathbf{a}, \mathbf{a}') \leq c\}$ for some constant $c \geq 0$, and $\mathcal{H}(\mathbf{a}, \mathbf{a}') = |\{1 \leq i \leq n \mid a_i \neq a_i'\}|$ denotes the Hamming distance between $\mathbf{a}$ and $\mathbf{a}'$. Obviously, set $\mathcal{M}_n^c$ can easily be constructed from $\mathcal{A}_n$ in polynomial time.

Recall an ε-*hitting set* for a class of families of branching programs is a set $M \subseteq \{0,1\}^n$ such that for every family $\{P_n\}$ in this class that satisfies $|P_n^{-1}(1)|/2^n \geq \varepsilon$ for every n, there is an n-bit input $\mathbf{a} \in M$ for each n such that $P_n(\mathbf{a}) = 1$.

Theorem 1. *$\mathcal{M}^3$ is a $\frac{191}{192}$-hitting set for the class of* simple *normalized read-once branching programs of width 3.*

In fact, our proof technique works for a more general class of normalized width-3 1-branching programs than the simple ones, which is defined by the following rather complicated restriction. Let $c \geq 0$ and $0 < \delta < \frac{1}{2}$ be an integer and real constant, respectively. We say that a family of normalized width-3 1-branching programs $\{P_n\}$ is (c, δ)-*restricted* if for every $n \geq 1$ either $m_n = d_n$ or there is a level $m_n < m_n' \leq d_n$ of P_n such that

$$p_2^{(m_n'-1)} \geq \delta\,, \tag{4}$$

$$t_{12}^{(m_n')} = 0\,, \tag{5}$$

$$c_n = \left|\left\{ m_n' < k \leq d_n \;\middle|\; p_2^{(k-1)} \geq \frac{1}{6}\,, p_2^{(k)} < \frac{1}{6}\,, t_{22}^{(k)} = \frac{1}{2} \right\}\right| \leq c\,. \tag{6}$$

Thus, we will first prove the following theorem:

Theorem 2. *$\mathcal{M}^{c+3}$ is a $\left(1 - \frac{\delta}{8}\right)$-hitting set for the class of (c, δ)-restricted normalized read-once branching programs of width 3.*

Proof. Let $\{P_n\}$ be a family of (c,δ)-restricted normalized width-3 1-branching programs such that $|P_n^{-1}(1)|/2^n \geq 1-\frac{\delta}{8}$ which reads

$$\frac{|P_n^{-1}(0)|}{2^n} \leq \frac{\delta}{8}\,, \tag{7}$$

and on the contrary suppose that

$$P_n(\mathbf{a}) = 0 \quad \text{for every} \quad \mathbf{a} \in \mathcal{M}_n^{c+3}\,. \tag{8}$$

Inequality (7) implies $p_3^{(d_n)} \leq |P_n^{-1}(0)|/2^n < \frac{1}{12}$ due to $\delta < \frac{1}{2}$, and hence $m_n < d_n$. It follows from the definition of (c,δ)-restriction that there must be a level $m_n < m_n' \leq d_n$ of P_n satisfying (4)–(6).

4 Constructing the Double-Edge Path

In this section, we will reduce the family $\{P_n\}$ to a family of normalized width-3 1-branching programs $\{P_n'\}$ satisfying condition (7) and

$$P_n'(\mathbf{a}) = 0 \quad \text{for every} \quad \mathbf{a} \in \mathcal{M}_n^{2}\,, \tag{9}$$

such that

$$t_{11}^{(k)} = 1 \quad \text{and} \quad t_{12}^{(k)}, t_{13}^{(k)} \in \{0,1\} \quad \text{for every} \quad k = m_n', \ldots, d_n\,. \tag{10}$$

We start with the *last* level $m_n' < m' \leq d_n$ that meets

$$p_2^{(m'-1)} \geq \frac{1}{6}\,, \quad p_2^{(m')} < \frac{1}{6}\,, \quad \text{and} \quad t_{22}^{(m')} = \frac{1}{2} \tag{11}$$

which implies $t_{11}^{(m')} = 1$ and $t_{12}^{(m')} = \frac{1}{2}$ by Lemma 2, if such m' exists; otherwise define $m' = m_n'$. In what follows we will show how to modify P_n below level m' in order to fulfill condition (10) for $k = m', \ldots, d_n$ at the cost of weakening the assumption (8) which will hold only for every $\mathbf{a} \in \mathcal{M}_n^{c+2}$. In particular, we will obtain ${t'}_{12}^{(m')} = 0$ which breaks (11) (cf. (5)). This modification procedure is then repeated every time for the new last m' satisfying (11) until $m' = m_n'$ inclusive, which is performed at most $c+1$ times according to (6). After that P_n' is produced which satisfies (7), (9), and (10).

For every level $k = m', \ldots, d_n$ denote

$$V_1^{(k)} = \begin{cases} \{v_1^{(k)}, v_2^{(k)}\} & \text{if} \quad p_2^{(k)} \geq \frac{1}{6} \\ \{v_1^{(k)}\} & \text{if} \quad p_2^{(k)} < \frac{1}{6} \end{cases} \quad \text{and} \quad V_3^{(k)} = \{v_1^{(k)}, v_2^{(k)}, v_3^{(k)}\} \setminus V_1^{(k)}\,. \tag{12}$$

In addition, define formally $V_3^{(m'-1)} = \{v_2^{(m'-1)}, v_3^{(m'-1)}\}$.

Lemma 3. *For every $k = m'+1, \ldots, d_n$, there is no edge leading from $V_1^{(k-1)}$ to $V_3^{(k)}$.*

Proof. Let $m' < k \leq d_n$. We will first observe that no edge leads from $V_1^{(k-1)}$ to $v_3^{(k)}$. It follows from Lemma 2.i that there is no edge from $v_1^{(k-1)}$ to $v_3^{(k)}$. If $v_2^{(k-1)} \in V_1^{(k-1)}$ then $p_2^{(k-1)} \geq \frac{1}{6}$ which means no edge from node $v_2^{(k-1)}$ to $v_3^{(k)}$ according to Lemma 2.ii. Further assume $v_2^{(k)} \in V_3^{(k)}$ and we will show that no edge leads from $V_1^{(k-1)}$ to $v_2^{(k)}$. Thus $p_2^{(k)} < \frac{1}{6}$ which guarantees no edge from node $v_1^{(k-1)}$ to $v_2^{(k)}$ by Lemma 2.iii. If $v_2^{(k-1)} \in V_1^{(k-1)}$, that is $p_2^{(k-1)} \geq \frac{1}{6}$, then there is no edge from $v_2^{(k-1)}$ to $v_2^{(k)}$ by Lemma 2.iv and by the fact that m' is the last level satisfying (11). □

Clearly, all sinks from $V_1^{(d_n)}$ have label 1 according to (7) and (12). Hence, it follows from Lemma 3 and (8) that

$$\mathcal{M}_n^{c+3} \subseteq \bigcup_{v \in V_3^{(k)}} M(v) \quad \text{for every} \quad k = m', \dots, d_n \,. \tag{13}$$

Suppose that on some level $m' \leq k \leq d_n$, there is only a single edge leading from a node $u \in V_3^{(k-1)}$ to node $v \in V_1^{(k)}$. Let $x_i \in X_n$ be the input variable tested at node u. Suppose that $\mathbf{a}' \in M(u)$ for some input $\mathbf{a}' \in \mathcal{M}_n^{c+2}$, and consider the input $\mathbf{a} \in \Omega_1(\{\mathbf{a}'\}) \subseteq \mathcal{M}_n^{c+3}$ that differs from $\mathbf{a}'$ in the ith bit only. One of the computational paths for $\mathbf{a}$ and $\mathbf{a}'$ that coincide from source s up to node u due to P_n is read-once, then follows the edge from u to v and ends in a sink from $V_1^{(d_n)}$ labeled by 1 according to Lemma 3, which contradicts $P_n(\mathbf{a}) = P_n(\mathbf{a}') = 0$. It follows that $\mathcal{M}_n^{c+2} \subseteq M(u')$ for the other node $u' \in V_3^{(k-1)} \setminus \{u\}$ which means that, in this case, $V_3^{(k-1)} = \{u, u'\}$ contains two nodes and both edges outgoing from u' lead to $V_3^{(k)}$. Branching program P'_n is created from P_n by redirecting both edges outgoing from u to node $v_1^{(k)}$ whenever a single edge from $u \in V_3^{(k-1)}$ to $v \in V_1^{(k)}$ occurs, for all $m' \leq k \leq d_n$. Moreover, P'_n is normalized by using Lemma 1 where non-zero in-degrees of nodes $v_2^{(k)}, v_3^{(k)}$ are guaranteed by two edges outgoing from u'. After this modification, $t_{12}^{(k)}, t_{13}^{(k)} \in \{0, 1\}$ for every $k = m', \dots, d_n$ (cf. (10)), and $P'_n(\mathbf{a}') = 0$ for every $\mathbf{a}' \in \mathcal{M}_n^{c+2}$ (cf. (8)) while inequality (7) is preserved for P'_n due to $|P'^{-1}_n(0)| \leq |P^{-1}_n(0)|$.

In addition, we will further modify P'_n so that the function computed by P'_n is not changed while $p_2^{(k)} < \frac{1}{6}$ for every $k = m', \dots, d_n$ which implies $t_{11}^{(k)} = 1$ by Lemma 2.iii, and thus ensures (10) for every $k = m', \dots, d_n$. First recall from (11) that $p_2^{(m')} < \frac{1}{6}$ for $m' > m'_n$. Suppose there is a sequence of levels $k = k_1, \dots, k_2$ with $p_2^{(k)} \geq \frac{1}{6}$ where $m' \leq k_1 \leq k_2 \leq d_n$ such that $p_2^{(k_1-1)} < \frac{1}{6}$ if $k_1 > m'_n$, and $p_2^{(k_2+1)} < \frac{1}{6}$ if $k_2 < d_n$. This means $V_3^{(k_1-1)} = \{v_2^{(k_1-1)}, v_3^{(k_1-1)}\}$ and $V_3^{(k)} = \{v_3^{(k)}\}$ for every $k = k_1, \dots, k_2$. Hence, $\mathcal{M}_n^{c+2} \subseteq M(v_3^{(k)})$ for all $k_1 \leq k \leq k_2$ by (13), which implies $t_{33}^{(k)} = 1$ for every $k = k_1 + 1, \dots, k_2$. According to Lemma 3, transitions $\mathbf{T}_k$ for $k_1 < k \leq k_2$ can be deleted whereas levels $k = k_1 = k_2 \geq m'$ are identified. Moreover, we know for $k < d_n$ that

$t_{11}^{(k+1)} = t_{12}^{(k+1)} = 1$ and $t_{23}^{(k+1)} = t_{33}^{(k+1)} = \frac{1}{2}$ since there is no edge from $V_1^{(k)} = \{v_1^{(k)}, v_2^{(k)}\}$ to $V_3^{(k+1)} = \{v_2^{(k+1)}, v_3^{(k+1)}\}$ by Lemma 3.

Recall that if there is an edge from $V_3^{(k-1)}$ to $V_1^{(k)}$ then this must be a double edge leading to $v_1^{(k)}$ by the construction of P'_n. For the case when there is no edge leading from $V_3^{(k-1)} = \{v_2^{(k-1)}, v_3^{(k-1)}\}$ to $v_1^{(k)}$ which implies $t_{11}^{(k)} = t_{21}^{(k)} = \frac{1}{2}$ and $t_{32}^{(k)} = t_{33}^{(k)} = 1$, transition $\mathbf{T}_k$ is deleted so that node $v_1^{(k-1)}$ is replaced by $v_1^{(k)}$ and two copies of $v_3^{(k)}$ are substituted for $v_2^{(k-1)}, v_3^{(k-1)}$. For $k < d_n$, this means ${t'}_{11}^{(k)} = 1$ and ${t'}_{22}^{(k)} = {t'}_{23}^{(k)} = {t'}_{32}^{(k)} = {t'}_{33}^{(k)} = \frac{1}{2}$, and for $k = d_n$, the new sink $v_1^{(d_n-1)}$ gets label 1 whereas $v_2^{(d_n-1)}, v_3^{(d_n-1)}$ are labeled by 0.

Further assume a double edge from $v_j^{(k-1)} \in V_3^{(k-1)} = \{v_2^{(k-1)}, v_3^{(k-1)}\}$ to $v_1^{(k)}$ exists and thus $\mathcal{M}_n^{c+2} \subseteq M(v_\ell^{(k-1)})$ for the other node $v_\ell^{(k-1)} \in V_3^{(k-1)} \setminus \{v_j^{(k-1)}\}$ which implies there is also a double edge from $v_\ell^{(k-1)}$ to $v_3^{(k)}$ since $V_1^{(k)} = \{v_1^{(k)}, v_2^{(k)}\}$. For $k < d_n$, nodes $v_1^{(k)}$ and $v_2^{(k)}$ are merged into ${v'}_1^{(k)}$, that is ${t'}_{11}^{(k)} = {t'}_{1j}^{(k)} = 1$ and ${t'}_{11}^{(k+1)} = 1$, whereas node $v_3^{(k)}$ is split into two nodes ${v'}_2^{(k)}, {v'}_3^{(k)}$ each having one incoming edge from $v_\ell^{(k-1)}$ and the same outgoing edges, that is ${t'}_{2\ell}^{(k)} = {t'}_{3\ell}^{(k)} = \frac{1}{2}$ and ${t'}_{22}^{(k+1)} = {t'}_{23}^{(k+1)} = {t'}_{32}^{(k+1)} = {t'}_{33}^{(k+1)} = \frac{1}{2}$. For $k = d_n$, transition $\mathbf{T}_{d_n}$ is deleted and the new sinks in $v_1^{(d_n-1)}, v_j^{(d_n-1)}$ have the same label 1 whereas $v_\ell^{(d_n-1)}$ gets label 0. This completes the construction of P'_n satisfying (7), (9), and (10).

Lemma 4. *For every level $k = m'_n, \ldots, d_n$ it holds*

(i) $t_{32}^{(k)}, t_{33}^{(k)} \leq \frac{1}{2}$,
(ii) $t_{12}^{(k)} = 0$,
(iii) $t_{22}^{(k)} \geq \frac{1}{2}$.

Proof.

(i) On the contrary suppose there is a double edge to $v_3^{(k)}$ on some level $m'_n \leq k \leq d_n$ which must lead from $V_3^{(k-1)} = \{v_2^{(k-1)}, v_3^{(k-1)}\}$ according to Lemma 2.i. Moreover, there is no edge from $V_3^{(k-1)}$ to $v_1^{(k)}$ since this would have to be a double edge by (10) inducing zero in-degree of $v_2^{(k)}$ which contradicts the fact that P'_n is normalized. Similarly, a double edge leading to $v_2^{(k)}$ would give rise to the identity transition possibly after exchanging $v_2^{(k)}$ and $v_3^{(k)}$. Hence, there is only a single edge from $V_3^{(k-1)}$ to $v_2^{(k)}$ implying $p_2^{(k)} \leq \frac{1}{2} p_2^{(k-1)}$ while the remaining three edges from $V_3^{(k-1)}$ (including the double edge) lead to $v_3^{(k)}$ implying $p_3^{(k)} > \frac{1}{2} p_2^{(k-1)}$, which contradicts $p_2^{(k)} \geq p_3^{(k)}$.

(ii) On the contrary suppose $t_{12}^{(k)} > 0$ on some level $m'_n \leq k \leq d_n$. We know $k > m'_n$ by assumption (5), and hence, $t_{11}^{(k)} = t_{11}^{(k-1)} = 1$ and $t_{12}^{(k)} = 1$ from (10). It follows that $\mathcal{M}_n^2 \subseteq M(v_2^{(k-2)}) \cup M(v_3^{(k-2)})$ according to (9) (cf. (13)). Thus let $u \in V_3^{(k-2)} = \{v_2^{(k-2)}, v_3^{(k-2)}\}$ be a node such that $\mathbf{a} \in M(u)$ for some $\mathbf{a} \in \mathcal{A}_n$. Suppose there is an edge leading from u to $v_1^{(k-1)}$ or to $v_2^{(k-1)}$ which are both connected via a double edge to $v_1^{(k)}$. Then there is an input vector $\mathbf{a}' \in \Omega_1(\{\mathbf{a}\}) \subseteq \mathcal{M}_n^2$ whose computational path coincides from source s up to node u with that for $\mathbf{a}$, then continues via $v_1^{(k-1)}$ or $v_2^{(k-1)}$ to $v_1^{(k)}$, and ends in sink $v_1^{(d_n)}$, which contradicts $P'_n(\mathbf{a}') = 0$. Hence, there must be a double edge from u to $v_3^{(k-1)}$ which is a contradiction to (i).

(iii) We know $t_{32}^{(k)} \leq \frac{1}{2}$ and $t_{12}^{(k)} = 0$ from (i) and (ii), respectively, which implies $t_{22}^{(k)} \geq \frac{1}{2}$. □

5 Asymptotic Analysis

Lemma 5. *The sink $v_2^{(d_n)}$ has label 0.*

Proof. Let $u \in V_3^{(d_n-1)} = \{v_2^{(d_n-1)}, v_3^{(d_n-1)}\}$ be a node labeled by $x_i \in X_n$ such that $\mathbf{a}, \mathbf{a}' \in M(u)$ for some $\mathbf{a} \in \mathcal{A}_n$ where $\mathbf{a}' \in \Omega_1(\{\mathbf{a}\}) \subseteq \mathcal{M}_n^2$ differs from $\mathbf{a}$ in the ith bit. Both edges outgoing from u must lead to a sink labeled by 0 due to $P_n(\mathbf{a}) = P_n(\mathbf{a}') = 0$. Since a double edge to $v_3^{(d_n)}$ breaks Lemma 4.i there must be an edge leading from node u to the sink $v_2^{(d_n)}$, and hence, $v_2^{(d_n)}$ has label 0. □

For any level $m'_n < r \leq d_n$ such that $t_{13}^{(r)} = 1$ denote by $h_r \geq 0$ the maximum number of levels above r satisfying $t_{22}^{(r-h)} = 1$ and $t_{23}^{(r-h)} = t_{33}^{(r-h)} = \frac{1}{2}$ for every $h = 1, \ldots, h_r$.

Lemma 6. *There exists level $m'_n + h_r + 2 \leq r \leq d_n$ such that $t_{13}^{(r)} = 1$ and $h_r < \log_2 n$.*

Proof. Denote by $\ell \geq m'_n + 1$ the level that meets $t_{22}^{(\ell)} = \frac{1}{2}$ and $t_{22}^{(k)} = 1$ for $k = m'_n + 1, \ldots, \ell - 1$, which implies $p_2^{(\ell-1)} = p_2^{(m'_n)}$. Thus, $p_2^{(\ell)} + p_3^{(\ell)} \geq p_2^{(\ell-1)} = p_2^{(m'_n)} \geq p_2^{(m'_n-1)}/2 \geq \delta/2$ according to Lemma 4.ii and (4). It follows from (7), (10) and Lemma 4.ii that a level $\ell < r \leq d_n$ exists such that $t_{13}^{(r)} = 1$. Moreover, $r - h_r > \ell$ by definition of h_r since $t_{22}^{(\ell)} = \frac{1}{2}$, which implies $r \geq \ell + h_r + 1 \geq m'_n + h_r + 2$. Let $m'_n + h_{r_1} + 2 \leq r_1 \leq r_2 \leq d_n$ be the least and greatest levels, respectively, such that $t_{13}^{(r_1)} = t_{13}^{(r_2)} = 1$.

In addition, we know that

$$p_2^{(r_1-h_{r_1}-1)} + p_3^{(r_1-h_{r_1}-1)} = p_2^{(\ell)} + p_3^{(\ell)} \geq \frac{\delta}{2} \tag{14}$$

and for any level $m'_n + h_r + 2 \leq r \leq d_n$ such that $t_{13}^{(r)} = 1$ it holds that

$$p_2^{(r)} + p_3^{(r)} = p_2^{(r-h_r-1)} + p_3^{(r-h_r-1)} - \frac{p_3^{(r-h_r-1)}}{2^{h_r}} > \left(p_2^{(r-h_r-1)} + p_3^{(r-h_r-1)}\right)\left(1 - \frac{1}{2^{h_r}}\right). \tag{15}$$

On the contrary suppose that $h_r \geq \log_2 n$ for all levels $m'_n + h_r + 2 \leq r \leq d_n$ such that $t_{13}^{(r)} = 1$. Thus,

$$\frac{|P_n^{-1}(0)|}{2^n} \geq p_2^{(d_n)} \geq \frac{1}{2}\left(p_2^{(d_n)} + p_3^{(d_n)}\right) = \frac{1}{2}\left(p_2^{(r_2)} + p_3^{(r_2)}\right) \geq$$

$$\frac{1}{2}\left(p_2^{(r_1-h_{r_1}-1)} + p_3^{(r_1-h_{r_1}-1)}\right)\left(1 - \frac{1}{2^{\log_2 n}}\right)^{\frac{d_n}{\log_2 n}} \geq \frac{\delta}{4}\left(1 - \frac{1}{n}\right)^{\frac{n}{\log_2 n}} \tag{16}$$

according to Lemma 5, (10), Lemma 4.ii, (14), and (15). By introducing the inequality

$$1 > \left(1 - \frac{1}{n}\right)^{\frac{n}{\log_2 n}} > 1 - \frac{1}{n} \cdot \frac{n}{\log_2 n} = 1 - \frac{1}{\log_2 n} \tag{17}$$

into (16) we obtain

$$\frac{|P_n^{-1}(0)|}{2^n} > \frac{\delta}{4}\left(1 - \frac{1}{\log_2 n}\right) \tag{18}$$

which contradicts (7). □

Consider level $m'_n + h_r + 2 \leq r \leq d_n$ such that $t_{13}^{(r)} = 1$ and $h_r < \log_2 n$, which exists according to Lemma 6. By definition of $\mathcal{A}_n$ there is a vector $\mathbf{a} \in \mathcal{A}_n$ such that if $\mathbf{a} \in M(v_3^{(r-h_r-1)})$ then the computational path for input $\mathbf{a}$ traverses nodes $v_3^{(r-h_r-1)}, v_3^{(r-h_r)}, \ldots, v_3^{(r-1)}, v_1^{(r)}$. It follows from the definition of h_r and Lemma 4.iii that $t_{22}^{(r-h_r-1)} = \frac{1}{2}$ implying $t_{32}^{(r-h_r-1)} = \frac{1}{2}$ by Lemma 4.ii. In addition, $t_{22}^{(r-h_r-2)} \geq \frac{1}{2}$ by Lemma 4.iii. Furthermore, either $t_{13}^{(r-h_r-2)} = 1$ implying $\mathbf{a} \in \mathcal{M}_n^2 \subseteq M(v_2^{(r-h_r-3)})$, or $t_{23}^{(r-h_r-2)} \geq \frac{1}{2}$ according to Lemma 4.i. which gives $\mathbf{a} \in \mathcal{M}_n^2 \subseteq M(v_2^{(r-h_r-3)}) \cup M(v_3^{(r-h_r-3)})$. In both cases, an input $\mathbf{a}' \in \Omega_2(\{\mathbf{a}\}) \subseteq \mathcal{M}_n^2$ exists whose computational path from source s up to level $r - h_r - 3$ coincides with that for $\mathbf{a}$, and then continues via $v_2^{(r-h_r-2)}$ to $v_3^{(r-h_r-1)}$, further traversing nodes $v_3^{(r-h_r)}, \ldots, v_3^{(r-1)}, v_1^{(r)}$, which contradicts $P_n(\mathbf{a}') = 0$. Thus assumption (7) leads to a contradiction which completes the proof of Theorem 2. □

Proof (Theorem 1). According to Theorem 2 it suffices to show that simple $\{P_n\}$ is $(0, \frac{1}{24})$-restricted. Consider first the case when there is a level $m_n < m' < d_n$ satisfying (11) and take the last such m' in P_n. By Lemma 2 we know that $t_{11}^{(m')} = 1$ and $t_{12}^{(m')} = t_{22}^{(m')} = \frac{1}{2}$, and hence, $t_{33}^{(m')} = \frac{1}{2}$ due to P_n is simple. Clearly, $\mathcal{M}_n^3 \subseteq M(v_2^{(m'-1)}) \cup M(v_3^{(m'-1)})$, and $\mathcal{M}_n^2 \subseteq M(v_3^{(m'-1)})$ from Lemma 3 and $t_{12}^{(m')} = \frac{1}{2}$, which implies $t_{23}^{(m')} = \frac{1}{2}$. It follows that $t_{12}^{(m'+1)} = 0$ since otherwise an input $\mathbf{a} \in \mathcal{M}_n^1$ would exist whose computational path leads through $v_2^{(m'-1)}$ or $v_3^{(m'-1)}$ and continues via $v_2^{(m')}$ to $v_1^{(m'+1)}$ contradicting $P_n(\mathbf{a}) = 0$. Thus define $m'_n = m' + 1$ which confirms $\{P_n\}$ is $(0, \frac{1}{24})$-restricted due to even $p_2^{(m'_n-1)} \geq \frac{1}{12}$ from (11).

For the case when (11) does not happen below m_n we employ the reduction from Section 4 for $m' = m_n + 1$, which ensures (10) for $k = m_n + 1, \ldots, d_n$, and $\mathcal{M}_n^2 \subseteq M(v_2^{(m_n)}) \cup M(v_3^{(m_n)})$. Clearly, there is at least one edge leading from a node $u \in V_3^{(m_n)} = \{v_2^{(m_n)}, v_3^{(m_n)}\}$ to $v_2^{(m_n+1)}$ implying $p_2^{(m_n+1)} \geq \frac{1}{24}$ due to $p_2^{(m_n)} \geq p_3^{(m_n)} \geq \frac{1}{12}$. On the contrary suppose $t_{12}^{(m_n+2)} > 0$. Hence, there is no edge from the other node $u' \in V_3^{(m_n)} \setminus \{u\}$ to $v_2^{(m_n+1)}$ and $\mathcal{A}_n \subseteq M(u')$ which excludes an edge from u' to $v_1^{(m_n+1)}$ according to (10). Thus, there must be a double edge from u' to $v_3^{(m_n+1)}$. Similarly, the second edge outgoing from u cannot be connected to $v_1^{(m_n+1)}$ while a double edge from u to $v_2^{(m_n+1)}$ or an edge from u to $v_3^{(m_n+1)}$ are also impossible due to P_n is normalized, which is a contradiction. Thus, $t_{12}^{(m_n+2)} = 0$, and $m'_n = m_n + 2$ confirms $\{P_n\}$ is $(0, \frac{1}{24})$-restricted. $\square$

Acknowledgment

The authors would like to thank Pavel Pudlák for pointing out the problem discussed in this paper and Petr Savický for stimulating collaboration in the early stages of this research.

References

1. Alon, N., Goldreich, O., Håstad, J., and Peralta, R.: Simple Constructions of Almost k-wise Independent Random Variables. Journal of Random structures and Algorithms **3** (3) (1992) 289–304
2. Goldreich, O. and Wigderson, A.: Improved Derandomization of BPP Using a Hitting Set Generator. Proceedings of the RANDOM'99 Third International Workshop on Randomization and Approximation Techniques in Computer Science, LNCS **1671**, Springer-Verlag, Berlin (1999) 131–137
3. Wegener, I.: Branching Programs and Binary Decision Diagrams—Theory and Applications. SIAM Monographs on Discrete Mathematics and Its Applications, SIAM, Philadelphia, PA (2000)