# A Characterization of Hitting Sets for 1-Branching Programs of Width 3 (Revised Version)

Šíma, Jiří
2009

**Institute of Computer Science**
**Academy of Sciences of the Czech Republic**

# A Characterization of Hitting Sets for 1-Branching Programs of Width 3 (Revised Version)

Jiří Šíma, Stanislav Žák

Technical report No. 1054

November 2009

Pod Vodárenskou věží 2, 182 07 Prague 8, phone: +420 266 053 111, fax: +420 286 585 789,
e-mail:sima@cs.cas.cz

Institute of Computer Science
Academy of Sciences of the Czech Republic

# A Characterization of Hitting Sets for 1-Branching Programs of Width 3 (Revised Version)

Jiří Šíma[1], Stanislav Žák[2]

Technical report No. 1054

November 2009

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. In this paper, we characterize the hitting sets for read-once branching programs of width 3 by a necessary and (in a certain sense) sufficient so-called richness condition which is independent of a rather technical formalism of branching programs. This result can substantially help in looking for polynomial time constructions of hitting sets for the underlying model which is illustrated by an example of a set that satisfies a special case of the richness condition.

Keywords:
derandomization, hitting set, read-once branching programs, bounded width

[1] Research partially supported by project 1M0545 of The Ministry of Education of the Czech Republic and the Institutional Research Plan AV0Z10300504.

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

**Acknowledgment:** The authors would like to thank Pavel Pudlák for pointing out the problem of hitting sets for width-3 1-branching programs.

# 1 Introduction

An $\varepsilon$-hitting set for a class of Boolean functions of $n$ variables is a set $H \subseteq \{0,1\}^n$ 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 $\varepsilon$, then there is also an input in $H$ 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 $\varepsilon$-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 models are investigated. In our previous work [3], we have made the first step for finding a polynomial time constructible hitting set for read-once branching programs of width 3. Although this computational model seems to be relatively weak we were able to prove the result by using the construction from [1] only if an additional, rather technical restriction is imposed on the branching programs confirming the hardness of the original problem. In particular, this restriction is met when one from all the patterns of level-to-level transitions in a normalized form of width-3 1-branching programs is excluded (see [3] for further details).

In this paper, we characterize the hitting sets for 1-branching programs of width 3 by a so-called *richness* condition which is independent of a rather technical formalism of branching programs. We prove that this richness condition is necessary and (in a certain sense) sufficient, which can help in looking for polynomial time constructions of hitting sets for read-once branching programs of width 3. For example, a special case of this condition is satisfied by a set constructed by Alon, Goldreich, Håstad, and Peralta in their paper [1]. By the result in this paper we know that the validity of the full richness condition for this set or its extension would provide a polynomial time constructible hitting set for read-once branching programs of width 3, which is still left for further research.

The paper is organized as follows. After a brief review of basic definitions regarding branching programs in Section 2 (see [4] for more information), the richness condition is formulated and proved to be necessary in Section 3. The main result that the richness condition is sufficient for a set to be a hitting set for width-3 1-branching programs is presented in Section 4. The subsequent four sections are devoted to the technical proof. We will conclude by discussion of future work in Section 9.

# 2 Normalized Width-$d$ 1-Branching Programs

A *branching program* $P$ 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 $P$ computes Boolean function $P : \{0,1\}^n \longrightarrow \{0,1\}$ as follows. The computational path of $P$ 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 $P(\mathbf{a})$. Denote by $P^{-1}(a) = \{\mathbf{a} \in \{0,1\}^n \,|\, P(\mathbf{a}) = a\}$ the set of inputs for which $P$ outputs $a \in \{0,1\}$. 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 $P$ 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 $P$ creates level 0 whereas the last level is composed of all sinks.

The number of levels decreased by 1 equals the *depth* of $P$ which is the length of its longest path, and the maximum number of nodes on one level is called the *width* of $P$.

For a 1-branching program $P$ of width $w$ define a $w \times w$ *transition matrix* $T_k$ 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 $v_j^{(k-1)}$ $(1 \leq j \leq w)$ on level $k-1$ of $P$ to node $v_i^{(k)}$ $(1 \leq i \leq w)$ 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, $\sum_{i=1}^{w} t_{ij}^{(k)} = 1$ since this sum equals the half of the out-degree of inner node $v_j^{(k-1)}$, and $2 \cdot \sum_{j=1}^{w} t_{ij}^{(k)}$ is the in-degree of node $v_i^{(k)}$. Denote by a column vector $\mathbf{p}^{(k)} = (p_1^{(k)}, \ldots, p_w^{(k)})^{\mathsf{T}}$ the *distribution* of inputs among $w$ nodes on level $k$ of $P$, that is, $p_i^{(k)}$ is the probability that a random input is tested at node $v_i^{(k)}$, which equals the ratio of the number 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 $\bigcup_{i=1}^{w} M(v_i^{(k)}) = \{0,1\}^n$ and $\sum_{i=1}^{w} p_i^{(k)} = 1$ 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 $T_k$ as

$$\mathbf{p}^{(k)} = T_k \cdot \mathbf{p}^{(k-1)} \,. \tag{2.1}$$

It is because the ratio of inputs coming to node $v_i^{(k)}$ from previous-level nodes equals $p_i^{(k)} = \sum_{j=1}^{w} t_{ij}^{(k)} p_j^{(k-1)}$ 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 $P$ of width $w$ is *normalized* if $P$ has the minimum depth among the programs computing the same function (e.g. $P$ does not contain the identity transition $T_k$) and satisfies

$$1 > p_1^{(k)} \geq p_2^{(k)} \geq \cdots \geq p_w^{(k)} > 0 \tag{2.2}$$

for every $k \geq \log_2 w$. Obviously, condition (2.2) can always be satisfied by permuting the nodes at each level of $P$:

**Lemma 1 ([3])** *Any width-$w$ 1-branching program can be normalized.*

In the sequel, we confine ourselves to the normalized 1-branching programs of width $w = 3$. Any such program $P$ 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

$$p_1^{(k)} > \frac{1}{3}\,, \qquad p_2^{(k)} < \frac{1}{2}\,, \qquad p_3^{(k)} < \frac{1}{3} \tag{2.3}$$

for every level $2 \leq k \leq d$ where $d \leq n$ is the depth of $P$.

# 3 A Necessary Condition

Let $\mathcal{P}$ be a class of branching programs and $\varepsilon > 0$ be a real constant. A set of input strings $H \subseteq \{0,1\}^*$ is called an *$\varepsilon$-hitting set* for class $\mathcal{P}$ if for sufficiently large $n$, for every branching program $P \in \mathcal{P}$ with $n$ input variables

$$\frac{|P^{-1}(1)|}{2^n} \geq \varepsilon \quad \text{implies} \quad (\exists\, \mathbf{a} \in H \cap \{0,1\}^n)\, P(\mathbf{a}) = 1\,. \tag{3.1}$$

Furthermore, we say that a set $A \subseteq \{0,1\}^*$ is *$\varepsilon$-rich* if for sufficiently large $n$, for any index set $I \subseteq \{1,\ldots,n\}$, and for any partition $\{Q_1,\ldots,Q_q,R_1,\ldots,R_r\}$ of $I$ where $q \geq 0$ and $r \geq 0$, it holds that if

$$\left(1 - \prod_{j=1}^{q}\left(1 - \frac{1}{2^{|Q_j|}}\right)\right) \times \prod_{j=1}^{r}\left(1 - \frac{1}{2^{|R_j|}}\right) \geq \varepsilon\,, \tag{3.2}$$

then for any $\mathbf{c} \in \{0,1\}^n$ there exists $\mathbf{a} \in A \cap \{0,1\}^n$ such that

$$(\exists\, j \in \{1,\ldots,q\})\,(\forall\, i \in Q_j)\, a_i = c_i \tag{3.3}$$

$$\text{and} \quad (\forall\, j \in \{1,\ldots,r\})\,(\exists\, i \in R_j)\, a_i \neq c_i\,. \tag{3.4}$$

Particularly for $q = 0$ inequality (3.2) reads

$$\prod_{j=1}^{r} \left(1 - \frac{1}{2^{|R_j|}}\right) \geq \varepsilon \tag{3.5}$$

and conjunction (3.3) and (3.4) reduces to the second conjunct (3.4), while for $r = 0$ inequality (3.2) reads

$$1 - \prod_{j=1}^{q} \left(1 - \frac{1}{2^{|Q_j|}}\right) \geq \varepsilon \tag{3.6}$$

and conjunction (3.3) and (3.4) reduces to the first conjunct (3.3).

**Theorem 1** *Every $\varepsilon$-hitting set for the class of read-once branching programs of width 3 is $\varepsilon$-rich.*

**Proof:** Let $H$ be an $\varepsilon$-hitting set for the class of read-once branching programs of width 3 and on the contrary assume that $H$ is not $\varepsilon$-rich. This means that for infinitely many $n$ there is an index set $I \subseteq \{1, \ldots, n\}$, a partition $\{Q_1, \ldots, Q_q, R_1, \ldots, R_r\}$ of $I$ satisfying (3.2), and a string $\mathbf{c} \in \{0,1\}^n$ such that every $\mathbf{a} \in H \cap \{0,1\}^n$ meets

$$(\forall\, j \in \{1, \ldots, q\})\, (\exists\, i \in Q_j)\, a_i \neq c_i \tag{3.7}$$

$$\text{or} \quad (\exists\, j \in \{1, \ldots, r\})\, (\forall i \in R_j)\, a_i = c_i\,. \tag{3.8}$$

We will use this partition and $\mathbf{c}$ for constructing a read-once branching program $P$ of width 3 such that

$$\frac{\left|P^{-1}(1)\right|}{2^n} \geq \varepsilon \quad \text{and} \quad (\forall\, \mathbf{a} \in H \cap \{0,1\}^n)\, P(\mathbf{a}) = 0\,, \tag{3.9}$$

which contradicts the assumption that $H$ is an $\varepsilon$-hitting set according to (3.1).

For the simplicity reason we assume here only the general case when $q \geq 1$ and $r \geq 1$, while the proof for $q = 0$ or $r = 0$ is similar. The branching program $P$ is composed of $q + r$ consecutive blocks corresponding to the partition classes $Q_1, \ldots, Q_q, R_1, \ldots, R_r$ which determine the indices of variables that are tested within these blocks. The block corresponding to $Q_j$ for $j \in \{1, \ldots, q\}$ starts on level $k_j = \sum_{\ell=1}^{j-1} |Q_\ell|$ of $P$ (e.g. formally $k_1 = 0$) with a transition satisfying $t_{11}^{(k_j+1)} = t_{21}^{(k_j+1)} = \frac{1}{2}$, followed by a sequence of transitions that meet $t_{11}^{(k)} = 1$ and $t_{12}^{(k)} = t_{22}^{(k)} = \frac{1}{2}$ for every $k = k_j + 2, \ldots, k_j + |Q_j|$, except for the boundary level $k_q + |Q_q| = k_{q+1}$, which is defined below. In addition, there is a parallel double-edge path leading from the node $v_3^{(k_2+1)}$ on level $k_2 + 1$ up to the node $v_3^{(k_{q+1}-1)}$, and thus $t_{33}^{(k)} = 1$ for every $k = k_2 + 2, k_2 + 3, \ldots, k_{q+1} - 1$. This path is wired up by $q - 2$ double edges coming from nodes $v_2^{(k_j)}$, that is $t_{32}^{(k_j+1)} = 1$ for every $j = 2, \ldots, q$. Finally, a special boundary transition is defined on level $k_{q+1}$ as $t_{31}^{(k_{q+1})} = t_{13}^{(k_{q+1})} = 1$ and $t_{12}^{(k_{q+1})} = t_{32}^{(k_{q+1})} = \frac{1}{2}$. Note that there are only two nodes $v_1^{(k_{q+1})}, v_3^{(k_{q+1})}$ on the boundary level $k_{q+1}$. Furthermore, $P$ continues analogously with blocks corresponding to $R_j$ for $j = 1, \ldots, r$, each starting on level $k_{q+j} = k_{q+1} + \sum_{\ell=1}^{j-1} |R_\ell|$ (e.g. formally $k_{q+r+1} = d$ is the depth of $P$) with the transition satisfying $t_{11}^{(k_{q+j}+1)} = t_{21}^{(k_{q+j}+1)} = \frac{1}{2}$, followed by $t_{11}^{(k)} = 1$ and $t_{12}^{(k)} = t_{22}^{(k)} = \frac{1}{2}$ for every $k = k_{q+j} + 2, \ldots, k_{q+j} + |R_j|$. Also the parallel double-edge path leading from the node $v_3^{(k_{q+1})}$ up to the sink $v_3^{(d)}$ is introduced and wired in $P$, that is, $t_{33}^{(k)} = 1$ for every $k = k_{q+1} + 1, \ldots, d$ and $t_{32}^{(k_{q+j}+1)} = 1$ for every $j = 2, \ldots, r$. The branching program $P$ then queries the value of each variable $x_i$ such that $i \in Q_j$ for some $j \in \{1, \ldots, q\}$ or $i \in R_j$ for some $j \in \{1, \ldots, r\}$ only on one level $k \in \{k_j, \ldots, k_{j+1} - 1\}$ or $k \in \{k_{q+j}, \ldots, k_{q+j+1} - 1\}$, respectively (i.e. the nodes on level $k$ are labeled with $x_i$), while the single edge leading to $v_2^{(k+1)}$ (or to $v_1^{(k_{q+1})}$ for $k = k_{q+1} - 1$) on the subsequent level $k + 1$ gets label $c_i$. Finally, the sink $v_1^{(d)}$ gets label 1 whereas the sinks $v_2^{(d)}$, $v_3^{(d)}$ are labeled with the output 0, which completes the construction of $P$.

Clearly, $P$ is a read-once branching program of width 3. The probability that an input reaches the node $v_3^{(k_{q+1})}$ on the boundary level $k_{q+1}$ can simply be computed as

$$p_3^{(k_{q+1})} = \prod_{j=1}^{q} \left(1 - \frac{1}{2^{|Q_j|}}\right) \tag{3.10}$$

while the probability of the complementary event that an input reaches $v_1^{(k_q+1)}$ equals $p_1^{(k_q+1)} = 1 - p_3^{(k_q+1)}$. Therefore, the probability that $P$ outputs 1 can be expressed and lower bounded by (3.2):

$$\frac{\left|P^{-1}(1)\right|}{2^n} = p_1^{(d)} = \left(1 - \prod_{j=1}^{q}\left(1 - \frac{1}{2^{|Q_j|}}\right)\right) \times \prod_{j=1}^{r}\left(1 - \frac{1}{2^{|R_j|}}\right) \geq \varepsilon \,. \tag{3.11}$$

Furthermore, we split $H \cap \{0,1\}^n = A_1 \cup A_2$ into two parts so that every $\mathbf{a} \in A_1$ satisfies the first term (3.7) of the underlying disjunction whereas every $\mathbf{a} \in A_2 = H \setminus A_1$ meets the second term (3.8). Thus, for any input $\mathbf{a} \in A_1$ and for every $j \in \{1, \ldots, r\}$ the block of $P$ corresponding to $Q_j$ contains a level $k \in \{k_j, \ldots, k_{j+1} - 1\}$ where variable $x_i$ is tested such that $a_i \neq c_i$. This ensures that the computational path for $\mathbf{a} \in A_1$ reaches $v_3^{(k_q+1)}$ and further continues through $v_3^{(k_{q+1}+1)}, \ldots, v_3^{(d)}$, which gives $P(\mathbf{a}) = 0$ for every $\mathbf{a} \in A_1$. Similarly, for any input $\mathbf{a} \in A_2$ there exists a block of $P$ corresponding to $R_j$ for some $j \in \{1, \ldots, r\}$ such that the computational path for $\mathbf{a}$ traverses nodes $v_1^{(k_{q+j})}, v_2^{(k_{q+j}+1)}, v_2^{(k_{q+j}+1)}, \ldots, v_2^{(k_{q+j}+|R_j|)}$. For $j < r$ this path continues through $v_3^{(k_{q+j+1}+1)}, \ldots, v_3^{(d)}$ whereas for $j = r$ it terminates at $v_2^{(d)}$, which gives $P(\mathbf{a}) = 0$ in both cases. Hence, $P$ satisfies (3.9), which completes the proof. □

# 4 A Sufficient Condition

For a given set $A \subseteq \{0,1\}^*$ and a natural constant $c \geq 0$ define $\Omega_c(A) = \{\mathbf{a}' \,|\, (\exists\, \mathbf{a} \in A)\, |\mathbf{a}| = |\mathbf{a}'| \,\&\, h(\mathbf{a}, \mathbf{a}') \leq c\}$ where $|\mathbf{a}|$ denotes the length of string $\mathbf{a}$ and $h(\mathbf{a}, \mathbf{a}')$ is the number bits in which $\mathbf{a}$ and $\mathbf{a}'$ differ (the Hamming distance).

**Theorem 2** *Denote $\delta = \sqrt{\frac{12}{13}}$. If $A$ is $(\delta^{11} - \delta^{12})\varepsilon^{12}$-rich for $\varepsilon > \delta$ then $H = \Omega_3(A)$ is an $\varepsilon$-hitting set for the class of read-once branching programs of width 3.*

**Proof:** After using Lemma 1, assume that a normalized read-once branching program $P$ of width 3 with sufficiently many input variables $n$ meets

$$\frac{\left|P^{-1}(1)\right|}{2^n} \geq \varepsilon > \delta > \frac{11}{12} \,. \tag{4.1}$$

We will prove that there exists $\mathbf{a} \in H$ such that $P(\mathbf{a}) = 1$. On the contrary, suppose that $P(\mathbf{a}) = 0$ for every $\mathbf{a} \in H$.

Clearly, sink $v_1^{(d)}$ of $P$ is labeled with 1 since $p_1^{(d)} > \frac{1}{3}$ due to (2.3) and $|P^{-1}(0)|/2^n < \frac{1}{12}$ according to (4.1). We will assume without loss of generality that sink $v_2^{(d)}$ of $P$ is labeled with 1 and $t_{11}^{(d)} = t_{21}^{(d)} = \frac{1}{2}$. In particular, if $v_2^{(d)}$ gets label 0, then $t_{11}^{(d)} = 1$ according to (4.1) since $p_1^{(d-1)} > \frac{1}{3}$, and one edge outgoing from $v_1^{(d-1)}$ can be redirected to $v_2^{(d)}$, while all the edges leading to $v_2^{(d)}$ are redirected to $v_3^{(d)}$ which is labeled with 0. If $v_3^{(d)}$ was labeled with 1, then the edges that originally led to $v_3^{(d)}$ are redirected to $v_1^{(d)}$. The case of $t_{21}^{(d)} = 1$ when $v_2^{(d)}$ gets label 1 can be resolved similarly. Moreover, we will show that $t_{32}^{(d)} > 0$. Thus, suppose $t_{32}^{(d)} = 0$, which implies $t_{33}^{(d)} > 0$. For $t_{13}^{(d)} + t_{23}^{(d)} > 0$ the computational path for an input $\mathbf{a}' \in M(v_3^{(d-1)}) \cap \Omega_1(A) \subseteq H$ that differs from $\mathbf{a} \in A$ ($P(\mathbf{a}) = 0$) in the $i$th bit such that $v_3^{(d-1)}$ is labeled with $x_i$ would end up in the sink labeled with 1, and hence $P(\mathbf{a}') = 1$. For $t_{33}^{(d)} = 1$, on the other hand, we could shorten $P$ by removing the last level $d$ without changing its function. We will further analyze $P$ by using the following lemma whose assumptions are trivially satisfied for $m = d$ according to (4.1).

**Lemma 2** *Let $m$ be a level of $P$ satisfying $t_{11}^{(m)} = t_{21}^{(m)} = \frac{1}{2}$, $t_{32}^{(m)} > 0$, and $p_3^{(m)} < \frac{1}{12}$. Further assume there is $\mathbf{a} \in A$ such that $P(\mathbf{a}') = 1$ for any input $\mathbf{a}' \in M(v_1^{(m)}) \cup M(v_2^{(m)})$ that agrees with $\mathbf{a}$ on the bits that are tested on the computational path for $\mathbf{a}'$ starting from level $m$ (in other words, if we put $\mathbf{a} \in A$ at node $v_1^{(m)}$ or $v_2^{(m)}$, then its onward computational path arrives to the sink labeled with 1). In addition, denote by $2 \leq \mu < m$ the least level of $P$ such that $t_{11}^{(\ell)} = 1$ for every $\ell = \mu + 1, \ldots, m - 1$. Then the following claims are true:*

**(i)** $3 < \mu < m - 1$.

**(ii)** *Define a* change-bit *path starting from $v \in \{v_2^{(k)}, v_3^{(k)}\}$ at level $\mu \le k < m$ to be a computational path of length at most 3 edges leading from $v$ to $v_1^{(\ell)}$ for some $k < \ell \le \min(k+3, m)$ or to $v_2^{(m)}$ for $m \le k+3$. Then there are no two simultaneous change-bit paths starting from $v_2^{(k)}$ and from $v_3^{(k)}$, respectively, at any level $\mu \le k < m$.*

**(iii)** *If $t_{12}^{(k+1)} > 0$ for some $\mu \le k < m$, then $t_{11}^{(\ell)} = t_{33}^{(\ell)} = 1$, $t_{12}^{(\ell)} = t_{22}^{(\ell)} = \frac{1}{2}$ for every $\ell = \mu+1, \ldots, k$, and $t_{12}^{(k+1)} = \frac{1}{2}$.*

**(iv)** *If $t_{13}^{(k+1)} > 0$ for some $\mu < k < m$, then one of the following four cases appears:*

*1. $t_{11}^{(k)} = t_{23}^{(k)} = 1$ and $t_{12}^{(k)} = t_{32}^{(k)} = \frac{1}{2}$,*

*2. $t_{11}^{(k)} = t_{23}^{(k)} = 1$ and $t_{22}^{(k)} = t_{32}^{(k)} = \frac{1}{2}$,*

*3. $t_{11}^{(k)} = t_{22}^{(k)} = 1$ and $t_{13}^{(k)} = t_{33}^{(k)} = \frac{1}{2}$,*

*4. $t_{11}^{(k)} = t_{22}^{(k)} = 1$ and $t_{23}^{(k)} = t_{33}^{(k)} = \frac{1}{2}$.*

*In addition, if $t_{23}^{(k)} = 1$ (case 1 or 2), then $t_{11}^{(\ell)} = t_{33}^{(\ell)} = 1$ and $t_{12}^{(\ell)} = t_{22}^{(\ell)} = \frac{1}{2}$ for every $\ell = \mu+1, \ldots, k-1$.*

**Proof:**

**(i)** For $\mu \le 3$, we would have an input $\mathbf{a}' \in M(v_1^{(\mu)}) \cap \Omega_3(A) \subseteq H$ which differs from the input $\mathbf{a} \in A$ satisfying the assumption of the lemma in at most three bits that are tested on the computational path for $\mathbf{a}'$ leading from the source $v_1^{(0)}$ to $v_1^{(\mu)}$, which gives $P(\mathbf{a}') = 1$ by $M(v_1^{(\mu)}) \subseteq M(v_1^{(m)}) \cup M(v_2^{(m)})$ and the assumption on $\mathbf{a}$. In addition, $t_{11}^{(m-1)} = 1$ because $t_{21}^{(m-1)} + t_{31}^{(m-1)} > 0$ implies $p_2^{(m-1)} > \frac{1}{6}$ and by $t_{32}^{(m)} > 0$ we get $p_3^{(m)} > \frac{1}{12}$, which is a contradiction.

**(ii)** Suppose there are two simultaneous change-bit paths starting from $v_2^{(k)}$ and from $v_3^{(k)}$, respectively, at some level $\mu \le k < m$, and let $\mathbf{a} \in A$ be the input satisfying the assumption of the lemma. Clearly, $\mathbf{a} \notin M(v_1^{(k)}) \subseteq M(v_1^{(m)}) \cup M(v_2^{(m)})$ since then $P(\mathbf{a}) = 1$ for $\mathbf{a} \in H$. Thus assume $\mathbf{a} \in M(v)$ for $v \in \{v_2^{(k)}, v_3^{(k)}\}$. Then there is an input $\mathbf{a}' \in M(v) \cap \Omega_3(A) \subseteq H$ which may differ from $\mathbf{a}$ only in the variables that are tested on the change-bit path starting from $v$ so that the computational path for $\mathbf{a}'$ follows this change-bit path. Hence, $\mathbf{a}' \in M(v_1^{(m)}) \cup M(v_2^{(m)})$ implying $P(\mathbf{a}') = 1$ due to $P$ is read-once. This completes the proof of (ii).

Denote by $v \in \{v_2^{(k)}, v_3^{(k)}\}$ a node at some level $\mu < k < m$ with the edge outgoing to $v_1^{(k+1)}$, and let $u$ be a node on level $k-1$ from which an edge leads to $v$ while $v' \in \{v_2^{(k)}, v_3^{(k)}\} \setminus \{v\}$ and $u' \in \{v_2^{(k-1)}, v_3^{(k-1)}\} \setminus \{u\}$ denote the other nodes. It follows from (ii) there is no edge from $u'$ to $v$ nor to $v_1^{(k)}$, which would establish two simultaneous change-bit paths starting from $v_2^{(k-1)}$ and from $v_3^{(k-1)}$, respectively. Hence, there must be a double edge from $u'$ to $v'$. Since $P$ is normalized, $u' = v_2^{(k-1)}$ and $v' = v_3^{(k)}$ cannot happen simultaneously. Moreover, the second edge from $u$ may lead either to $v_1^{(k)}$ or to $v'$ if $v' \ne v_3^{(k)}$. Now, the possible cases can be summarized:

**(iii)** For $t_{12}^{(k+1)} > 0$ we know $v = v_2^{(k)}$ and $v' = v_3^{(k)}$, which implies $t_{11}^{(k)} = t_{33}^{(k)} = 1$ and $t_{12}^{(k)} = t_{22}^{(k)} = \frac{1}{2}$. The proposition follows when this argument is applied recursively for $k$ replaced with $k-1$ etc. In addition, we will prove that $t_{12}^{(k+1)} < 1$ for $\mu \le k < m$. For $t_{12}^{(k+1)} = 1$ we would have $t_{23}^{(k+1)} = t_{33}^{(k+1)} = \frac{1}{2}$. For $k > \mu$ one could shorten $P$ by identifying level $k$ with $\mu$ without changing its function. For $k = \mu > 3$, on the other hand, there are at least two edges leading to $v_3^{(\mu)}$ because otherwise if only one edge leads to $v_3^{(\mu)}$ from $u \in \{v_1^{(\mu-1)}, v_2^{(\mu-1)}, v_3^{(\mu-1)}\}$, then either $\mathbf{a} \notin M(u)$, which means $\mathbf{a} \in M(v_1^{(\mu)}) \cup M(v_2^{(\mu)}) = M(v_1^{(\mu+1)}) \subseteq M(v_1^{(m)}) \cup M(v_2^{(m)})$

implying $P(\mathbf{a}) = 1$, or $\mathbf{a} \in M(u)$ providing $\mathbf{a}' \in \Omega_1(A) \subseteq H$ which may differ from $\mathbf{a}$ in the variable that is tested at $u$ so that $\mathbf{a}' \in M(v_1^{(\mu)}) \cup M(v_2^{(\mu)})$ implying $P(\mathbf{a}') = 1$. Hence, we can split $v_3^{(\mu)}$ into two nodes and merge $v_1^{(\mu)}$ and $v_2^{(\mu)}$ while preserving the function of $P$.

**(iv)** For $t_{13}^{(k+1)} > 0$ we know $v = v_3^{(k)}$ and $v' = v_2^{(k)}$ and the four cases listed in the proposition are obtained when the choice of $u \in \{v_2^{(k-1)}, v_3^{(k-1)}\}$ is combined with whether the second edge from $u$ leads to $v_1^{(k)}$ or to $v'$. In addition, the remaining part for case 1 and 2 follows from (iii). In particular, in case 2 there is a path from $v_2^{(k-1)}$ to $v_1^{(k+1)}$ via $v_3^{(k)}$, and a similar analysis applies for $v = v_2^{(k-1)}$ excluding two change-bit paths starting from $v_2^{(k-2)}$ and $v_3^{(k-2)}$, respectively. □

Let $\mu \leq \nu \leq m$ be the greatest level such that $t_{12}^{(\ell)} + t_{13}^{(\ell)} > 0$ for every $\ell = \mu + 1, \ldots, \nu$. From Lemma 2 it follows:

**Corollary 1** *There exists $\mu \leq \gamma \leq \nu$ such that*

1. $t_{11}^{(\ell)} = t_{33}^{(\ell)} = 1$ *and* $t_{12}^{(\ell)} = t_{22}^{(\ell)} = \frac{1}{2}$ *for* $\ell = \mu + 1, \ldots, \gamma - 1$ *(Lemma 2.iii),*

2. $t_{11}^{(\gamma)} = t_{23}^{(\gamma)} = 1$ *and* $t_{32}^{(\gamma)} = \frac{1}{2}$ *if* $\mu < \gamma < \nu$ *(case 1 of Lemma 2.iv),*

3. $t_{11}^{(\ell)} = t_{22}^{(\ell)} = 1$ *and* $t_{33}^{(\ell)} = \frac{1}{2}$ *for* $\ell = \gamma + 1, \ldots, \nu - 1$ *(case 3 of Lemma 2.iv),*

4. $t_{12}^{(\ell)} = 0$ *for* $\ell = \nu + 1, \ldots, m$ *(Lemma 2.iii).*

In addition, $t_{12}^{(\nu)} < 1$ for $\nu > \mu$ according to Lemma 2.iii. Similarly $t_{13}^{(\nu)} < 1$ for $\nu > \mu$ since otherwise $P$ could be shortened by the argument analogous to the proof of $t_{12}^{(\nu)} = \frac{1}{2}$ given in Lemma 2.iii for $k + 1 = \nu$.

# 5 Definition of Partition Classes

With regard to Corollary 1, we define partition class $R$ to be a set of indices of the variables that are tested on the single-edge computational path $v_2^{(\mu)}, v_2^{(\mu+1)}, \ldots, v_2^{(\gamma-1)}, v_3^{(\gamma)}, v_3^{(\gamma+1)}, \ldots,\ v_3^{(\nu-1)}$ (or $v_3^{(\mu)}, v_3^{(\mu+1)}, \ldots, v_3^{(\nu-1)}$ if $\gamma = \mu$ or $v_2^{(\mu)}, v_2^{(\mu+1)}, \ldots, v_2^{(\nu-1)}$ if $\gamma = \nu$). For the future use of condition (3.3) and (3.4) we also define relevant bits of string $\mathbf{c} \in \{0,1\}^n$. Thus, let $c_i$ be the corresponding labels of the edges creating this computational path including the edge outgoing from the last node $v_3^{(\nu-1)}$ (or $v_2^{(\nu-1)}$ if $\gamma = \nu$) which leads to $v_2^{(\nu)}$ or to $v_3^{(\nu)}$. Moreover, let $\max(\nu - 1, \mu) \leq \omega \leq m$ be the greatest level such that the parallel double-edge path leading from $v_2^{(\mu)}$ to $v_2^{(\nu-1)}$ (for $\gamma = \mu$) or from $v_3^{(\mu)}$ to $v_2^{(\nu-1)}$ (for $\mu < \gamma < \nu$) or from $v_3^{(\mu)}$ to $v_3^{(\nu-1)}$ (for $\gamma = \nu$) further continues up to level $\omega$ containing only nodes $v_\ell \in \{v_2^{(\ell)}, v_3^{(\ell)}\}$ for every $\ell = \mu, \ldots, \omega$.

Unless explicitly stated otherwise, we will further assume $\omega < m$ throughout this section, which implies $t_{12}^{(m)} = 0$ since otherwise $t_{12}^{(m)} = t_{32}^{(m)} = \frac{1}{2}$ forces $t_{33}^{(m)} = 1$ by Lemma 2.ii prolonging the double-edge path from $v_3^{(\mu)}$ up to $v_3^{(m)}$ according to Lemma 2.iii. We will show that $t_{13}^{(m)} > 0$. On the contrary, suppose that $t_{13}^{(m)} = 0$, which implies $t_{22}^{(m)} = t_{23}^{(m)} = 0$ due to $P$ is normalized, and hence $t_{32}^{(m)} = t_{33}^{(m)} = 1$. Moreover, we know that $t_{11}^{(m-1)} = 1$ and $t_{11}^{(m)} = t_{21}^{(m)} = \frac{1}{2}$. Thus, $v_2^{(m-1)}$ and $v_3^{(m-1)}$ can be merged and replaced by $v_3^{(m)}$, while $v_1^{(m-1)}$ replaces $v_1^{(m-2)}$, which shortens $P$ without changing its function. Thus, $t_{13}^{(m)} > 0$ which implies $t_{32}^{(m)} = 1$ since $t_{22}^{(m)} > 0$ is excluded by Lemma 2.ii. Then Lemma 2.iv can be employed for $k = m - 1$ where only case 3 and 4 may occur due to $\omega < m$ is assumed. In case 3, $t_{13}^{(m-1)} > 0$ and Lemma 2.iv can again be applied recursively for $k = m - 2$ etc.

In general, starting with $j = 1$ and $\sigma_1 = m$ that meets $t_{13}^{(\sigma_j)} > 0$, we define $\omega \leq \lambda_j < \sigma_j - 1$ to be the least level such that the transitions from case 3 or 4 of Lemma 2.iv, that is, $t_{11}^{(\ell)} = t_{22}^{(\ell)} = 1$ and $t_{33}^{(\ell)} = \frac{1}{2}$, appear for all levels $\ell = \lambda_j + 1, \ldots, \sigma_j - 1$. Note that $\lambda_j > \mu$ because $\lambda_j = \mu$ ensures $t_{22}^{(\mu+1)} = 1$ implying $\omega > \mu = \lambda_j$ by the definition of $\omega$, which contradicts $\omega \leq \lambda_j$. Clearly, case 4 from

Lemma 2.iv occurs at level $\lambda_j + 1$, that is $t_{23}^{(\lambda_j+1)} = \frac{1}{2}$, since $t_{13}^{(\lambda_j+1)} = \frac{1}{2}$ (case 3) for $\lambda_j > \omega$ would force case 1 or 2 at level $\lambda_j < \mu$ by the definition of $\lambda_j$, which would be in contradiction to $\omega \le \lambda_j$ according to Lemma 2.iv, while $t_{13}^{(\lambda_j+1)} = \frac{1}{2}$ for $\lambda_j = \omega$ contradicts the definition of $\omega$. Also denote by $\lambda_j + 1 < \kappa_j \le \sigma_j$ the least level such that $t_{13}^{(\kappa_j)} > 0$, which exists since at least $t_{13}^{(\sigma_j)} > 0$. Now we can define partition class $Q_j$ to be a set of indices of the variables that are tested on the computational path $v_3^{(\lambda_j)}, v_3^{(\lambda_j+1)}, \ldots, v_3^{(\kappa_j-1)}$, and let $c_i$ be the corresponding labels of the edges creating this path including the edge outgoing from the last node $v_3^{(\kappa_j-1)}$ to $v_1^{(\kappa_j)}$, which correctly extends the definition of $\mathbf{c} \in \{0,1\}^n$ due to $P$ is read-once. Finally, define new $\omega + 1 < \sigma_{j+1} \le \lambda_j$ to be the greatest level such that $t_{13}^{(\sigma_{j+1})} > 0$ and continue in our recursive definition of $\lambda_{j+1}, \kappa_{j+1}, Q_{j+1}$ with $j$ replaced by $j+1$ etc. if such $\sigma_{j+1}$ exists, otherwise set $q = j$ and the definition of partition classes $Q_1, \ldots, Q_q$ is complete. For $\omega = m$, on the other hand, no such partition class is defined, and we set $q = 0$.

Now we will lower bound $p_3^{(m)}$ in terms of $p_2^{(\omega+1)} + p_3^{(\omega+1)}$. For any $1 \le j \le q$, we know that $t_{11}^{(\ell)} = t_{22}^{(\ell)} = 1$ and $t_{23}^{(\ell)} = t_{33}^{(\ell)} = \frac{1}{2}$ for every $\ell = \lambda_j + 1, \ldots, \kappa_j - 1$, which gives

$$\begin{align} p_2^{(\kappa_j-1)} + p_3^{(\kappa_j-1)} &= p_2^{(\lambda_j)} + p_3^{(\lambda_j)} \tag{5.1} \\ p_3^{(\kappa_j-1)} = \frac{p_3^{(\lambda_j)}}{2^{|Q_j|-1}} &\le \frac{p_2^{(\lambda_j)} + p_3^{(\lambda_j)}}{2^{|Q_j|}} \tag{5.2} \end{align}$$

because $p_3^{(\lambda_j)} \le (p_2^{(\lambda_j)} + p_3^{(\lambda_j)})/2$. It follows from the definition of $\sigma_{j+1}$ and equation (5.1) that

$$p_2^{(\sigma_{j+1})} + p_3^{(\sigma_{j+1})} = p_2^{(\lambda_j)} + p_3^{(\lambda_j)} = p_2^{(\kappa_j-1)} + p_3^{(\kappa_j-1)} \tag{5.3}$$

for $1 \le j < q$, and

$$p_2^{(\omega+1)} + p_3^{(\omega+1)} = p_2^{(\lambda_q)} + p_3^{(\lambda_q)} = p_2^{(\kappa_q-1)} + p_3^{(\kappa_q-1)} \tag{5.4}$$

since $t_{12}^{(\ell)} = 0$ for every $\ell = \omega + 2, \ldots, m$ by Corollary 1.4 where $\nu + 1 \le \omega + 2$, while for $\lambda_q = \omega$, we know $t_{11}^{(\lambda_q+1)} = t_{22}^{(\lambda_q+1)} = 1$ and $t_{23}^{(\lambda_q+1)} = t_{33}^{(\lambda_q+1)} = \frac{1}{2}$. Moreover, we know $t_{22}^{(\ell)} = 1$ for every $\ell = \kappa_j, \ldots, \sigma_j - 1$ and $t_{12}^{(\sigma_j)} = 0$, which implies

$$\begin{align} p_2^{(\sigma_j)} + p_3^{(\sigma_j)} &\ge p_2^{(\kappa_j-1)} + p_3^{(\kappa_j-1)} - p_3^{(\kappa_j-1)} \ge p_2^{(\kappa_j-1)} + p_3^{(\kappa_j-1)} - \frac{p_2^{(\lambda_j)} + p_3^{(\lambda_j)}}{2^{|Q_j|}} \nonumber \\ &= \left(p_2^{(\sigma_{j+1})} + p_3^{(\sigma_{j+1})}\right)\left(1 - \frac{1}{2^{|Q_j|}}\right) \tag{5.5} \end{align}$$

for $1 < j < q$ according to (5.2) and (5.3), while formula (5.5) reads

$$p_3^{(m)} = p_3^{(\sigma_1)} \ge \left(p_2^{(\sigma_2)} + p_3^{(\sigma_2)}\right)\left(1 - \frac{1}{2^{|Q_1|}}\right) \tag{5.6}$$

for $j = 1 < q$ due to $t_{32}^{(m)} = 1$, whereas (5.5) is rewritten with

$$p_2^{(\sigma_q)} + p_3^{(\sigma_q)} \ge \left(p_2^{(\omega+1)} + p_3^{(\omega+1)}\right)\left(1 - \frac{1}{2^{|Q_q|}}\right) \tag{5.7}$$

for $j = q > 1$ according to (5.4). Starting with (5.6), inequality (5.5) is applied recursively for $j = 2, \ldots, q-1$, and, in the end, (5.7) is employed, which gives

$$p_3^{(m)} \ge \left(p_2^{(\omega+1)} + p_3^{(\omega+1)}\right) \prod_{j=1}^{q} \left(1 - \frac{1}{2^{|Q_j|}}\right) \tag{5.8}$$

holding also for the special case of $q = 1$. This can be rewritten as

$$p_1^{(m)} + p_2^{(m)} \le 1 - \left(1 - p_1^{(\omega+1)}\right) \prod_{j=1}^{q} \left(1 - \frac{1}{2^{|Q_j|}}\right) . \tag{5.9}$$

# 6 The Structure of $P$ below Level $\mu$

In this section, we will further analyze the structure of branching program $P$ below level $\mu$, provided that

$$p_3^{(\mu)} < \frac{1}{12}\,, \tag{6.1}$$

$$\prod_{j=1}^{q}\left(1-\frac{1}{2^{|Q_j|}}\right) > \frac{4}{5} \tag{6.2}$$

where the product in (6.2) formally equals 1 for $q = 0$. Condition (6.2) together with $p_3^{(m)} < \frac{1}{12}$ implies

$$p_2^{(\omega+1)} + p_3^{(\omega+1)} < \frac{5}{48} \tag{6.3}$$

for $\omega < m$ according to (5.8). It follows from (6.1) that $t_{31}^{(\mu)} = 0$ which implies $t_{21}^{(\mu)} > 0$ by the definition of $\mu$, and $p_3^{(\mu-1)} < \frac{1}{6}$ due to $p_3^{(\mu)} \geq p_3^{(\mu-1)}/2$, which gives $p_1^{(\mu-1)} + p_2^{(\mu-1)} > \frac{5}{6}$. Hence,

$$p_2^{(\mu)} \geq \frac{p_1^{(\mu-1)}}{2} \geq \frac{p_1^{(\mu-1)} + p_2^{(\mu-1)}}{4} > \frac{5}{24}\,. \tag{6.4}$$

We will prove that $t_{12}^{(\mu+1)} = \frac{1}{2}$. For $\omega = \mu$, the case of $t_{12}^{(\mu+1)} = 0$ implies $p_2^{(\omega+1)} + p_3^{(\omega+1)} \geq p_2^{(\mu)} > \frac{5}{24}$ according to (6.4), which contradicts (6.3), while for $t_{12}^{(\mu+1)} = 1 = t_{11}^{(\mu+1)}$ nodes $v_1^{(\mu)}$ and $v_2^{(\mu)}$ could be merged and $v_3^{(\mu)}$ could be split into two nodes (there are at least two edges leading to $v_3^{(\mu)}$ because otherwise if only one edge leads to $v_3^{(\mu)}$, then $\mathbf{a}' \in \Omega_1(A) \subseteq H$ would exist such that $P(\mathbf{a}') = 1$), which means the underlying analysis for $\mu$ could be transferred down to $\mu - 1$ due to $t_{31}^{(\mu)} = 0$. For $\omega > \mu$, on the other hand, we know there is a double-edge path starting from $v_2^{(\mu)}$ or $v_3^{(\mu)}$ and traversing $v \in \{v_2^{(\mu+1)}, v_3^{(\mu+1)}\}$ which ends at level $\omega$. For $v = v_2^{(\mu+1)}$, either $t_{22}^{(\mu+1)} = 1$, or $t_{23}^{(\mu+1)} = 1$ and $t_{32}^{(\mu+1)} = \frac{1}{2}$ which implies $t_{22}^{(\mu+1)} = \frac{1}{2}$ in this case since $t_{12}^{(\mu+1)} = \frac{1}{2}$ leads to a contradiction $\frac{1}{12} > p_3^{(\mu)} = p_2^{(\mu+1)} \geq p_3^{(\mu+1)} = p_2^{(\mu)}/2 > \frac{5}{48}$ according to (6.1) and (6.4). Thus, $t_{22}^{(\mu+1)} > 0$, $t_{22}^{(\ell)} = 1$ for $\ell = \mu+2, \ldots, \omega$, and $t_{12}^{(\omega+1)} = 0$ for $\omega < m$ according to Lemma 2.iii. Hence, $p_2^{(\omega+1)} + p_3^{(\omega+1)} \geq p_2^{(\mu)}/2 > \frac{5}{48}$ for $\omega < m$ according to (6.4), which contradicts (6.3), whereas an analogous contradiction $\frac{1}{12} > p_3^{(m)} \geq p_2^{(\mu)}/2 > \frac{5}{48}$ is obtained for $\omega = m$. It follows that $v = v_3^{(\mu+1)}$ which implies $t_{33}^{(\mu+1)} = 1$ and $t_{12}^{(\mu+1)} = t_{22}^{(\mu+1)} = \frac{1}{2}$ by the normalization of $P$. In addition, $t_{11}^{(\mu)} = t_{21}^{(\mu)} = \frac{1}{2}$ because $t_{21}^{(\mu)} = 1$ would imply $t_{12}^{(\mu)} > 0$ and $t_{13}^{(\mu)} > 0$ by the normalization of $P$, which together with $t_{12}^{(\mu+1)} = \frac{1}{2}$ would provide $\mathbf{a}' \in \Omega_1(A)$ such that $P(\mathbf{a}') = 1$ using three 'change-bit' paths $v_1^{(\mu-1)}, v_2^{(\mu)}, v_1^{(\mu+1)}$ and $v_2^{(\mu-1)}, v_1^{(\mu)}$ and $v_3^{(\mu-1)}, v_1^{(\mu)}$, respectively, starting at level $\mu - 1$ (cf. Lemma 2.ii).

Furthermore, define $2 \leq m' \leq \mu$ to be the greatest level such that $t_{32}^{(m')} > 0$, which exists since at least $t_{32}^{(2)} > 0$. We will show that $t_{33}^{(k)} = 1$ for $k = m'+1, \ldots, \mu$. On the contrary let $m' < k \leq \mu$ be the greatest level such that $t_{33}^{(k)} < 1$, that is $t_{33}^{(\ell)} = 1$ for $\ell = k+1, \ldots, \mu$. Obviously $t_{33}^{(k)} > 0$ because $t_{32}^{(\ell)} = 0$ for every $\ell = m'+1, \ldots, k, \ldots, \mu$ by the definition of $m'$, and also $t_{31}^{(\ell)} = 0$ for every $\ell = k, \ldots, \mu$ since otherwise $p_3^{(\mu)} \geq p_3^{(\ell)} > \frac{1}{6}$ which contradicts (6.1). Thus, $t_{33}^{(k)} = \frac{1}{2}$ and the edge from $v_3^{(k-1)}$ to $v_3^{(k)}$ is the only edge that leads to $v_3^{(k)}$ due to $t_{31}^{(k)} = t_{32}^{(k)} = 0$. Hence, the other edge from $v_3^{(k-1)}$ goes either to $v_1^{(k)}$ or to $v_2^{(k)}$. For the input $\mathbf{a} \in A$ from the assumption of Lemma 2, either $\mathbf{a} \in M(v_1^{(k)}) \cup M(v_2^{(k)})$ or an input $\mathbf{a}' \in M(v_3^{(k-1)}) \cap \Omega_1(A)$ exists which may differ from $\mathbf{a} \in A$ only in the $i$th bit such that $v_3^{(k-1)}$ is labeled with $x_i$. Since $M(v_1^{(k)}) \cup M(v_2^{(k)}) = M(v_1^{(\mu)}) \cup M(v_2^{(\mu)})$ and $t_{12}^{(\mu+1)} = \frac{1}{2}$ there is $\mathbf{a}' \in \Omega_2(A)$ such that $P(\mathbf{a}') = 1$ by the argument similar to Lemma 2.ii. Thus $t_{33}^{(k)} = 1$ for $k = m'+1, \ldots, \mu$, and

$$p_1^{(m')} + p_2^{(m')} = p_1^{(\mu)} + p_2^{(\mu)} \tag{6.5}$$

$$p_3^{(m')} = p_3^{(\mu)} < \frac{1}{12} \tag{6.6}$$

according to (6.1). Note that inequality (6.6) ensures $m' \geq 4$ due to $p_3^{(3)} \geq 1/2^3$.

We will show that $t_{11}^{(m')} = t_{21}^{(m')} = \frac{1}{2}$. Obviously, $t_{31}^{(m')} = 0$ since otherwise $p_3^{(m')} > \frac{1}{6}$ which contradicts (6.6). Moreover, $t_{21}^{(m')} = 1$ together with $t_{32}^{(m')} > 0$ would imply $p_3^{(m')} \geq p_2^{(m'-1)}/2 \geq (p_2^{(m'-1)} + p_3^{(m'-1)})/4 \geq p_1^{(m')}/4 > \frac{1}{12}$ violating (6.6). Finally, suppose that $t_{11}^{(m')} = 1$ which implies $t_{32}^{(m')} = \frac{1}{2}$ due to $P$ is normalized. For $t_{33}^{(m')} = 0$ the only edge to $v_3^{(m')}$ would be from $v_2^{(m'-1)}$. Then the input $\mathbf{a} \in A$ from the assumption of Lemma 2 belongs either to $M(v_1^{(m'-1)}) \cup M(v_3^{(m'-1)}) \subseteq M(v_1^{(\mu)}) \cup M(v_2^{(\mu)})$ or an input $\mathbf{a}' \in M(v_2^{(m'-1)}) \cap \Omega_1(A)$ exists which may differ from $\mathbf{a} \in A$ only in the $i$th bit such that $v_2^{(m'-1)}$ is labeled with $x_i$. Since $t_{12}^{(\mu+1)} = \frac{1}{2}$ there is $\mathbf{a}' \in \Omega_2(A)$ such that $P(\mathbf{a}') = 1$ by the argument similar to Lemma 2.ii. Hence $t_{33}^{(m')} > 0$ which implies $t_{22}^{(m')} = t_{23}^{(m')} = \frac{1}{2}$ because of $p_2^{(m')} \geq p_3^{(m')} \geq (p_2^{(m'-1)} + p_3^{(m'-1)})/2$, but then again either $\mathbf{a} \in M(v_1^{(m'-1)})$ or an input $\mathbf{a}' \in (M(v_2^{(m'-1)}) \cup M(v_3^{(m'-1)})) \cap \Omega_1(A)$ exists such that $\mathbf{a}' \in M(v_2^{(m')})$, which gives $\mathbf{a}' \in (M(v_1^{(m')}) \cup M(v_2^{(m')})) \cap \Omega_2(A) \subseteq H$ such that $P(\mathbf{a}') = 1$. The last possibility $t_{11}^{(m')} = t_{21}^{(m')} = \frac{1}{2}$ follows.

We will upper bound $p_1^{(\omega+1)}$ for $\omega < m$ or $p_1^{(m)} + p_2^{(m)}$ for $\omega = m$ in terms of $p_1^{(m')} + p_2^{(m')}$. For this purpose, we will first prove

$$p_1^{(\mu)} + p_2^{(\mu)} \leq 4p_2^{(\mu)} \,. \tag{6.7}$$

For $\mu > m'$ we have $p_1^{(\mu)} + p_2^{(\mu)} = p_1^{(\mu-1)} + p_2^{(\mu-1)} \leq 2p_1^{(\mu-1)} \leq 4p_2^{(\mu)}$ due to $t_{21}^{(\mu)} = \frac{1}{2}$. For $\mu = m'$ we know $t_{21}^{(m')} = \frac{1}{2}$ and $t_{32}^{(m')} > 0$, which gives $4p_2^{(\mu)} = 4p_2^{(m')} \geq 2p_1^{(m'-1)} = 2(1 - (p_2^{(m'-1)} + p_3^{(m'-1)})) \geq 2(1 - 2p_2^{(m'-1)}) \geq 2(1 - 4p_3^{(m')}) > 1 > p_1^{(\mu)} + p_2^{(\mu)}$ according to (6.6).

It follows from the definition of partition class $R$ (see Section 5) that

$$p_1^{(\nu)} = p_1^{(\mu)} + p_2^{(\mu)} \left(1 - \frac{1}{2^{|R|}}\right) \tag{6.8}$$

for $\nu < m$, whereas $p_1^{(\nu)}$ is replaced with $p_1^{(m)} + p_2^{(m)}$ in (6.8) for $\nu = m$. We know by the definition of $\nu$ that $t_{12}^{(\nu+1)} = t_{13}^{(\nu+1)} = 0$ for $\nu < m$ (implying $\nu < m-1$ due to $t_{13}^{(m)} > 0$), which means both $t_{32}^{(\nu+1)} = 1$ and $t_{33}^{(\nu+1)} = 1$ are excluded since $P$ is normalized. We will first assume $\omega > \nu$. The double-edge path from the definition of $\omega$ passes through a double edge from $v \in \{v_2^{(\nu)}, v_3^{(\nu)}\}$ to $v_2^{(\nu+1)}$, while the two edges from the other node $v' \in \{v_2^{(\nu)}, v_3^{(\nu)}\} \setminus \{v\}$ lead to $v_2^{(\nu+1)}$ and $v_3^{(\nu+1)}$. For $\omega < m$, we have $t_{22}^{(\ell)} = 1$ and $t_{33}^{(\ell)} = \frac{1}{2}$ for $\ell = \nu+2, \ldots, \omega$, and $t_{12}^{(\omega+1)} = 0$ by Corollary 1.4, while the same holds for the special case of $\omega = m$, except for level $m$ where $t_{32}^{(m)} = 1$. Hence, $p_3^{(\nu+1)} = p_2^{(\mu)}/2^{|R|+1}$ upper bounds the fraction of inputs whose computational paths traverse nodes $v', v_3^{(\nu+1)}, v_3^{(\nu+2)}, \ldots, v_3^{(\ell)}, v_1^{(\ell+1)}$ for some $\nu + 1 \leq \ell \leq \min(\omega, m-1)$. It follows that

$$p_1^{(\omega+1)} \leq p_1^{(\nu)} + \frac{p_2^{(\mu)}}{2^{|R|+1}} \tag{6.9}$$

which is valid for any $\nu - 1 \leq \omega < m$ since obviously $p_1^{(\omega+1)} = p_1^{(\nu)}$ for $m > \omega \in \{\nu - 1, \nu\}$, while $p_1^{(\omega+1)}$ is replaced with $p_1^{(m)} + p_2^{(m)}$ in (6.9) for $\nu < \omega = m$. Finally, equation (6.8) is plugged into (6.9), and inequalities (6.7) and (6.5) are employed, which results in

$$\begin{aligned} p_1^{(\omega+1)} &\leq p_1^{(\mu)} + p_2^{(\mu)} \left(1 - \frac{1}{2^{|R|}}\right) + \frac{p_2^{(\mu)}}{2^{|R|+1}} = p_1^{(\mu)} + p_2^{(\mu)} \left(1 - \frac{1}{2^{|R|+1}}\right) \\ &\leq \left(p_1^{(m')} + p_2^{(m')}\right) \left(1 - \frac{1}{2^{|R|+3}}\right) \end{aligned} \tag{6.10}$$

for $\omega < m$ whereas $p_1^{(\omega+1)}$ is replaced with $p_1^{(m)} + p_2^{(m)}$ in (6.10) for $\omega = m$. Formula (6.10) can further be plugged into (5.9) as

$$p_1^{(m)} + p_2^{(m)} \leq 1 - \left(1 - \left(p_1^{(m')} + p_2^{(m')}\right) \left(1 - \frac{1}{2^{|R|+3}}\right)\right) \prod_{j=1}^{q} \left(1 - \frac{1}{2^{|Q_j|}}\right) \tag{6.11}$$

which is even valid for $\omega = m$ (i.e. $q = 0$) according to (6.10) which reads $p_1^{(m)} + p_2^{(m)} \leq (p_1^{(m')} + p_2^{(m')})(1 - 1/2^{|R|+3})$ for $\omega = m$.

# 7 Recursion for $m$

In the previous sections we have analyzed the block of $P$ from level $m'$ through $m$. We will now employ this block analysis recursively so that $m = m_r$ is replaced by $m' = m_{r+1}$. For this purpose, we will introduce additional index $b = 1, \ldots, r$ to the underlying objects in order to differentiate among respective blocks. For example, the partition classes $R, Q_1, \ldots, Q_q$ defined in Section 5 corresponding to the $b$th block are denoted as $R_b, Q_{b1}, \ldots, Q_{bq_b}$, respectively.

We will formally proceed by induction on $r$ starting with $r = 0$ and $m_0 = d$. In the induction step for $r + 1$, let the assumptions of Lemma 2 hold for $m = m_r$, and we assume that condition (6.1) is satisfied for the previous blocks, that is,

$$p_3^{(\mu_b)} < \frac{1}{12} \tag{7.1}$$

for every $b = 1, \ldots, r$. In addition, let

$$\begin{aligned} \varrho_r &> \delta\,\varepsilon\,, & (7.2)\\ 1 - \Pi_r &< (1-\delta)\,\varepsilon & (7.3) \end{aligned}$$

where

$$\begin{aligned} \varrho_k &= \prod_{b=1}^{k} \alpha_b\,, \qquad \alpha_b = \left(1 - \frac{1}{2^{|R_b|+3}}\right)\,, & (7.4)\\ \Pi_k &= \prod_{b=1}^{k} \pi_b\,, \qquad \pi_b = \prod_{j=1}^{q_b} \left(1 - \frac{1}{2^{|Q_{bj}|}}\right) & (7.5) \end{aligned}$$

for $k = 1, \ldots, r$, and formally $\varrho_0 = \Pi_0 = 1$ and $\pi_b = 1$ for $q_b = 0$. It follows from (7.5) and (7.3) that

$$\pi_b \geq \Pi_r > 1 - (1-\delta)\,\varepsilon \geq \delta > \frac{4}{5} \tag{7.6}$$

which verifies assumption (6.2) for every $b = 1, \ldots, r$. Hence, we can employ recursive inequality (6.11) from Section 6 which is rewritten as

$$p_{b-1} \leq 1 - (1 - p_b\alpha_b)\pi_b = 1 - \pi_b + p_b\alpha_b\pi_b \tag{7.7}$$

for $b = 1, \ldots, r$ where notation $p_b = p_1^{(m_b)} + p_2^{(m_b)}$ is introduced. Starting with

$$p_0 = p_1^{(d)} + p_2^{(d)} \geq \varepsilon \tag{7.8}$$

which follows from (4.1), recurrence (7.7) can be solved as

$$\begin{aligned} \varepsilon &\leq \sum_{k=1}^{r}(1-\pi_k)\prod_{b=1}^{k-1}\alpha_b\pi_b + p_r\prod_{b=1}^{r}\alpha_b\pi_b < \sum_{k=1}^{r}(1-\pi_k)\Pi_{k-1} + p_r\varrho_r\Pi_r\\ &= 1 - \Pi_r + p_r\varrho_r\Pi_r\,. & (7.9) \end{aligned}$$

Throughout this section, we will further consider the case when also

$$1 - \Pi_{r+1} < (1-\delta)\,\varepsilon \tag{7.10}$$

(cf. assumption (7.3)) which implies

$$\pi_{r+1} > \delta > \frac{4}{5} \tag{7.11}$$

by analogy to (7.6), while the case complementary to (7.10), which concludes the induction, will be resolved below in Section 8. For $\omega_{r+1} < m_r$, we know

$$p_r \leq 1 - \left(p_2^{(\omega_{r+1}+1)} + p_3^{(\omega_{r+1}+1)}\right) \pi_{r+1} \tag{7.12}$$

according to (5.9), and

$$p_2^{(\omega_{r+1}+1)} + p_3^{(\omega_{r+1}+1)} \geq p_3^{(\mu_{r+1})} \tag{7.13}$$

by the definition of $\omega_{r+1}$ and Lemma 2.iii–iv for $k = \omega_{r+1}$, which altogether gives

$$\varepsilon < 1 - \Pi_r + \left(1 - p_3^{(\mu_{r+1})}\pi_{r+1}\right) \varrho_r \Pi_r \tag{7.14}$$

according to (7.9). Hence,

$$\delta\,\varepsilon < \left(1 - p_3^{(\mu_{r+1})}\pi_{r+1}\right) \varrho_r \Pi_r < 1 - p_3^{(\mu_{r+1})}\pi_{r+1} \tag{7.15}$$

follows from (7.3), which gives

$$p_3^{(\mu_{r+1})}\pi_{r+1} < 1 - \delta^2 \tag{7.16}$$

by the assumption of $\varepsilon > \delta$, implying

$$p_3^{(\mu_{r+1})} < \frac{1-\delta^2}{\delta} < \frac{1}{12} \tag{7.17}$$

due to (7.11), which is valid also for $\omega_{r+1} = m_r$ since $p_3^{(\mu_{r+1})} \leq p_3^{(m_r)} < \frac{1}{12}$ in this case. Therefore, assumptions (6.1) and (6.2) of the analysis in Section 6 are met also for the $(r+1)$st block according to (7.17) and (7.11), respectively, which justifies recurrence inequality (7.7) for $b = r+1$ leading to the solution

$$\varepsilon < 1 - \Pi_{r+1} + p_{r+1}\varrho_{r+1}\Pi_{r+1} \tag{7.18}$$

by analogy to (7.9) where $r$ is replaced with $r+1$. By combining (7.18) with (7.10), we obtain

$$\varrho_{r+1} > p_{r+1}\varrho_{r+1}\Pi_{r+1} > \delta\,\varepsilon\,. \tag{7.19}$$

Thus, inductive assumptions (7.1)–(7.3) are valid for $r$ replaced by $r+1$ according to (7.17), (7.19), and (7.10), respectively.

In order to proceed in the next induction step, we still need to verify the assumptions of Lemma 2 for $m = m_{r+1}$ that replaces $m'$ for which we have shown $t_{11}^{(m_{r+1})} = t_{21}^{(m_{r+1})} = \frac{1}{2}$, $t_{32}^{(m_{r+1})} > 0$, and $p_3^{(m_{r+1})} < \frac{1}{12}$ in Section 6. It suffices to show that $\mathbf{a} \in A$ exists such that if we put $\mathbf{a}$ at node $v_1^{(m_{r+1})}$ or $v_2^{(m_{r+1})}$, then its onward computational path arrives to the sink labeled with 1. For this purpose, we exploit the fact that $A$ is $(\delta^{11} - \delta^{12})\varepsilon^{12}$-rich after showing corresponding condition (3.5) for partition $\{R_1, \ldots, R_{r+1}\}$ of $I = \bigcup_{b=1}^{r+1} R_b$. In particular,

$$(\delta^{11} - \delta^{12})\varepsilon^{12} < (\delta\,\varepsilon)^{11} < \prod_{b=1}^{r+1}\left(1 - \frac{1}{2^{|R_b|}}\right) \tag{7.20}$$

follows from (7.19) since for any $1 \leq b \leq r+1$,

$$\left(1 - \frac{1}{2^{|R_b|+3}}\right)^{11} < 1 - \frac{1}{2^{|R_b|}} \tag{7.21}$$

for $|R_b| \geq 1$ because $f(x) = \ln(1 - \frac{1}{x})/\ln(1 - \frac{1}{8x})$ is a decreasing function for $x = 2^{|R_b|} \geq 2$ and $f(2) < 11$. This provides required $\mathbf{a} \in A$ such that for every $b = 1, \ldots, r$ there exists $i \in R_b$ that meets $a_i \neq c_i$ according to (3.4). Obviously, the computational path for this $\mathbf{a}$ ends up in a sink $v_1^{(d)}$ or $v_2^{(d)}$ labeled with 1 when we put $\mathbf{a}$ at node $v_1^{(m_{r+1})}$ or $v_2^{(m_{r+1})}$ by the definition of $R_b$, $c_i$, and the structure of branching program $P$. Thus, the inductive assumptions are met for $r+1$ and we can proceed recursively for $r$ replaced with $r+1$ etc. until condition (7.10) is broken.

# 8 The End of Induction

In this section, we will consider the case of

$$1 - \Pi_{r+1} \geq (1-\delta)\,\varepsilon \tag{8.1}$$

complementary to (7.10), which concludes the induction in Section 7 as follows. We will again employ the fact that $A$ is $(\delta^{11} - \delta^{12})\varepsilon^{12}$-rich. First condition (3.2) for partition $\{Q_{11}, \ldots, Q_{1q_1}, Q_{21}, \ldots, Q_{2q_2}, \ldots, Q_{r+1,1}, \ldots, Q_{r+1,q_{r+1}},\ R_1, \ldots, R_r\}$ of $I = \bigcup_{b=1}^{r+1} \bigcup_{j=1}^{q_b} Q_{bj} \cup \bigcup_{b=1}^{r} R_b$ is verified as

$$\begin{aligned} \left(1 - \prod_{b=1}^{r+1} \prod_{j=1}^{q_b} \left(1 - \frac{1}{2^{|Q_{bj}|}}\right)\right) \prod_{b=1}^{r} \left(1 - \frac{1}{2^{|R_b|}}\right) \quad &> \quad (1 - \Pi_{r+1})\varrho_r^{11} \\ > (1-\delta)\varepsilon\,(\delta\,\varepsilon)^{11} \quad &= \quad (\delta^{11} - \delta^{12})\varepsilon^{12} \end{aligned} \tag{8.2}$$

according to (7.21), (8.1), and (7.2). This provides $\mathbf{a} \in A$ such that there exists block $1 \leq b \leq r+1$ and $1 \leq j \leq q_b$ satisfying $a_i = c_i$ for every $i \in Q_{bj}$, and simultaneously, for every $b = 1, \ldots, r$ there exists $i \in R_b$ that meets $a_i \neq c_i$ according to (3.3) and (3.4). Using the first part (3.3) of the condition for $\mathbf{a}$, we will prove below that there is $\mathbf{a}' \in \Omega_2(A) \subseteq H$ such that $\mathbf{a}'$ differs from $\mathbf{a}$ in at most two bits which are tested by $P$ only below level $m_{b-1}$ and $\mathbf{a}' \in M(v_1^{(m_{b-1})}) \cup M(v_2^{(m_{b-1})})$, while the second part (3.4) then guarantees that $P(\mathbf{a}') = 1$.

For the notation simplicity, we will henceforth omit the block index $b$. Thus within the $b$th block we have $1 \leq j \leq q$ such that $a_i = c_i$ for every $i \in Q_j$, and denote $\lambda = \lambda_j > \mu$ for this $j$. Clearly, $\omega < m$ due to $q > 0$. We will show below that there are two generalized 'change-bit' paths (cf. Lemma 2.ii) starting from $v_2^{(k)}$ and from $v_3^{(k)}$, respectively, at some level $3 < \max(\lambda - 2, \mu) \leq k < \lambda$, which may also lead to $v_3^{(\lambda)}$ in addition to $v_1^{(\lambda-1)}$ and $v_1^{(\lambda)}$. By the argument similar to Lemma 2.ii extended now with condition (3.3), this gives $\mathbf{a}' \in \Omega_2(A) \subseteq H$ such that $h(\mathbf{a}', \mathbf{a}) \leq 2$ and $\mathbf{a}' \in M(v_1^{(m_{b-1})}) \cup M(v_2^{(m_{b-1})})$, which implies $P(\mathbf{a}') = 1$ by condition (3.4). This will complete the proof of Theorem 2.

Consider first the case when $t_{12}^{(\lambda)} = t_{13}^{(\lambda)} = 0$. Obviously, $t_{22}^{(\lambda)} < 1$ follows from the definition of $\lambda$ for $\lambda > \omega$ and from the definition of $\omega$ for $\lambda = \omega$, which gives $t_{22}^{(\lambda)} = t_{32}^{(\lambda)} = \frac{1}{2}$ and $t_{23}^{(\lambda)} > 0$ due to $P$ is normalized. For $t_{33}^{(\lambda)} = \frac{1}{2}$ we obtain two change-bit paths $v_2^{(\lambda-1)}, v_3^{(\lambda)}$ and $v_3^{(\lambda-1)}, v_3^{(\lambda)}$. Hence, $t_{33}^{(\lambda)} = 0$ which ensures $t_{23}^{(\lambda)} = 1$ and $\lambda > \mu + 1$ since $\lambda = \mu + 1$ would give $\omega > \lambda$. Consider first the case when $t_{12}^{(\lambda-1)} = t_{13}^{(\lambda-1)} = 0$, which implies $t_{22}^{(\lambda-1)} > 0$ and $t_{23}^{(\lambda-1)} > 0$ by $t_{11}^{(\lambda-1)} = 1$ and the normalization of $P$, providing two change-bit paths $v_2^{(\lambda-2)}, v_2^{(\lambda-1)}, v_3^{(\lambda)}$ and $v_3^{(\lambda-2)}, v_2^{(\lambda-1)}, v_3^{(\lambda)}$. Two change-bit paths $v_2^{(\lambda-2)}, v_1^{(\lambda-1)}$ and $v_3^{(\lambda-2)}, v_1^{(\lambda-1)}$ are also guaranteed when $t_{12}^{(\lambda-1)} > 0$ and $t_{13}^{(\lambda-1)} > 0$ appear simultaneously. For $t_{12}^{(\lambda-1)} = 0$ and $t_{13}^{(\lambda-1)} > 0$, we have $t_{22}^{(\lambda-1)} > 0$ by the normalization of $P$, which together with $t_{32}^{(\lambda)} = \frac{1}{2}$ produces two change-bit paths $v_2^{(\lambda-2)}, v_2^{(\lambda-1)}, v_3^{(\lambda)}$ and $v_3^{(\lambda-2)}, v_1^{(\lambda-1)}$. For $t_{12}^{(\lambda-1)} > 0$ and $t_{13}^{(\lambda-1)} = 0$, the case of $t_{23}^{(\lambda-1)} > 0$ ensures two change-bit paths $v_2^{(\lambda-2)}, v_1^{(\lambda-1)}$ and $v_3^{(\lambda-2)}, v_2^{(\lambda-1)}, v_3^{(\lambda)}$, while for $t_{23}^{(\lambda-1)} = 0$ we obtain $t_{12}^{(\lambda-1)} = t_{22}^{(\lambda-1)} = \frac{1}{2}$ and $t_{33}^{(\lambda-1)} = 1$, which implies $\lambda = \nu + 1$ and $\omega > \lambda$ by Lemma 2.iii contradicting the definition of $\lambda \geq \omega \geq \nu - 1$.

Now consider the case when $t_{13}^{(\lambda)} > 0$ which implies $t_{12}^{(\lambda)} = 0$. Furthermore, $t_{22}^{(\lambda)} < 1$ follows from the definition of $\lambda$ for $\lambda > \omega$ and from the definition of $\omega$ for $\lambda = \omega$. Hence, $t_{32}^{(\lambda)} > 0$ which produces two change-bit paths $v_2^{(\lambda-1)}, v_3^{(\lambda)}$ and $v_3^{(\lambda-1)}, v_1^{(\lambda)}$. Finally, consider the case when $t_{12}^{(\lambda)} > 0$ (i.e. $t_{13}^{(\lambda)} = 0$) for which $t_{33}^{(\lambda)} > 0$ generates two change-bit $v_2^{(\lambda-1)}, v_1^{(\lambda)}$ and $v_3^{(\lambda-1)}, v_3^{(\lambda)}$, while for $t_{33}^{(\lambda)} = 0$ we obtain $t_{32}^{(\lambda)} = \frac{1}{2}$ and $t_{23}^{(\lambda)} = 1$, which implies $\lambda = \nu$ and $\omega > \lambda$ by Lemma 2.iii contradicting the definition of $\lambda \geq \omega \geq \nu - 1$. □

# 9 Discussion and Future Work

The aim of this study is to support the effort for seeking polynomial time constructions of hitting sets for branching programs. We have achieved partial progress along this line for 1-branching programs of depth 3 in our previous work [3] by using the result due to Alon, Goldreich, Håstad, and Peralta [1] who provided a polynomial time constructible set $A^*$ satisfying the following condition: For any $Q \subseteq \{1,\ldots,n\}$ of size $|Q| \leq \log n$ and for any $\mathbf{c} \in \{0,1\}^n$ there is $\mathbf{a} \in A^* \cap \{0,1\}^n$ such that $a_i = c_i$ for every $i \in Q$. On the other hand, observe that for any partition $\{Q_1,\ldots,Q_q\}$ of $I \subseteq \{1,\ldots,n\}$ that meets condition (3.6) there must be $1 \leq j \leq q$ such that $|Q_j| \leq \log n$ since, in the opposite case, we would have

$$\prod_{j=1}^{q}\left(1-\frac{1}{2^{|Q_j|}}\right) \geq \left(1-\frac{1}{2^{\log n}}\right)^{\frac{n}{\log n}} > 1-\frac{1}{n}\cdot\frac{n}{\log n} = 1-\frac{1}{\log n} > 1-\varepsilon \tag{9.1}$$

for any $\varepsilon > 0$, for sufficiently large $n > 2^{1/\varepsilon}$, which breaks (3.6). It follows that the first conjunct (3.3) from the richness condition holds for $A^*$. The validity of the second conjunct (3.4) for $A^*$ (or its extension), which would imply that $\Omega_3(A^*)$ is a hitting set for width-3 1-branching programs according to Theorem 2, still remains an open problem for further research.

# Bibliography

[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., 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] Šíma, J., Žák, S.: A polynomial time constructible hitting set for restricted 1-branching programs of width 3. Proceedings of the SOFSEM 2007 Thirty-Third International Conference on Current Trends in Theory and Practice of Informatics, LNCS **4362**, Springer-Verlag, Berlin (2007) 522–531

[4] Wegener, I.: Branching Programs and Binary Decision Diagrams—Theory and Applications. SIAM Monographs on Discrete Mathematics and Its Applications, SIAM, Philadelphia, PA (2000)