Almost k-Wise Independent Sets Establish Hitting Sets for Width-3 1-Branching Programs

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. Recently, an interest in constructing pseudorandom or hitting set generators for restricted branching programs has increased, which is motivated by the fundamental problem of derandomizing space bounded computations. Such constructions have been known only in the case of width 2 and in very restricted cases of bounded width. In our previous work, we have introduced a so-called richness condition which is, in a certain sense, sufficient for a set to be a hitting set for read-once branching programs of width 3. In this paper, we prove that, for a suitable constant C, any almost $C \log n$-wise independent set satisfies this richness condition. Hence, we achieve an explicit polynomial time construction of a hitting set for read-once branching programs of width 3 with the acceptance probability greater than $\sqrt{12/13}$ by using the result due to Alon et al. (1992).

1 Introduction

The relationship between deterministic and probabilistic computations is one of the central issues in complexity theory. This problem can be tackled by constructing polynomial time pseudorandom [10] or *hitting set* generators [6] which, however, belongs to the hardest problems in computer science even for severely restricted computational models. In particular, derandomizing space bounded computations has attracted much interest over a decade. We consider *read-once branching (1-branching) programs* [14] of polynomial size for which pseudorandom generators with seed length $O(\log^2 n)$ have been known for a long time through a result of Nisan [9]. Recently, considerable attention has been paid to improving this to $O(\log n)$ in the constant-width case, which is a fundamental problem with many applications in circuit lower bounds and derandomization [8]. The problem has been resolved for width 2 but the known techniques provably fail for width 3 [2, 8], which applies even to hitting set generators [4].

In the case of width 3, we do not know of any significant improvement over Nisan's result except for severely restricted so-called *regular* (oblivious) read-once branching programs of constant width having the in-degree of every vertex equal to 2, for which pseudorandom generators have recently been constructed

* This research was partially supported by projects GA ČR P202/10/1333, MŠMT ČR 1M0545, and AV0Z10300504.

with seed length $O(\log n \log\log n)$ [3, 4]. There has also been some recent progress in the case of *permutation* (oblivious) read-once branching programs of bounded width whose edges labeled with 0 (respectively 1) define a one to one mapping for each level-to-level transition [8], for which a pseudorandom generator has been constructed with seed length $O(\log n)$ [7]. In our paper [11], we made the first step for finding a polynomial time constructible hitting set for width 3. Using the result due to Alon et al. [1], we achieved such a construction if an additional, rather technical restriction is imposed on the program structure. For example, this restriction is met if one special pattern of level-to-level transitions in a normalized form of so-called *simple* width-3 1-branching programs is excluded, which covers the regular and permutation cases (see [11] for further details).

In our previous work [12, 13], we have introduced a so-called *richness* condition which is independent of the notion of branching programs. In fact, a rich set is a hitting set for special read-once CNFs (or even for the read-once conjunctions of DNFs and CNFs with properly bounded monomial and clause sizes, respectively [12]). Thus, a related line of study concerns pseudorandom generators for read-once formulas, such as read-once DNFs [5]. This richness condition proves to be sufficient in a sense that any rich set extended with all strings within Hamming distance of at most 3 is a hitting set for width-3 1-branching programs with the acceptance probability greater than $\sqrt{12/13}$. In this paper, we prove that, for a suitable constant C, any almost $C\log n$-wise independent set satisfies the richness condition. In the proof, the probability that there is a certain input which ensures the richness of an almost k-wise independent set, is lower bounded by a positive number (e.g. by using the inclusion-exclusion principle). It follows that our result combined with an efficient construction of almost k-wise independent sets, e.g. due to Alon et al. [1], provides a polynomial time construction of a hitting set for width-3 1-branching programs.

The paper is organized as follows. After a brief review of basic definitions regarding branching programs, the richness condition and its sufficiency is presented in Section 2. The main result that any almost $O(\log n)$-wise independent set is rich is formulated in Section 3 where the main steps of the technical proof occupying the subsequent four Sections 4–7 are outlined. Our result is summarized in Section 8.

2 Branching Programs and the Richness Condition

We start with a brief review of basic formal definitions regarding branching programs (see [14] for more information). 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 maximum number of nodes on one level is called the *width* of P.

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 *ε-hitting set* for class $\mathcal{P}$ if for sufficiently large n, for every branching program $P \in \mathcal{P}$ with n input variables,

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

Furthermore, we say that a set $A \subseteq \{0,1\}^*$ is *ε-rich* if for sufficiently large n, for any index set $I \subseteq \{1,\ldots,n\}$, for any partition $\{R_1,\ldots,R_r\}$ of I $(r \geq 0)$ satisfying

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

and for any $Q \subseteq \{1,\ldots,n\} \setminus I$ such that $|Q| \leq \log n$, for any $\mathbf{c} \in \{0,1\}^n$ there exists $\mathbf{a} \in A \cap \{0,1\}^n$ that meets

$$(\forall\, i \in Q)\, a_i = c_i \text{ and } (\forall\, j \in \{1,\ldots,r\})\, (\exists\, i \in R_j)\, a_i \neq c_i\,. \tag{3}$$

Note that formula (3) can be interpreted as a read-once CNF (each variable occurs at most once) which contains at most logarithmic number of single literals together with clauses whose sizes satisfy (2). Hence, any rich set is a hitting set for such read-once CNFs. In the following theorem, we formulate our previous result [12, 13] that the richness condition is, in a certain sense, sufficient for a set to be a hitting set for read-once branching programs of width 3.

Theorem 1 ([12, 13]). *If A is $(\delta\,\varepsilon)^{11}$-rich for $\varepsilon > \delta = \sqrt{12/13}$, then $H = \Omega_3(A) = \{\mathbf{a}' \in \{0,1\}^n \,|\, n \geq 1\, \&\, (\exists \mathbf{a} \in A \cap \{0,1\}^n)\, h(\mathbf{a},\mathbf{a}') \leq 3\}$, where $h(\mathbf{a},\mathbf{a}')$ is the Hamming distance between $\mathbf{a}$ and $\mathbf{a}'$ (i.e. the number bits in which $\mathbf{a}$ and $\mathbf{a}'$ differ), is an ε-hitting set for the class of width-3 read-once branching programs.*

3 Almost *k*-wise Independent Sets Are Rich

The following theorem shows that the richness condition introduced in previous Section 2 is satisfied by almost k-wise independent sets. Hence, in order to achieve an explicit polynomial time construction of a hitting set for read-once branching programs of width 3, we can combine Theorem 1 with the result due to Alon et al. [1] who provided simple efficient constructions of almost k-wise independent sets. In particular, for $\beta > 0$ and $k = O(\log n)$ it is possible to construct a (k, β)-*wise independent set* $\mathcal{A} \subseteq \{0,1\}^*$ in time polynomial in $\frac{n}{\beta}$ such that for sufficiently large n and any index set $S \subseteq \{1,\ldots,n\}$ of size $|S| \le k$, the probability that a given $\mathbf{c} \in \{0,1\}^n$ coincides with a string $\mathbf{a} \in \mathcal{A}_n = \mathcal{A} \cap \{0,1\}^n$ on the bit locations from S is almost uniform, that is

$$\left| \frac{|\mathcal{A}_n^S(\mathbf{c})|}{|\mathcal{A}_n|} - \frac{1}{2^{|S|}} \right| \le \beta\,, \tag{4}$$

where $\mathcal{A}_n^S(\mathbf{c}) = \{\mathbf{a} \in \mathcal{A}_n \,|\, (\forall i \in S)\, a_i = c_i\}$. We will prove that, for suitable k, any almost k-wise independent set is ε-rich.

Theorem 2. *Let $\varepsilon > 0$, C be the least odd integer greater than $(\frac{2}{\varepsilon} \ln \frac{1}{\varepsilon})^2$, and $0 < \beta < \frac{1}{n^{C+3}}$. Then any $(\lceil (C+2)\log n \rceil, \beta)$-wise independent set is ε-rich.*

Proof. Let $\mathcal{A} \subseteq \{0,1\}^*$ be a $(\lceil (C+2)\log n \rceil, \beta)$-wise independent set. We will show that $\mathcal{A}$ is ε-rich. Assume $\{R_1, \ldots, R_r\}$ is a partition of index set $I \subseteq \{1,\ldots,n\}$ satisfying condition (2), and $Q \subseteq \{1,\ldots,n\} \setminus I$ such that $|Q| \le \log n$. In order to show for a given $\mathbf{c} \in \{0,1\}^n$ that there is $\mathbf{a} \in \mathcal{A}_n$ that meets (3) for Q and partition $\{R_1, \ldots, R_r\}$, we will prove that the probability

$$p = \frac{\left| \mathcal{A}_n^Q(\mathbf{c}) \setminus \bigcup_{j=1}^r \mathcal{A}_n^{R_j}(\mathbf{c}) \right|}{|\mathcal{A}_n|} \tag{5}$$

of the event that $\mathbf{a} \in \mathcal{A}_n$ chosen uniformly at random satisfies $\mathbf{a} \in \mathcal{A}_n^Q(\mathbf{c})$ and $\mathbf{a} \notin \mathcal{A}_n^{R_j}(\mathbf{c})$ for every $j = 1, \ldots, r$, is *strictly positive.*

The main idea of the proof lies in lower bounding the probability (5). We briefly comment on the main steps of the proof which are schematically depicted in Figure 1 including references to corresponding sections, lemmas, and equations. In Section 4, we will first modify the partition classes R_j so that their cardinalities are at most logarithmic whereas the classes of small constant cardinalities are merged with Q and also $\mathbf{c}$ is adjusted correspondingly. Lemma 1 then ensures that the probability p from (5) is lower bounded when using these modified classes. Furthermore, Bonferroni inequality (the inclusion-exclusion principle) and the assumption concerning the almost k-wise independence are employed in Section 5 where also the classes of the same cardinality are grouped. In Section 6, we will further reduce the underlying lower bound on p only to a sum over frequent cardinalities of partition classes to which Taylor's theorem is applied in Section 7, whereas a corresponding Lagrange remainder is bounded using the assumption on constant C.

4 Modifications of Partition Classes

We properly modify the underlying partition classes in order to further upper bound their cardinalities by the logarithmic function so that the assumption

Modifications of Partition Classes (Section 4)

- superlogarithmic cardinalities:
  $R'_j \subseteq R_j$ so that $|R'_j| \le \log n$ (6)
- small constant cardinalities:
  $R_{\le} = \bigcup_{|R'_j| \le \sigma} R'_j$ where σ is a constant (11) & (14)
  $\longrightarrow Q' = Q \cup R_{\le}$ (16), $c'_i = 1 - c_i$ for $i \in R_{\le}$ (19)

Lemma 1: $p \ge \dfrac{\left|\mathcal{A}_n^{Q'}(\mathbf{c}') \setminus \bigcup_{j=1}^{r'} \mathcal{A}_n^{R'_j}(\mathbf{c}')\right|}{|\mathcal{A}_n|}$ (20)

$\Big\downarrow$ **Bonferroni inequality**

$$p \ge \sum_{k=0}^{C'} (-1)^k \sum_{1 \le j_1 < j_2 < \cdots < j_k \le r'} \frac{\left|\mathcal{A}_n^{\bigcup_{i=1}^{k} R'_{j_i} \cup Q'}(\mathbf{c}')\right|}{|\mathcal{A}_n|} \qquad (22)$$

$\Big\downarrow$ **almost k-wise independence** (Section 5)

$$p \ge \frac{1}{2^{|Q'|}} \left(\sum_{k=0}^{C'} (-1)^k \sum_{1 \le j_1 < j_2 < \cdots < j_k \le r'} \prod_{i=1}^{k} \frac{1}{2^{\left|R'_{j_i}\right|}} - \frac{\varepsilon'}{8} \right) \qquad (25)\ \&\ (26)$$

Grouping the Same Cardinalities (Lemma 2)

$\sigma < s_1, \ldots, s_{m'} \le \log n$ … cardinalities of R'_j

$r_i = \left|\left\{ j \,|, \left|R'_j\right| = s_i \right\}\right|$ … the number of classes of cardinality s_i

$$p > \frac{1}{n^2} \left(\sum_{k=0}^{C'} (-1)^k \sum_{\substack{k_1 + \cdots + k_{m'} = k \\ 0 \le k_1 \le r_1, \ldots, 0 \le k_{m'} \le r_{m'}}} \prod_{i=1}^{m'} \frac{t_i^{k_i}}{k_i!} \prod_{j=1}^{k_i - 1} \left(1 - \frac{j}{r_i}\right) - \frac{\varepsilon'}{8} \right) \qquad (30)$$

where $t_i = \dfrac{r_i}{2^{s_i}}$ (8)

Frequent Cardinalities (Section 6 & Lemma 3)

$r_1 > r_2 > \cdots > r_{m''} > \varrho$ where ϱ is a constant (11) & (12)

$$p > \frac{1}{n^2} \left(\sum_{k=0}^{C'} (-1)^k \sum_{\substack{k_1 + \cdots + k_{m''} = k \\ k_1 \ge 0, \ldots, k_{m''} \ge 0}} \prod_{i=1}^{m''} \frac{t_i^{k_i}}{k_i!} - \frac{\varepsilon'}{2} \right) \qquad (41)\ \&\ \text{Lemma 4.i}$$

$\Big\downarrow$ multinomial theorem

$$p > \tfrac{1}{n^2} \left(\textstyle\sum_{k=0}^{C'} \frac{\left(-\sum_{i=1}^{m''} t_i\right)^k}{k!} - \frac{\varepsilon'}{2} \right) \qquad (43)$$

$\Big\downarrow$ **Taylor's theorem** (Section 7)

$$p > \tfrac{1}{n^2} \left(e^{-\sum_{i=1}^{m''} t_i} - \mathcal{R}_{C'+1}\left(-\textstyle\sum_{i=1}^{m''} t_i\right) - \frac{\varepsilon'}{2} \right) \qquad (44)$$

$\Big\downarrow$ (2) $\longrightarrow \sum_{i=1}^{m} t_i < \ln \frac{1}{\varepsilon'}$ (10)
Lagrange remainder $\mathcal{R}_{C'+1}\left(-\sum_{i=1}^{m''} t_i\right) < \frac{\varepsilon'}{4}$ (Lemma 4.ii)

$$p > \tfrac{\varepsilon'}{4n^2} > 0 \qquad (51)$$

Fig. 1. The main steps of the proof

concerning almost $\lceil (C+2)\log n \rceil$-wise independence of $\mathcal{A}$ can be applied in the following Section 5. Thus, we confine ourselves to at most logarithmic-size arbitrary subsets R'_j of partition classes R_j, that is

$$R'_j \begin{cases} = R_j & \text{if } |R_j| \leq \log n \\ \subset R_j \text{ so that } |R'_j| = \lfloor \log n \rfloor & \text{otherwise}\,, \end{cases} \tag{6}$$

which ensures $R'_j \subseteq R_j$ and $|R'_j| \leq \log n$ for every $j = 1, \ldots, r$. For these new classes, assumption (2) can be rewritten as

$$\prod_{j=1}^{r} \left(1 - \frac{1}{2^{|R'_j|}}\right) > \left(1 - \frac{1}{2^{\log n}}\right)^{\frac{n}{\log n}} \prod_{|R_j| \leq \log n} \left(1 - \frac{1}{2^{|R_j|}}\right)$$
$$> \left(1 - \frac{1}{n} \cdot \frac{n}{\log n}\right) \varepsilon = \left(1 - \frac{1}{\log n}\right) \varepsilon = \varepsilon'\,, \tag{7}$$

where $\varepsilon' > 0$ is arbitrarily close to ε for sufficiently large n.

Denote by $\{s_1, s_2, \ldots, s_m\} = \{|R'_1|, \ldots, |R'_r|\}$ the set of all cardinalities $1 \leq s_i \leq \log n$ of classes $R'_1, \ldots, R'_r$, and for every $i = 1, \ldots, m$, let $r_i = |\{j \,|\, |R'_j| = s_i\}|$ be the number of classes R'_j having cardinality s_i, that is, $r = \sum_{i=1}^{m} r_i$. Furthermore, we define

$$t_i = \frac{r_i}{2^{s_i}} > 0 \quad \text{for } i = 1, \ldots, m\,. \tag{8}$$

It follows from (7) and (8) that

$$0 < \varepsilon' < \prod_{j=1}^{r} \left(1 - \frac{1}{2^{|R'_j|}}\right) = \prod_{i=1}^{m} \left(\left(1 - \frac{1}{2^{s_i}}\right)^{2^{s_i}}\right)^{t_i} < e^{-\sum_{i=1}^{m} t_i} \tag{9}$$

implying

$$\sum_{i=1}^{m} t_i < \ln \frac{1}{\varepsilon'}\,. \tag{10}$$

Moreover, we define constants

$$\varrho = \frac{C}{1 - \left(1 - \frac{\varepsilon'^2}{4(1+\varepsilon'^2)}\right)^{\frac{1}{C}}} > C \geq 1\,, \qquad \sigma = \log\left(\frac{4\varrho\,(1+\varepsilon'^2)}{\varepsilon'^2}\right) \tag{11}$$

which are used for sorting the cardinalities $s_1, \ldots, s_m$ so that

$$r_i > \varrho \text{ and } s_i > \sigma \quad \text{for} \quad i = 1, \ldots, m'' \tag{12}$$
$$r_i \leq \varrho \text{ and } s_i > \sigma \quad \text{for} \quad i = m''+1, \ldots, m' \tag{13}$$
$$s_i \leq \sigma \quad \text{for} \quad i = m'+1, \ldots, m\,. \tag{14}$$

We will further confine ourselves to the first $m' \geq 0$ cardinalities satisfying $s_i > \sigma$ for $i = 1, \ldots, m'$. Without loss of generality, we can also sort the corresponding partition classes so that $|R'_j| > \sigma$ for $j = 1, \ldots, r'$, whereas $|R'_j| \leq \sigma$ for $j = r'+1, \ldots, r$, which implies

$$r' = \sum_{i=1}^{m'} r_i = \sum_{i=1}^{m'} t_i 2^{s_i} > \frac{4\varrho\,(1+\varepsilon'^2)}{\varepsilon'^2} \sum_{i=1}^{m'} t_i \tag{15}$$

according to (8), (12)–(13), and (11). We include the remaining constant-size classes R'_j for $j = r'+1, \ldots, r$ into Q, that is,

$$Q' = Q \cup \bigcup_{j=r'+1}^{r} R'_j \tag{16}$$

whose size can be upper bounded as

$$|Q'| \leq \log n + \sum_{i=m'+1}^{m} r_i \log\left(\frac{4\varrho\,(1+\varepsilon'^2)}{\varepsilon'^2}\right) < 2\log n \tag{17}$$

for sufficiently large n, since

$$\sum_{i=m'+1}^{m} r_i = \sum_{i=m'+1}^{m} t_i 2^{s_i} < \frac{4\varrho\,(1+\varepsilon'^2)}{\varepsilon'^2} \ln\frac{1}{\varepsilon'} \tag{18}$$

according to (8), (10), (14), and (11). This completes the definition of new classes $Q', R'_1, \ldots, R'_{r'}$. In addition, we define $\mathbf{c}' \in \{0,1\}^n$ that differs from $\mathbf{c}$ exactly on the constant number of bit locations from $R'_{r'+1}, \ldots, R'_r$, e.g.

$$c'_i = \begin{cases} 1 - c_i & \text{if } i \in \bigcup_{j=r'+1}^{r} R'_j \\ c_i & \text{otherwise.} \end{cases} \tag{19}$$

The modified $Q', R'_1, \ldots, R'_{r'}$ and $\mathbf{c}'$ are used in the following lemma for lower bounding the probability (5).

Lemma 1.

$$p \geq \frac{\left|\mathcal{A}_n^{Q'}(\mathbf{c}') \setminus \bigcup_{j=1}^{r'} \mathcal{A}_n^{R'_j}(\mathbf{c}')\right|}{|\mathcal{A}_n|} = \frac{\left|\mathcal{A}_n^{Q'}(\mathbf{c}')\right|}{|\mathcal{A}_n|} - \frac{\left|\bigcup_{j=1}^{r'} \mathcal{A}_n^{R'_j \cup Q'}(\mathbf{c}')\right|}{|\mathcal{A}_n|}\,. \tag{20}$$

Proof. For verifying the lower bound in (20) it suffices to show that $\mathcal{A}_n^{Q'}(\mathbf{c}') \setminus \bigcup_{j=1}^{r'} \mathcal{A}_n^{R'_j}(\mathbf{c}') \subseteq \mathcal{A}_n^{Q}(\mathbf{c}) \setminus \bigcup_{j=1}^{r} \mathcal{A}_n^{R_j}(\mathbf{c})$ according to (5). Assume $\mathbf{a} \in \mathcal{A}_n^{Q'}(\mathbf{c}') \setminus \bigcup_{j=1}^{r'} \mathcal{A}_n^{R'_j}(\mathbf{c}')$, which means $\mathbf{a} \in \mathcal{A}_n^{Q'}(\mathbf{c}') \subseteq \mathcal{A}_n^{Q}(\mathbf{c}') = \mathcal{A}_n^{Q}(\mathbf{c})$ and $\mathbf{a} \notin \mathcal{A}_n^{R'_j}(\mathbf{c}') = \mathcal{A}_n^{R'_j}(\mathbf{c}) \supseteq \mathcal{A}_n^{R_j}(\mathbf{c})$ for every $j = 1, \ldots, r'$ by definitions (6), (16), (19), and the fact that $S_1 \subseteq S_2$ implies $\mathcal{A}_n^{S_2}(\mathbf{c}) \subseteq \mathcal{A}_n^{S_1}(\mathbf{c})$. In addition, $\mathbf{a} \in \mathcal{A}_n^{Q'}(\mathbf{c}')$ implies $\mathbf{a} \notin \mathcal{A}_n^{R_j}(\mathbf{c})$ for every $j = r'+1, \ldots, r$ according to (19), and hence, $\mathbf{a} \in \mathcal{A}_n^{Q}(\mathbf{c}) \setminus \bigcup_{j=1}^{r} \mathcal{A}_n^{R_j}(\mathbf{c})$. This completes the proof of the lower bound, while the equality in (20) follows from $\mathcal{A}_n^{R'_j \cup Q'}(\mathbf{c}') \subseteq \mathcal{A}_n^{Q'}(\mathbf{c}')$ for every $j = 1, \ldots, r'$. □

5 Almost k-Wise Independence

Furthermore, we will upper bound the probability of the finite union of events appearing in formula (20) by using Bonferroni inequality for constant number $C' = \min(C, r')$ of terms, which gives

$$p \geq \frac{\left|\mathcal{A}_n^{Q'}(\mathbf{c}')\right|}{|\mathcal{A}_n|} - \sum_{k=1}^{C'} (-1)^{k+1} \sum_{1 \leq j_1 < j_2 < \cdots < j_k \leq r'} \frac{\left|\bigcap_{i=1}^{k} \mathcal{A}_n^{R'_{j_i} \cup Q'}(\mathbf{c}')\right|}{|\mathcal{A}_n|} \tag{21}$$

$$= \sum_{k=0}^{C'} (-1)^k \sum_{1 \leq j_1 < j_2 < \cdots < j_k \leq r'} \frac{\left|\mathcal{A}_n^{\bigcup_{i=1}^{k} R'_{j_i} \cup Q'}(\mathbf{c}')\right|}{|\mathcal{A}_n|} \tag{22}$$

according to Lemma 1. For notational simplicity, the inner sum in (22) over $1 \leq j_1 < j_2 < \cdots < j_k \leq r'$ for $k = 0$ reads formally as it includes one summand $|\mathcal{A}_n^{Q'}(\mathbf{c}')|/|\mathcal{A}_n|$. Note that C' is odd for $C < r'$, while equality holds in (21) for $C' = r'$, which is the probabilistic inclusion-exclusion principle. For any $0 \leq k \leq C' \leq C$, we know $\left|\bigcup_{i=1}^{k} R'_{j_i} \cup Q'\right| \leq \lceil (C+2) \log n \rceil$ according to (6) and (17), and hence,

$$\frac{\left|\mathcal{A}_n^{\bigcup_{i=1}^{k} R'_{j_i} \cup Q'}(\mathbf{c}')\right|}{|\mathcal{A}_n|} \geq \frac{1}{2^{|Q'| + \sum_{i=1}^{k} \left|R'_{j_i}\right|}} - \beta = \frac{1}{2^{|Q'|}} \prod_{i=1}^{k} \frac{1}{2^{\left|R'_{j_i}\right|}} - \beta \tag{23}$$

(where the product in (23) equals formally 1 for $k = 0$) and similarly,

$$-\frac{\left|\mathcal{A}_n^{\bigcup_{i=1}^{k} R'_{j_i} \cup Q'}(\mathbf{c}')\right|}{|\mathcal{A}_n|} \geq -\frac{1}{2^{|Q'|}} \prod_{i=1}^{k} \frac{1}{2^{\left|R'_{j_i}\right|}} - \beta \tag{24}$$

according to (4) since $\mathcal{A}$ is $(\lceil (C+2) \log n \rceil, \beta)$-wise independent. We plug these inequalities into (22), which leads to

$$\begin{aligned} p &\geq \sum_{k=0}^{C'} (-1)^k \sum_{1 \leq j_1 < j_2 < \cdots < j_k \leq r'} \frac{1}{2^{|Q'|}} \prod_{i=1}^{k} \frac{1}{2^{\left|R'_{j_i}\right|}} - \beta \sum_{k=0}^{C'} \binom{r'}{k} \\ &\geq \frac{1}{2^{|Q'|}} \left(\sum_{k=0}^{C'} (-1)^k \sum_{1 \leq j_1 < j_2 < \cdots < j_k \leq r'} \prod_{i=1}^{k} \frac{1}{2^{\left|R'_{j_i}\right|}} - \beta \, 2^{|Q'|} \, (r'+1)^{C'} \right), \end{aligned} \tag{25}$$

where

$$\beta \, 2^{|Q'|} \, (r'+1)^{C'} < \frac{1}{n^{C+3}} \, n^2 \, n^C = \frac{1}{n} < \frac{\varepsilon'}{8} \tag{26}$$

for sufficiently large $n > 8/\varepsilon'$ by using the assumption on β, inequality (17), $r' < n$ (e.g., $r' = n$ would break (11)–(13)), and $C' \leq C$. The following lemma rewrites the inner sum in formula (25).

Lemma 2. *For $0 \le k \le C'$,*

$$\sum_{1 \le j_1 < j_2 < \cdots < j_k \le r'} \prod_{i=1}^{k} \frac{1}{2^{|R'_{j_i}|}} = \sum_{\substack{k_1+\cdots+k_{m'}=k \\ 0 \le k_1 \le r_1, \ldots, 0 \le k_{m'} \le r_{m'}}} \prod_{i=1}^{m'} \frac{t_i^{k_i}}{k_i!} \prod_{j=1}^{k_i-1} \left(1 - \frac{j}{r_i}\right) . \tag{27}$$

Proof. By grouping the classes of the same cardinality together, the left-hand side of inequality (27) can be rewritten as

$$\sum_{1 \le j_1 < j_2 < \cdots < j_k \le r'} \prod_{i=1}^{k} \frac{1}{2^{|R'_{j_i}|}} = \sum_{\substack{k_1+k_2+\cdots+k_{m'}=k \\ 0 \le k_1 \le r_1, \ldots, 0 \le k_{m'} \le r_{m'}}} \prod_{i=1}^{m'} \binom{r_i}{k_i} \left(\frac{1}{2^{s_i}}\right)^{k_i} , \tag{28}$$

where $k_1, \ldots, k_{m'}$ denote the numbers of classes of corresponding cardinalities $s_1, \ldots, s_{m'}$ considered in a current summand, and

$$\binom{r_i}{k_i} \left(\frac{1}{2^{s_i}}\right)^{k_i} = \frac{r_i\,(r_i-1)\cdots(r_i-k_i+1)}{k_i!} \left(\frac{t_i}{r_i}\right)^{k_i} = \frac{t_i^{k_i}}{k_i!} \prod_{j=1}^{k_i-1} \left(1 - \frac{j}{r_i}\right) \tag{29}$$

according to (8). □

Thus, we plug equations (26) and (27) into (25) and obtain

$$p > \frac{1}{n^2} \left(\sum_{k=0}^{C'} (-1)^k \sum_{\substack{k_1+\cdots+k_{m'}=k \\ 0 \le k_1 \le r_1, \ldots, 0 \le k_{m'} \le r_{m'}}} \prod_{i=1}^{m'} \frac{t_i^{k_i}}{k_i!} \prod_{j=1}^{k_i-1} \left(1 - \frac{j}{r_i}\right) - \frac{\varepsilon'}{8} \right) . \tag{30}$$

Note that for $m' = 0$ (implying $r' = C' = 0$), the inner sum in (30) equals 1.

6 Frequent Cardinalities

We sort out the terms with frequent cardinalities (12) from the sum in formula (30), that is,

$$p > \frac{1}{n^2} \left(\sum_{k=0}^{C'} (-1)^k \sum_{\substack{k_1+\cdots+k_{m''}=k \\ 0 \le k_1 \le r_1, \ldots, 0 \le k_{m''} \le r_{m''}}} \prod_{i=1}^{m''} \frac{t_i^{k_i}}{k_i!} \prod_{j=1}^{k_i-1} \left(1 - \frac{j}{r_i}\right) - T_1 - \frac{\varepsilon'}{8} \right) , \tag{31}$$

where the inner sum in (31) equals zero for $k > r'' = \sum_{i=1}^{m''} r_i$, and

$$T_1 = \sum_{k=0}^{C'} (-1)^{k+1} \sum_{\substack{k_1+\cdots+k_{m'}=k \\ 0 \le k_1 \le r_1, \ldots, 0 \le k_{m'} \le r_{m'} \\ (\exists\, m''+1 \le \ell \le m')\, k_\ell > 0}} \prod_{i=1}^{m'} \frac{t_i^{k_i}}{k_i!} \prod_{j=1}^{k_i-1} \left(1 - \frac{j}{r_i}\right) \tag{32}$$

sums up the terms including rare cardinalities (13). In addition, we know

$$1 \geq \prod_{i=1}^{m''} \prod_{j=1}^{k_i-1} \left(1 - \frac{j}{r_i}\right) > \left(1 - \frac{C}{\varrho}\right)^C = 1 - \frac{\varepsilon'^2}{4(1+\varepsilon'^2)} \tag{33}$$

according to (12), (11), and $k_i \leq k = \sum_{i=1}^{m''} k_i \leq C' \leq C < \varrho$. The upper and lower bound (33) on the underlying product are used to lower bound the negative terms of (31) for odd k and the positive terms for even k, respectively, that is,

$$p > \frac{1}{n^2} \left(\sum_{k=0}^{C'} (-1)^k \sum_{\substack{k_1+\cdots+k_{m''}=k \\ 0 \leq k_1 \leq r_1, \ldots, 0 \leq k_{m''} \leq r_{m''}}} \prod_{i=1}^{m''} \frac{t_i^{k_i}}{k_i!} - \frac{\varepsilon'^2}{4(1+\varepsilon'^2)} T_2 - T_1 - \frac{\varepsilon'}{8} \right) \tag{34}$$

where

$$T_2 = \sum_{k=0,2,4,\ldots}^{C'} \sum_{\substack{k_1+\cdots+k_{m''}=k \\ 0 \leq k_1 \leq r_1, \ldots, 0 \leq k_{m''} \leq r_{m''}}} \prod_{i=1}^{m''} \frac{t_i^{k_i}}{k_i!} \,. \tag{35}$$

The following lemma upper bounds the above-introduced terms T_1 and T_2.

Lemma 3.
(i) $T_1 < \frac{\varepsilon'}{8}$.
(ii) $T_2 < \frac{1+\varepsilon'^2}{2\,\varepsilon'}$.

Proof.
(i) We can only take the terms of (32) for odd $k = 1, 3, 5, \ldots$ into account since those for even k are nonpositive (e.g. the term for $k = 0$ equals zero because there is no $m'' + 1 \leq \ell \leq m'$ such that $k_\ell > 0$ in this case). Thus,

$$\begin{aligned} T_1 &\leq \sum_{k=1,3,5,\ldots}^{C'} \sum_{\substack{k_1+\cdots+k_{m'}=k \\ 0 \leq k_1 \leq r_1, \ldots, 0 \leq k_{m'} \leq r_{m'} \\ (\exists\, m''+1 \leq \ell \leq m')\, k_\ell > 0}} \frac{r_\ell}{2^{s_\ell}} \frac{1}{k_\ell} \frac{t_\ell^{k_\ell - 1}}{(k_\ell - 1)!} \prod_{\substack{i=1 \\ i \neq \ell}}^{m'} \frac{t_i^{k_i}}{k_i!} \\ &\leq \frac{\varrho}{2^\sigma} \sum_{k=1,3,5,\ldots}^{C'} \sum_{\substack{k_1+\cdots+k_{m'}=k \\ 0 \leq k_1 \leq r_1, \ldots, 0 \leq k_{m'} \leq r_{m'} \\ (\exists\, m''+1 \leq \ell \leq m')\, k_\ell > 0}} \frac{t_\ell^{k_\ell - 1}}{(k_\ell - 1)!} \prod_{\substack{i=1 \\ i \neq \ell}}^{m'} \frac{t_i^{k_i}}{k_i!} \end{aligned} \tag{36}$$

according to (8) and (13). Formula (36) is rewritten by replacing indices $k_\ell - 1$ and $k - 1$ with k_ℓ and k, respectively, which is further upper bounded by removing the upper bounds that are set on indices $k_1, \ldots, k_{m'}$ and by omitting the condition concerning the existence of special index ℓ, as follows:

$$T_1 \leq \frac{\varrho}{2^\sigma} \sum_{k=0,2,4,\ldots}^{C'-1} \sum_{\substack{k_1+\cdots+k_{m'}=k \\ k_1 \geq 0, \ldots, k_{m'} \geq 0}} \prod_{i=1}^{m'} \frac{t_i^{k_i}}{k_i!} = \frac{\varrho}{2^\sigma} \sum_{k=0,2,4,\ldots}^{C'-1} \frac{\left(\sum_{i=1}^{m'} t_i\right)^k}{k!} \,, \tag{37}$$

where the multinomial theorem is employed. Notice that the sum on the right-hand side of equation (37) represents the first few terms of Taylor series of the hyperbolic cosine at point $\sum_{i=1}^{m'} t_i \geq 0$, which implies

$$T_1 < \frac{\varrho}{2^\sigma} \cosh\left(\sum_{i=1}^{m'} t_i\right) < \frac{\varepsilon'^2}{4(1+\varepsilon'^2)} \cdot \frac{\frac{1}{\varepsilon'} + \varepsilon'}{2} = \frac{\varepsilon'}{8} \tag{38}$$

according to (10) and (11) since the hyperbolic cosine is an increasing function for nonnegative arguments.

(ii) Similarly as in the proof of (i), we apply the multinomial theorem (cf. (37)) and the Taylor series of the hyperbolic cosine (cf. (38)) to (35), which gives

$$T_2 \leq \sum_{k=0,2,4,\ldots}^{C'} \sum_{\substack{k_1+\cdots+k_{m''}=k \\ k_1\geq 0,\ldots,k_{m''}\geq 0}} \prod_{i=1}^{m''} \frac{t_i^{k_i}}{k_i!} \leq \cosh\left(\sum_{i=1}^{m''} t_i\right) < \frac{1+\varepsilon'^2}{2\,\varepsilon'}\,. \tag{39}$$

□

We plug the bounds from Lemma 3 into (34) and obtain

$$p > \frac{1}{n^2}\left(\sum_{k=0}^{C'}(-1)^k \sum_{\substack{k_1+\cdots+k_{m''}=k \\ 0\leq k_1\leq r_1,\ldots,0\leq k_{m''}\leq r_{m''}}} \prod_{i=1}^{m''} \frac{t_i^{k_i}}{k_i!} - \frac{3\,\varepsilon'}{8}\right). \tag{40}$$

7 Taylor's Theorem

In order to apply the multinomial theorem again, we remove the upper bounds that are set on indices in the inner sum of formula (40), that is,

$$p > \frac{1}{n^2}\left(\sum_{k=0}^{C'}(-1)^k \sum_{\substack{k_1+\cdots+k_{m''}=k \\ k_1\geq 0,\ldots,k_{m''}\geq 0}} \prod_{i=1}^{m''} \frac{t_i^{k_i}}{k_i!} - T - \frac{3\,\varepsilon'}{8}\right), \tag{41}$$

which is corrected by introducing additional term

$$T = \sum_{k=0}^{C'}(-1)^k \sum_{\substack{k_1+\cdots+k_{m''}=k \\ k_1\geq 0,\ldots,k_{m''}\geq 0 \\ (\exists 1\leq \ell\leq m'')\, k_\ell > r_\ell}} \prod_{i=1}^{m''} \frac{t_i^{k_i}}{k_i!}\,. \tag{42}$$

Thus, inequality (41) can be further rewritten as

$$p > \frac{1}{n^2}\left(\sum_{k=0}^{C'} \frac{\left(-\sum_{i=1}^{m''} t_i\right)^k}{k!} - T - \frac{3\,\varepsilon'}{8}\right) \tag{43}$$

$$= \frac{1}{n^2}\left(e^{-\sum_{i=1}^{m''} t_i} - \mathcal{R}_{C'+1}\left(-\sum_{i=1}^{m''} t_i\right) - T - \frac{3\,\varepsilon'}{8}\right)\,, \tag{44}$$

where Taylor's theorem is employed for the exponential function at point $-\sum_{i=1}^{m''} t_i$ producing the Lagrange remainder

$$\mathcal{R}_{C'+1}\left(-\sum_{i=1}^{m''} t_i\right) = \frac{\left(-\sum_{i=1}^{m''} t_i\right)^{C'+1}}{(C'+1)!}\, e^{-\vartheta \sum_{i=1}^{m''} t_i} < \left(\frac{\sum_{i=1}^{m''} t_i}{\sqrt{C'}}\right)^{C'+1} \tag{45}$$

with parameter $0 < \vartheta < 1$. Note that the upper bound in (45) assumes $C' > 0$, whereas for $C' = r' = 0$ implying $m'' = m' = 0$, we know $\mathcal{R}_1(0) = 0$. This remainder together with term T are upper bounded in the following lemma.

Lemma 4.
(i) $T < \frac{\varepsilon'}{8}$.
(ii) $\mathcal{R}_{C'+1}\left(-\sum_{i=1}^{m''} t_i\right) < \frac{\varepsilon'}{4}$.

Proof.
(i) We take only the summands of (42) for even $k \geq 2$ into account since the summands for odd k are not positive, while for $k = 0$ there is no $1 \leq \ell \leq m''$ such that $0 = k \geq k_\ell > r_\ell \geq 1$, which gives

$$T \leq \sum_{k=2,4,6,\ldots}^{C'} \sum_{\substack{k_1+\cdots+k_{m''}=k \\ k_1\geq 0,\ldots,k_{m''}\geq 0 \\ (\exists 1\leq \ell \leq m'')\, k_\ell > r_\ell}} \frac{1}{2^{s_\ell}}\, \frac{r_\ell}{k_\ell}\, \frac{t_\ell^{k_\ell - 1}}{(k_\ell - 1)!} \prod_{\substack{i=1 \\ i\neq \ell}}^{m''} \frac{t_i^{k_i}}{k_i!}$$

$$\leq \frac{1}{2^\sigma} \sum_{k=2,4,6,\ldots}^{C'} \sum_{\substack{k_1+\cdots+k_{m''}=k \\ k_1\geq 0,\ldots,k_{m''}\geq 0 \\ (\exists 1\leq \ell \leq m'')\, k_\ell > r_\ell}} \frac{t_\ell^{k_\ell - 1}}{(k_\ell - 1)!} \prod_{\substack{i=1 \\ i\neq \ell}}^{m''} \frac{t_i^{k_i}}{k_i!} \tag{46}$$

using (8) and (12). Formula (46) is rewritten by replacing indices $k_\ell - 1$ and $k - 1$ with k_ℓ and k, respectively, which is further upper bounded by omitting the condition concerning the existence of special index ℓ, as follows:

$$T \leq \frac{1}{2^\sigma} \sum_{k=1,3,5,\ldots}^{C'-1} \sum_{\substack{k_1+\cdots+k_{m''}=k \\ k_1\geq 0,\ldots,k_{m''}\geq 0}} \prod_{i=1}^{m''} \frac{t_i^{k_i}}{k_i!} = \frac{1}{2^\sigma} \sum_{k=1,3,5,\ldots}^{C'-1} \frac{\left(\sum_{i=1}^{m''} t_i\right)^k}{k!}\,, \tag{47}$$

where the multinomial theorem is employed. Notice that the sum on the right-hand side of equation (47) represents the first few terms of Taylor series of the hyperbolic sine at point $\sum_{i=1}^{m''} t_i$, which implies

$$T \leq \frac{1}{2^\sigma} \sinh\left(\sum_{i=1}^{m''} t_i\right) < \frac{\varepsilon'^2}{4\varrho\,(1+\varepsilon'^2)} \cdot \frac{\frac{1}{\varepsilon'} - \varepsilon'}{2} < \frac{\varepsilon'}{8} \tag{48}$$

according to (10) and (11) since the hyperbolic sine is an increasing function.

(ii) For $C' = C \geq 1$, Lagrange remainder (45) can further be upper bounded as

$$\mathcal{R}_{C'+1}\left(-\sum_{i=1}^{m''} t_i\right) < \left(\frac{\ln\frac{1}{\varepsilon'}}{\sqrt{C}}\right)^{C+1} < \left(\frac{\varepsilon'}{2}\right)^{C+1} < \frac{\varepsilon'}{4} \tag{49}$$

for sufficiently large n by using (10) and the definition of C, while for $C' = r' < C$, the underlying upper bound

$$\mathcal{R}_{C'+1}\left(-\sum_{i=1}^{m''} t_i\right) \leq \left(\frac{\sum_{i=1}^{m'} t_i}{\frac{4\varrho\,(1+\varepsilon'^2)}{\varepsilon'^2}}\right)^{\frac{r'+1}{2}} < \frac{\ln\frac{1}{\varepsilon'}}{\frac{4\varrho\,(1+\varepsilon'^2)}{\varepsilon'^2}} < \frac{\varepsilon'}{4} \tag{50}$$

can be obtained from (15) and (10). □

Finally, inequality (9) together with the upper bounds from Lemma 4 are plugged into (44), which leads to

$$p > \frac{\varepsilon'}{4n^2} = \frac{\varepsilon}{4n^2}\left(1 - \frac{1}{\log n}\right) > 0 \tag{51}$$

according to (7). Thus, we have proven that for any $\mathbf{c} \in \{0,1\}^n$ the probability that there is $\mathbf{a} \in \mathcal{A}_n$ satisfying the conjunction (3) for Q and partition $\{R_1, \ldots, R_r\}$ is strictly positive, which means such $\mathbf{a}$ does exist. This completes the proof that $\mathcal{A}$ is ε-rich. □

8 Conclusion

In the present paper, we have made an important step in the effort to construct hitting set generators for the model of read-once branching programs of bounded width. Such constructions have so far been known only in the case of width 2 and in very restricted cases of bounded width (e.g. permutation or regular oblivious read-once branching programs). We have now provided an explicit polynomial-time construction of a hitting set for read-once branching programs of width 3 with the acceptance probability greater than $\sqrt{12/13}$. From the point of view of derandomization of unrestricted models, our result still appears to be unsatisfactory. The issue of whether our technique based on the richness condition can be extended to the case of width 4 or to bounded width represents an open problem for further research. Another challenge for improving our result is to optimize parameter ε, e.g. to achieve the result for $\varepsilon \leq \frac{1}{n}$, which would be important for practical derandomizations.

References

1. Alon, N., Goldreich, O., Håstad, J., and Peralta, R.: Simple constructions of almost k-wise independent random variables. Random Structures and Algorithms **3** (3) (1992) 289–304
2. Bogdanov, A., Dvir, Z., Verbin, E., Yehudayoff, A.: Pseudorandomness for width 2 branching programs. ECCC Report No. **70** (2009)
3. Braverman, M., Rao, A., Raz, R., Yehudayoff, A.: Pseudorandom generators for regular branching programs. Proceedings of the FOCS 2010 Fifty-First Annual IEEE Symposium on Foundations of Computer Science (2010) 41–50
4. Brody, J., Verbin, E.: The coin problem, and pseudorandomness for branching programs. Proceedings of the FOCS 2010 Fifty-First Annual IEEE Symposium on Foundations of Computer Science (2010) 30–39
5. De, A., Etesami, O., Trevisan, L., Tulsiani, M.: Improved pseudorandom generators for depth 2 circuits. Proceedings of the RANDOM 2010 Fourteenth International Workshop on Randomization and Computation, LNCS **6302**, Springer-Verlag, Berlin (2010) 504–517
6. 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
7. Koucký, M., Nimbhorkar, P., Pudlák, P: Pseudorandom generators for group products. To appear in Proceedings of the STOC 2011 Forty-Third ACM Symposium on Theory of Computing, ACM, New York, NY (2011)
8. Meka, R., Zuckerman, D.: Pseudorandom generators for polynomial threshold functions. Proceedings of the STOC 2010 Forty-Second ACM Symposium on Theory of Computing, ACM, New York, NY (2010) 427–436
9. Nisan, N.: Pseudorandom generators for space-bounded computation. Combinatorica **12** (4) (1992) 449–461
10. Nisan, N., Wigderson, A.: Hardness vs. randomness. Journal of Computer and System Sciences **49** (2) (1994) 149–167
11. 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
12. Šíma, J., Žák, S.: A polynomial time construction of a hitting set for read-once branching programs of width 3. ECCC Report No. **88** (2010)
13. Šíma, J., Žák, S.: A sufficient condition for sets hitting the class of read-once branching programs of width 3. (submitted)
14. Wegener, I.: Branching Programs and Binary Decision Diagrams—Theory and Applications. SIAM Monographs on Discrete Mathematics and Its Applications, SIAM, Philadelphia, PA (2000)