On Pseudorandomness and Resource-Bounded Measure*

V. Arvind
Institute of Mathematical Sciences
C. I. T. Campus
Chennai 600 113, India

Johannes Köbler
Abteilung Theoretische Informatik,
Universität Ulm,
D-89069 Ulm, Germany

Abstract

In this paper we extend a key result of Nisan and Wigderson [NW94] to the nondeterministic setting: for all $\alpha > 0$ we show that if there is a language in $\mathrm{E} = \mathrm{DTIME}(2^{O(n)})$ that is hard to approximate by nondeterministic circuits of size $2^{\alpha n}$, then there is a pseudorandom generator that can be used to derandomize $\mathrm{BP} \cdot \mathrm{NP}$ (in symbols, $\mathrm{BP} \cdot \mathrm{NP} = \mathrm{NP}$).

By applying this extension we are able to answer some open questions in [Lut97] regarding the derandomization of the classes $\mathrm{BP} \cdot \Sigma_k^{\mathrm{P}}$ and $\mathrm{BP} \cdot \Theta_k^{\mathrm{P}}$ under plausible measure theoretic assumptions. As a consequence, if Θ_2^{P} does not have p-measure 0, then $\mathrm{AM} \cap \mathrm{coAM}$ is low for Θ_2^{P}. Thus, in this case, the graph isomorphism problem is low for Θ_2^{P}. By using the Nisan-Wigderson design of a pseudorandom generator we unconditionally show the inclusion $\mathrm{MA} \subseteq \mathrm{ZPP}^{\mathrm{NP}}$ and that $\mathrm{MA} \cap \mathrm{coMA}$ is low for $\mathrm{ZPP}^{\mathrm{NP}}$.

1 Introduction

In recent years, following the development of resource-bounded measure theory, pioneered by Lutz [Lut92, Lut93], plausible complexity-theoretic assumptions like $\mathrm{P} \neq \mathrm{NP}$ have been replaced by the possibly stronger, but arguably plausible measure-theoretic assumption

*Preliminary versions of this paper appeared as Ulmer Informatik-Bericht Nr. 97-05 [AK97a] and in the Proceedings of the 17th Conference on Foundations of Software Technology and Theoretical Computer Science [AK97b].

$\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$. With this assumption as hypothesis, a number of interesting complexity-theoretic conclusions have been derived, which are not known to follow from $\mathrm{P} \neq \mathrm{NP}$. Two prominent examples of such results are: there are Turing-complete sets for NP that are not many-one complete [LM96], there are NP problems for which search does not reduce to decision [LM96, BG94].

Recently, Lutz [Lut97] has shown that the hypothesis $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ (in fact, the possibly weaker hypothesis $\mu_{\mathrm{p}}(\Delta_k^{\mathrm{P}}) \neq 0$, $k \geq 2$) implies that $\mathrm{BP} \cdot \Delta_k^{\mathrm{P}} = \Delta_k^{\mathrm{P}}$ (in other words, $\mathrm{BP} \cdot \Delta_k^{\mathrm{P}}$ can be derandomized). This has an improved lowness consequence: it follows that if $\mu_{\mathrm{p}}(\Delta_2^{\mathrm{P}}) \neq 0$ then $\mathrm{AM} \cap \mathrm{coAM}$ is low for Δ_2^{P} (i.e., any $\mathrm{AM} \cap \mathrm{coAM}$ language is powerless as oracle to Δ_2^{P} machines). It also follows from $\mu_{\mathrm{p}}(\Delta_2^{\mathrm{P}}) \neq 0$ that if $\mathrm{NP} \subseteq \mathrm{P/poly}$ then $\mathrm{PH} = \Delta_2^{\mathrm{P}}$. Thus the results of Lutz's paper [Lut97] have opened up a study of derandomization of randomized complexity classes and new lowness properties under assumptions about the resource-bounded measure of different complexity classes.

The results of Lutz in [Lut97] (and also a preceding paper [Lut93]) are intimately related to research on derandomizing randomized algorithms based on the idea of trading hardness for randomness [Sha81, Yao82, NW94]. In particular, Lutz makes essential use of the explicit design of a pseudorandom generator that stretches a short random string to a long pseudorandom string that looks random to *deterministic* polynomial-size circuits. More precisely, the Nisan-Wigderson generator is built from a set (assumed to exist) that is in E and, for some $\alpha > 0$, *is hard to approximate* by circuits of size $2^{\alpha n}$. As shown in [NW94], such a pseudorandom generator can be used to derandomize BPP.

In Section 3 of the present paper we extend the just mentioned result of Nisan and Wigderson to the nondeterministic setting. We show that their generator can also be used to derandomize the Arthur-Merlin class $\mathrm{AM} = \mathrm{BP} \cdot \mathrm{NP}$, provided it is built from a set in E that is hard to approximate by *nondeterministic* circuits of size $2^{\alpha n}$ for some $\alpha > 0$. Very recently [IW97], the result of Nisan and Wigderson has been improved by weakening the assumption that there exists a set A in E that is hard to approximate: it actually suffices that A has *worst-case* circuit complexity $2^{\Omega(n)}$. We leave it as an open question whether a similar improvement is possible for the non-deterministic case. (For related results on derandomizing BPP see [ACR96, ACR97].)

In Section 4 we apply our extension of the Nisan and Wigderson result to the non-deterministic case to answer some questions left open by Lutz in [Lut97]. We show that for all $k \geq 2$, $\mu_{\mathrm{p}}(\Sigma_k^{\mathrm{P}} \cap \Pi_k^{\mathrm{P}}) \neq 0$ implies $\mathrm{BP} \cdot \Sigma_k^{\mathrm{P}} = \Sigma_k^{\mathrm{P}}$ (see Figs. 1 and 2 for a comparison of the known inclusion structure with the inclusion structure of these classes if $\mu_{\mathrm{p}}(\Delta_2^{\mathrm{P}}) \neq 0$). Furthermore, we show under the possibly stronger assumption $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ that with the help of a logarithmic number of advice bits also $\mathrm{BP} \cdot \mathrm{NP}$ can be derandomized (i.e., $\mathrm{BP} \cdot \mathrm{NP} \subseteq \mathrm{NP}/\log$). Under the hypothesis $\mu_{\mathrm{p}}(\mathrm{NP} \cap \mathrm{coNP}) \neq 0$ we are able to prove that indeed $\mathrm{BP} \cdot \mathrm{NP} = \mathrm{NP}$ which has some immediate strong implications as, for example, Graph Isomorphism is in $\mathrm{NP} \cap \mathrm{coNP}$.

Relatedly, in Section 5 we show that for all $k \geq 2$, $\mu_{\mathrm{p}}(\Theta_k^{\mathrm{P}}) \neq 0$ implies $\mathrm{BP} \cdot \Theta_k^{\mathrm{P}} = \Theta_k^{\mathrm{P}}$, answering an open problem stated in [Lut97]. Thus, $\mu_{\mathrm{p}}(\Theta_2^{\mathrm{P}}) \neq 0$ has the remarkable consequence that $\mathrm{AM} \cap \mathrm{coAM}$ (and consequently the graph isomorphism problem) is low for Θ_2^{P}.

Finally, we show in Section 6 that the Arthur-Merlin class MA is contained in $\mathrm{ZPP}^{\mathrm{NP}}$ and that $\mathrm{MA} \cap \mathrm{coMA}$ is even low for $\mathrm{ZPP}^{\mathrm{NP}}$.

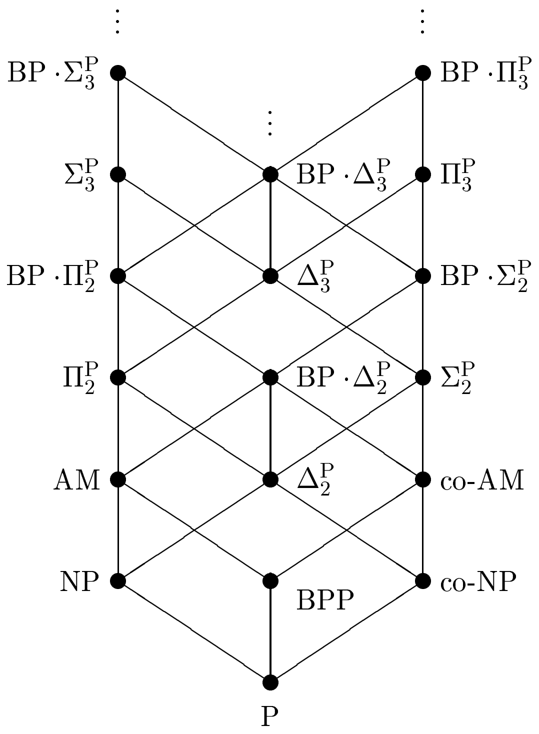

Fig. 1. Known inclusion structure

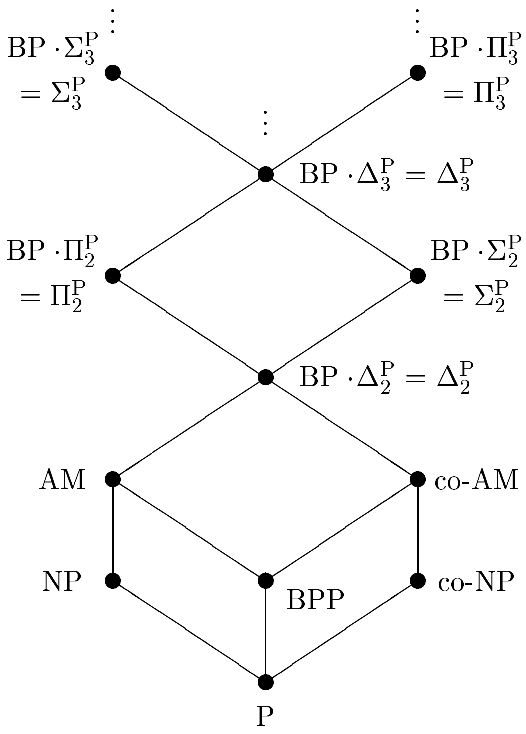

Fig. 2. Inclusion structure if $\mu_{\mathrm{p}}(\Delta_2^{\mathrm{P}}) \neq 0$

2 Preliminaries

In this section we give formal definitions and describe the results of Nisan and Wigderson [NW94] and of Lutz [Lut97] which we generalize in this paper.

We use the binary alphabet $\Sigma = \{0, 1\}$. The cardinality of a finite set X is denoted by $\|X\|$ and the length of $x \in \Sigma^*$ by $|x|$. The complement of a set $A \subseteq \Sigma^*$ is denoted by $\bar{A} = \{x \in \Sigma^* \mid x \notin A\}$. For a class C of sets we denote by co-C the class $\{\bar{A} \mid A \in \mathrm{C}\}$. The join $A \oplus B$ of two sets A and B is defined as $A \oplus B = \{0x \mid x \in A\} \cup \{1x \mid x \in B\}$. The characteristic function of a set $L \subseteq \Sigma^*$ is defined as $L(x) = 1$ if $x \in L$, and $L(x) = 0$ otherwise. The restriction of $L(x)$ to strings of length n can be considered as an n-ary boolean function that we denote by $L^{=n}$. Conversely, each n-ary boolean function g defines a finite language $\{x \in \Sigma^n \mid g(x) = 1\}$ that we denote by L_g.

The definitions of complexity classes we consider like P, NP, AM, E, EXP etc. can be found in standard books [BDG95, BDG90, Pap94]. A set $A \subseteq \{0\}^*$ is called *tally* ($A \in$ Tally for short). By log we denote the function $\log x = \max\{1, \lceil \log_2 x \rceil\}$ and $\langle \cdot, \cdot \rangle$

denotes a standard pairing function. For a string $x \in \Sigma^*$, $num(x)$ denotes the natural number whose binary representation is given by $1x$,

For a class C of sets and a class F of functions from 1^* to Σ^*, let C/F [KL80] be the class of sets A such that there is a set $B \in$ C and a function $h \in$ F such that for all $x \in \Sigma^*$,

$$x \in A \Leftrightarrow \langle x, h(1^{|x|})\rangle \in B.$$

The function h is called an *advice function* for A.

The BP-operator [Sch89] assigns to each complexity class C a randomized version BP$\cdot$C as follows. A set L belongs to BP $\cdot$ C if there exist a polynomial p and a set $D \in$ C such that for all x, $|x| = n$

$$\begin{aligned} x \in L &\Rightarrow Prob_{r \in_R \{0,1\}^{p(n)}}[\langle x, r\rangle \in D] \geq 2/3, \\ x \notin L &\Rightarrow Prob_{r \in_R \{0,1\}^{p(n)}}[\langle x, r\rangle \in D] \leq 1/3. \end{aligned}$$

Here, the subscript $r \in_R \{0,1\}^{p(n)}$ means that the probability is taken by choosing r uniformly at random from $\{0,1\}^{p(n)}$.

We recall the definition of oracle circuits first introduced by Wilson in [Wil85]. The definition below is essentially from Lutz and Schmidt [LS93]. An *oracle circuit* is a directed acyclic graph $\gamma = (V, E)$, with vertex set V consisting of inputs, standard gates (that compute AND, OR, and NOT), a special output gate, and oracle gates. The inputs have indegree 0. The AND and OR gates have indegree 2, and NOT gates have indegree 1. An oracle gate can have any positive integer k as its indegree. The function computed at an oracle gate depends upon the oracle being considered. Thus, if A is the oracle, a k-input oracle gate computes 1 iff its input string is in $A \cap \{0,1\}^k$. The edges denote wires connecting an input/gate to another gate. Thus, an n-input oracle circuit with oracle A computes an n-ary boolean function in the usual manner.

Let $\gamma = (V, E)$ be an n-input oracle circuit with $V = I \cup G_s \cup G_o$, where I is the set of inputs, G_s is the set of standard gates, and G_o is the set of oracle gates. Following Lutz and Schmidt [LS93] we define the size of γ to be $\text{size}(\gamma) = 2|G_s| + \sum_{g \in G_o} k_g$, where k_g is the indegree of the oracle gate g. This differs by a constant factor from the original definition of size [Wil85] which is $\|E\|$: It can be easily seen that $\|E\| \leq \text{size}(\gamma) \leq 2\|E\|$.

A *nondeterministic circuit* c has two kinds of input gates: in addition to the actual inputs $x_1, \ldots, x_n$, c has a series of distinguished *guess inputs* $y_1, \ldots, y_m$. The value computed by c on input $x \in \Sigma^n$ is 1 if there exists a $y \in \Sigma^m$ such that $c(xy) = 1$, and 0 otherwise [SV85]. Nondeterministic oracle circuits and their size are defined exactly as for deterministic oracle circuits.

We next define boolean functions that are hard-to-approximate and related notions. For a real number s and an oracle set $A \subseteq \Sigma^*$, $\mathcal{CIR}^A(n, s)$ ($\mathcal{NCIR}^A(n, s)$) denotes the class of boolean functions $f : \{0,1\}^n \to \{0,1\}$ that can be computed by some (nondeterministic) oracle circuit c of size at most s having access to A. Furthermore, for a real valued function $s : \mathcal{N} \to \mathcal{R}$ let $\mathcal{CIR}^A(s) = \bigcup_{n\geq 0} \mathcal{CIR}^A(n, s(n))$ and $\mathcal{NCIR}^A(s) = \bigcup_{n \geq 0} \mathcal{NCIR}^A(n, s(n))$. In case $A = \emptyset$ we always omit the superscript $\emptyset$.

Definition 1 *(cf.* [Yao82, NW94]*) Let $\mathcal{C}$ be a set of boolean functions and let $r : \mathcal{N} \to \mathcal{R}$ be a real valued function.*

1. *A boolean function $f : \{0,1\}^n \to \{0,1\}$ is said to be* s-hard for $\mathcal{C}$ *if for all n-ary boolean functions h in $\mathcal{C}$,*

$$\frac{1}{2} - \frac{1}{s} < \frac{\|\{x \in \{0,1\}^n \mid f(x) = h(x)\}\|}{2^n} < \frac{1}{2} + \frac{1}{s}.$$

2. *A set $L \subseteq \Sigma^*$ is said to be* r-hard for $\mathcal{C}$ *if for all but finitely many n, the n-ary boolean function $L^{=n}$ is $r(n)$-hard for $\mathcal{C}$.*

3. *A language class* D *is called* r-hard for $\mathcal{C}$ *if some language $L \in$ D is r-hard for $\mathcal{C}$.*

4. *A boolean function f (a language L, or a language class* D*) is called* $\mathcal{CIR}^A(r)$-hard *if f (resp. L,* D*) is r-hard for $\mathcal{CIR}^A(r)$. The notion of* $\mathcal{NCIR}^A(r)$-hardness *is defined in the same way.*

The already discussed result of Nisan and Wigderson can be stated in relativized form as follows.

Theorem 2 [NW94] *For all $\alpha > 0$ and all oracles A and B, if E^A is $\mathcal{CIR}^B(2^{\alpha n})$-hard, then $\mathrm{BP} \cdot \mathrm{P}^B \subseteq \mathrm{P}^B/\mathrm{FP}^A$.*

The concept of resource-bounded measure was introduced in [Lut92]. We briefly recall some basic definitions from [Lut92, Lut97] leading to the definition of a language class having p-measure 0. Intuitively, if a class C of languages has p-measure 0, then $\mathrm{C} \cap \mathrm{E}$ forms a negligible small subclass of the complexity class E (where $\mathrm{E} = \bigcup_{c>0} \mathrm{DTIME}(2^{cn})$; see [Lut92, Lut97] for more motivation).

Definition 3 [Lut92, Lut97]

1. *A function $d : \Sigma^* \to \mathcal{R}^+$ is called a* supermartingale *if for all $w \in \Sigma^*$,*

$$d(w) \geq (d(w0) + d(w1))/2.$$

2. *The* success set *of a supermartingale d is defined as*

$$\mathrm{S}^\infty[d] = \{A \mid \limsup_{l \to \infty} d(A(s_1) \cdots A(s_l)) = \infty\}$$

where $s_1 = \lambda, s_2 = 0, s_3 = 1, s_4 = 00, s_5 = 01, \ldots$ is the standard enumeration of Σ^* in lexicographic order. The unitary success set *of d is*

$$\mathrm{S}^1[d] = \bigcup_{d(w) \geq 1} \mathrm{C}_w$$

where, for each $w \in \Sigma^*$, C_w is the class of languages A such that $A(s_1) \ldots A(s_{|w|}) = w$.

3. *A function $d : \mathcal{N}^i \times \Sigma^* \to \mathcal{R}$ is said to be* p-computable *if there is a function $f : \mathcal{N}^{i+1} \times \Sigma^* \to \mathcal{R}$ such that $f(r, k_1, \cdots, k_i, w)$ is computable in time $(r + k_1 + \cdots + k_i + |w|)^{O(1)}$ and $|f(r, k_1, \cdots, k_i, w) - d(k_1, \cdots, k_i, w)| \leq 2^{-r}$.*

4. *A class* X *of languages* has p-measure 0 *(in symbols, $\mu_{\mathrm{p}}(\mathrm{X}) = 0$) if there is a* p-*computable supermartingale d such that $\mathrm{X} \subseteq \mathrm{S}^\infty[d]$.*

In the context of resource-bounded measure, it is interesting to ask for the measure of the class of all sets A for which E^A is not $\mathcal{CIR}^A(2^{\alpha n})$-hard. Building on initial results in [Lut93] it is shown in [AS94] that this class has p-measure 0.

Lemma 4 [AS94] *For all $0 < \alpha < 1/3$, $\mu_{\mathrm{p}}\{A \mid \mathrm{E}^A$ is not $\mathcal{CIR}^A(2^{\alpha n})$-hard$\} = 0$.*

Lutz strengthened this to the following result that is more useful for some applications.

Lemma 5 [Lut97] *For all $0 < \alpha < 1/3$ and all oracles $B \in \mathrm{E}$,*

$$\mu_{\mathrm{p}}\{A \mid \mathrm{E}^A \textit{ is not } \mathcal{CIR}^{A \oplus B}(2^{\alpha n})\textit{-hard}\} = 0.$$

As a consequence of the above lemma, Lutz derives the following theorem.

Theorem 6 [Lut97] *For $k \geq 2$, if $\mu_{\mathrm{p}}(\Delta_k^{\mathrm{P}}) \neq 0$ then $\mathrm{BP} \cdot \Delta_k^{\mathrm{P}} \subseteq \Delta_k^{\mathrm{P}}$.*

It is not hard to see that Theorem 6 can be extended to any complexity class $\mathrm{C} \subseteq \mathrm{EXP} = \bigcup_{c>0} \mathrm{DTIME}(2^{n^c})$ that is closed under join and polynomial-time Turing reducibility (see also Corollary 24). For example, if $\oplus\mathrm{P}$ does not have p-measure 0, then $\mathrm{BP}\cdot\oplus\mathrm{P} \subseteq \oplus\mathrm{P}$, implying [Tod91] that the polynomial hierarchy is contained in $\oplus\mathrm{P}$. In Sections 4 and 5 we address the question whether $\mathrm{BP} \cdot \Sigma_k^{\mathrm{P}} = \Sigma_k^{\mathrm{P}}$ (or $\mathrm{BP} \cdot \Theta_k^{\mathrm{P}} = \Theta_k^{\mathrm{P}}$) can also be derived from $\mu_{\mathrm{p}}(\Delta_k^{\mathrm{P}}) \neq 0$, and whether stronger consequences can be derived from $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$ and $\mu_{\mathrm{p}}(\mathrm{NP} \cap \mathrm{coNP}) \neq 0$.

3 Derandomizing AM in Relativized Worlds

In this section we show that the Nisan-Wigderson generator can also be used to derandomize the Arthur-Merlin class $\mathrm{AM} = \mathrm{BP} \cdot \mathrm{NP}$ [Bab85]. We start by recalling some notation from [NW94].

Let n, l, m, k be positive integers. A collection $\mathcal{D} = (D_1, \ldots, D_n)$ of sets $D_i \subseteq \{1, \ldots, l\}$ is called a (n, l, m, k)-*design* if

- for all $i = 1, \ldots, n$, $\|D_i\| = m$, and
- for all $i \neq j$, $\|D_i \cap D_j\| \leq k$.

Using $\mathcal{D}$ we get from a set C a sequence of boolean functions $g^C_{D_i} : \{0,1\}^l \to \{0,1\}$, $i = 1, \ldots, n$, defined as

$$g^C_{D_i}(s_1, \ldots, s_l) \quad = \quad C^{=m}(s_{i_1}, \ldots, s_{i_m}) \text{ where } D_i = \{i_1, \ldots, i_m\}.$$

By concatenating the values of these functions we get a function $g^C_{\mathcal{D}} : \{0,1\}^l \to \{0,1\}^n$ where $g^C_{\mathcal{D}}(s) = g^C_{D_1}(s) \ldots g^C_{D_n}(s)$.

A *pseudorandom generator* is a sequence of functions $g_n : \{0,1\}^{l(n)} \to \{0,1\}^n$, $n \geq 1$, mapping seeds of length $l(n) < n$ to pseudorandom strings of length n. Next we define what it means that a pseudorandom generator is secure against a class of boolean functions.

Definition 7 *Let $\mathcal{C}$ be a set of boolean functions.*

1. *A function $g : \{0,1\}^l \to \{0,1\}^n$, where $l < n$, is said to be $\mathcal{C}$-*secure*, if for all n-ary boolean functions f in $\mathcal{C}$,*

$$\left| Prob_{y \in_R \{0,1\}^n}[f(y) = 1] - Prob_{s \in_R \{0,1\}^l}[f(g(s)) = 1] \right| \leq 1/n.$$

2. *A pseudorandom generator $g_n : \{0,1\}^{l(n)} \to \{0,1\}^n$, $n \geq 1$, is said to be $\mathcal{C}$-*secure*, if for almost all n, g_n is $\mathcal{C}$-secure.*

As shown by Nisan and Wigderson [NW94, Lemma 2.4], the output of $g^C_{\mathcal{D}}$ looks random to any small deterministic circuit, provided that C is hard to approximate by deterministic circuits of a certain size (in other words, the hardness of C implies that the pseudorandom generator $g^C_{\mathcal{D}}$ is secure against small deterministic circuits). The following lemma shows that $g^C_{\mathcal{D}}$ is also secure against small nondeterministic circuits provided C is hard to approximate by nondeterministic circuits of a certain size. As pointed out in [Rud97], this appears somewhat counter-intuitive since a nondeterministic circuit c might guess the seed given to the pseudorandom generator $g^C_{\mathcal{D}}$ and then verify that the guess is correct. But note that in our case, this strategy is ruled out by the size restriction on c which prevents c from simulating $g^C_{\mathcal{D}}$.

Lemma 8 *Let $\mathcal{D}$ be a (n, l, m, k)-*design *and let C be a set such that the boolean function $C^{=m}$ is n^2-hard for $\mathcal{NCIR}^B(m, n^2 + n2^k)$. Then the function $g^C_{\mathcal{D}} : \{0,1\}^l \to \{0,1\}^n$ is $\mathcal{NCIR}^B(n^2)$-secure.*

Proof. Let $\mathcal{D} = (D_1, \ldots, D_n)$ be a (n, l, m, k)-*design*. The proof is along similar lines as that of [NW94, Lemma 2.4]. We show that if there is a nondeterministic oracle circuit c of size at most n^2 such that

$$\left| Prob_{y \in_R \{0,1\}^n}[c^B(y) = 1] - Prob_{s \in_R \{0,1\}^l}[c^B(g^C_{\mathcal{D}}(s)) = 1] \right| > 1/n,$$

then $C^{=m}$ is not n^2-hard for $\mathcal{NCIR}^B(m, n^2 + n2^k)$. Let $S_1, \ldots, S_l$ and $Z_1, \ldots, Z_n$ be independently and uniformly distributed random variables over $\{0,1\}$ and let $S = (S_1, \ldots, S_l)$.

Then we can restate the inequality above as follows (recall that $g^C_{D_i}(s)$ is the ith bit of $g^C_{\mathcal{D}}(s)$):

$$\Big|Prob[c^B(Z_1,\ldots,Z_n)=1]-Prob[c^B(g^C_{D_1}(S),\ldots,g^C_{D_n}(S))=1]\Big|>1/n.$$

Now consider the random variables

$$X_i=c^B(g^C_{D_1}(S),\ldots,g^C_{D_{i-1}}(S),Z_i,\ldots,Z_n),\ i=1,\ldots,n+1.$$

Since $X_1=c^B(Z_1,\ldots,Z_n)$ and since $X_{n+1}=c^B(g^C_{D_1}(S),\ldots,g^C_{D_n}(S))$, we can fix an index $j\in\{1,\ldots,n\}$ such that

$$\Big|Prob[X_j=1]-Prob[X_{j+1}=1]\Big|>1/n^2. \tag{1}$$

Consider the boolean function $h:\{0,1\}^l\times\{0,1\}^{n-j+1}\to\{0,1\}$ defined as

$$h(s,z_j,\ldots,z_n) \;=\; \begin{cases} z_j, & \text{if } c^B(g^C_{D_1}(s),\ldots,g^C_{D_{j-1}}(s),z_j,\ldots,z_n)=0,\\ 1-z_j, & \text{otherwise.}\end{cases}$$

Since

$$\begin{aligned}
&Prob[h(S,Z_j,\ldots,Z_n)=g^C_{D_j}(S)]-1/2\\
&= Prob[X_j=0\wedge Z_j=g^C_{D_j}(S)]+Prob[X_j=1\wedge Z_j\neq g^C_{D_j}(S)]-1/2\\
&= Prob[Z_j=g^C_{D_j}(S)]+Prob[X_j=1]-2\cdot Prob[X_j=1\wedge Z_j=g^C_{D_j}(S)]-1/2\\
&= Prob[X_j=1]-2\cdot Prob[X_{j+1}=1\wedge Z_j=g^C_{D_j}(S)]\\
&= Prob[X_j=1]-Prob[X_{j+1}=1]
\end{aligned}$$

it follows that (1) is equivalent to

$$\Big|Prob[h(S,Z_j,\ldots,Z_n)=g^C_{D_j}(S)]-1/2\Big|>1/n^2. \tag{2}$$

Since $g^C_{D_j}(s_1,\ldots,s_l)$ only depends on the bits s_i with $i\in D_j$, we can apply an averaging argument to find fixed bits $\hat{s}_i$, $i\notin D_j$ and fixed bits $\hat{z}_j,\ldots,\hat{z}_n$ such that (2) still holds under the condition that $S_i=\hat{s}_i$ for all $i\notin D_j$ and $Z_i=\hat{z}_i$ for all $i=j,\ldots,n$. Since $g^C_{D_j}(s_1,\ldots,s_l)=C^{=m}(s_1,\ldots,s_m)$ (for notational convenience we assume w.l.o.g. that $D_j=\{1,\ldots,m\}$) we thus get

$$\Big|Prob[h(S_1,\ldots,S_m,\hat{s}_{m+1},\ldots,\hat{s}_l,\hat{z}_j,\ldots,\hat{z}_n)=C^{=m}(S_1,\ldots,S_m)]-1/2\Big|>1/n^2.$$

Now consider the nondeterministic oracle circuit c' that on input $s_1,\ldots,s_m$ first evaluates the functions $g^C_{D_1},g^C_{D_2},\ldots,g^C_{D_{j-1}}$ on $(s_1,\ldots,s_m,\hat{s}_{m+1},\ldots,\hat{s}_l)$, and then simulates the oracle circuit c^B to compute

$$c^B(g^C_{D_1}(s_1,\ldots,s_m,\hat{s}_{m+1},\ldots,\hat{s}_l),\ldots,g^C_{D_{j-1}}(s_1,\ldots,s_m,\hat{s}_{m+1},\ldots,\hat{s}_l),\hat{z}_j,\ldots,\hat{z}_n).$$

Then, depending on whether $\hat{z}_j = 0$ or $\hat{z}_j = 1$, c'^B either computes the boolean function that maps $(s_1, \ldots, s_m)$ to $h(s_1, \ldots, s_m, \hat{s}_{m+1}, \ldots, \hat{s}_l, \hat{z}_j, \ldots, \hat{z}_n)$ or it computes the negation of this function and hence it follows that

$$\left|Prob[c'^B(S_1, \ldots, S_m) = C^{=m}(S_1, \ldots, S_m)] - 1/2\right| > 1/n^2.$$

Since each of $g^C_{D_1}(s_1, \ldots, s_m, \hat{s}_{m+1}, \ldots, \hat{s}_l), \ldots, g^C_{D_{j-1}}(s_1, \ldots, s_m, \hat{s}_{m+1}, \ldots, \hat{s}_l)$ depends on at most k input bits, these values can be computed by a deterministic subcircuit of size at most 2^k (namely, the brute-force circuit that evaluates that particular k-ary boolean function). This means that the size of c' is at most $n^2 + n2^k$, implying that $C^{=m}$ is not n^2-hard for $\mathcal{NCIR}^B(m, n^2 + n2^k)$. ■

For our extension of Theorem 2 we also need the following lemma.

Lemma 9 [NW94] *Let c be a positive integer. Then there is a polynomial-time algorithm that on input 0^n outputs a $(n, l(n), m(n), k(n))$-design $\mathcal{D}_n$, where $l(n) = 2c^2 \log n$, $m(n) = c \log n$, and $k(n) = \log n$.*

By combining Lemma 9 with Lemma 8 we easily get the following theorem.

Theorem 10 *Let $\alpha > 0$. If C is $\mathcal{NCIR}^B(2^{\alpha n})$-hard, then there is an $\mathcal{NCIR}^B(n^2)$-secure pseudorandom generator $g_n : \{0,1\}^{l(n)} \to \{0,1\}^n$, $n \geq 1$, such that $l(n) = O(\log n)$ and the set $\{\langle 0^n, 0^j, s\rangle \mid s \in \{0,1\}^{l(n)}$ and the j-th bit of $g_n(s)$ is $1\}$ polynomial-time many-one reduces to the tally set $\{0^{num(x)} \mid x \in C\}$.*

Proof. Let $\alpha > 0$ and let C be an $\mathcal{NCIR}^B(2^{\alpha n})$-hard language. Then for almost all n, the boolean function $C^{=n}$ is $\mathcal{NCIR}^B(n, 2^{\alpha n})$-hard. Thus, letting $c = \lceil 3/\alpha \rceil$ and $m(n) = c \log n$, it follows that for almost all n, $C^{=m(n)}$ is n^3-hard for $\mathcal{NCIR}^B(m(n), n^3)$. Now let $l(n) = 2c^2 \log n$ and $k(n) = \log n$. Then we can apply Lemma 8 and Lemma 9 to get on input 0^n a $(n, l(n), m(n), k(n))$-design $\mathcal{D}_n$ with the property that for almost all n the function $g_n = g^C_{\mathcal{D}_n} : \{0,1\}^{l(n)} \to \{0,1\}^n$ is $\mathcal{NCIR}^B(n^2)$-secure.

Furthermore, consider the function f defined as

$$f(0^n, 0^j, s) = 0^{num(s_{j_1} \cdots s_{j_m})},$$

where $j_1, \ldots, j_m$ are the indices in the j-th set D_j of the design $\mathcal{D}_n$. It is easy to see that the set $\{\langle 0^n, 0^j, s\rangle \mid s \in \{0,1\}^{l(n)}$ and the j-th bit of $g_n(s)$ is $1\}$ many-one reduces via f to the set $\{0^{num(x)} \mid x \in C\}$. Since $\mathcal{D}_n$ is computable in polynomial time in n, f is also computable in polynomial time. ■

In the next theorem we use the Nisan-Wigderson generator to derandomize the class $\mathrm{BP} \cdot \mathrm{NP}^B$.

Theorem 11 *Let A and B be oracles and let $\alpha > 0$. If E^A is $\mathcal{NCIR}^B(2^{\alpha n})$-hard, then $\mathrm{BP} \cdot \mathrm{NP}^B \subseteq \mathrm{NP}^B/\mathrm{FP}^A$. In particular, if E^B is $\mathcal{NCIR}^B(2^{\alpha n})$-hard, then $\mathrm{BP} \cdot \mathrm{NP}^B = \mathrm{NP}^B$.*

Proof. Let $L \in \mathrm{BP} \cdot \mathrm{NP}^B$. Then there exist a polynomial p and a set $D \in \mathrm{NP}^B$ such that for all x, $|x| = n$

$$\begin{aligned} x \in L &\Rightarrow Prob_{r \in_R \{0,1\}^{p(n)}}[\langle x, r\rangle \in D] \geq 2/3, \\ x \notin L &\Rightarrow Prob_{r \in_R \{0,1\}^{p(n)}}[\langle x, r\rangle \in D] \leq 1/3. \end{aligned}$$

For a fixed input x, the decision procedure for D on input x, r can be simulated by some nondeterministic oracle circuit c_x with input r, implying that

$$\begin{aligned} x \in L &\Rightarrow Prob_{r \in_R \{0,1\}^{p(n)}}[c_x^B(r) = 1] \geq 2/3, \\ x \notin L &\Rightarrow Prob_{r \in_R \{0,1\}^{p(n)}}[c_x^B(r) = 1] \leq 1/3 \end{aligned}$$

where w.l.o.g. we can assume that the size of c_x is bounded by $p^2(|x|)$.

Let $C \in \mathrm{E}^A$ be an $\mathcal{NCIR}^B(2^{\alpha n})$-hard language. By Theorem 10 there is an $\mathcal{NCIR}^B(n^2)$-secure pseudorandom generator $g_n : \{0,1\}^{l(n)} \to \{0,1\}^n$, $n \geq 1$, such that $l(n) = O(\log n)$ and the set $\{\langle 0^n, 0^j, s\rangle \mid s \in \{0,1\}^{l(n)}$ and the j-th bit of $g_n(s)$ is $1\}$ polynomial-time many-one reduces to the tally set $T = \{0^{num(x)} \mid x \in C\}$. Notice that since $C \in \mathrm{E}^A$, T belongs to P^A. Thus, since $l(p(n)) = O(\log n)$, it is possible to compute the advice function $h(1^n) = g_{p(n)}(0^{l(p(n))}) \cdots g_{p(n)}(1^{l(p(n))})$ in FP^A. Hence, the following procedure witnesses $B \in \mathrm{NP}^B/\mathrm{FP}^A$:

> **input** x, $|x| = n$, and a sequence $h(1^n) = r_1 \ldots r_{2^{l(p(n))}}$ of strings of length $p(n)$;
> **if** the number of r_i for which $c_x^B(r_i) = 1$ is at least $2^{l(p(n))-1}$ **then**
> **accept else reject**

■

4 Derandomizing BP$\cdot\Sigma_k^{\mathrm{P}}$ if $\Sigma_k^{\mathrm{P}} \cap \Pi_k^{\mathrm{P}}$ is Not Small

In this section we apply the relativized derandomization of the previous section to extend Lutz's Theorem 6 to the Σ_k^{P} levels of the polynomial hierarchy. A crucial result used in the proof of Lutz's Lemma 5 is the fact that there are many n-ary boolean functions that are $\mathcal{CIR}(2^{\alpha n})$-hard (see Lemma 12 stated below). In Lemma 14 we establish the same bound for the nondeterministic case.

Lemma 12 [Lut93] *For each α such that $0 < \alpha < 1/3$, there is a constant n_0 such that for all $n \geq n_0$ and all oracles A, the number of boolean functions $f : \{0,1\}^n \to \{0,1\}$ that are not $\mathcal{CIR}^A(2^{\alpha n})$-hard is at most $2^{2^n} \cdot e^{-2^{n/4}}$.*

We recall another useful bound derived in [LS93].

Lemma 13 [LS93] *For $n \leq q$, $\|\mathcal{CIR}^A(n,q)\| \leq 2685(4eq)^q$.*

Lemma 14 *For each α such that $0 < \alpha < 1/3$, there is a constant n_0 such that for all $n \geq n_0$ and all oracles A, the number of n-ary boolean functions that are not $\mathcal{NCIR}^A(2^{\alpha n})$-hard is at most $2^{2^n} \cdot e^{-2^{n/4}}$.*

Proof. The proof follows an essentially similar counting argument as in the deterministic case (see [Lut93]). In the sequel, let $q = 2^{\alpha n}$ and let $\mathcal{NCIR}_j^A(n,q)$ denote the class of n-ary boolean functions computed by nondeterministic oracle circuits of size q with exactly j guess inputs, having access to oracle A. Notice that $\mathcal{NCIR}^A(n,q) = \bigcup_{j=0}^{q-n} \mathcal{NCIR}_j^A(n,q)$, implying that $\|\mathcal{NCIR}^A(n,q)\| \leq \sum_{j=0}^{q-n} \|\mathcal{NCIR}_j^A(n,q)\|$. By Lemma 13 we have

$$\|\mathcal{CIR}^A(n,q)\| \leq a(4eq)^q$$

where $a = 2685$. Since each function in $\mathcal{NCIR}_j^A(n,q)$ is uniquely determined by an $n+j$-ary boolean function in $\mathcal{CIR}^A(n+j,q)$, it follows that

$$\|\mathcal{NCIR}^A(n,q)\| \leq \sum_{j=0}^{q-n} a(4eq)^q \leq aq(4eq)^q.$$

We now place a bound on the number of n-ary boolean functions that are not $\mathcal{NCIR}^A(q)$-hard. Let

$$\mathrm{DELTA}(n,q) = \{D \subseteq \Sigma^n \mid \|D\| \leq (1/2 - 1/q)2^n\} \cup \{D \subseteq \Sigma^n \mid \|D\| \geq (1/2 + 1/q)2^n\}.$$

Applying standard Chernoff bounds, as shown in [Lut93], it can be seen that for a small constant $c > 0$, $\|\mathrm{DELTA}(n,q)\| \leq 2^{2^n} 2^{-c2^{(1-2\alpha)n}}$. Now, from the notion of $\mathcal{NCIR}^A(q)$-hard functions (Definition 1) it easily follows that there are at most

$$\|\mathcal{NCIR}^A(n,q)\| \cdot \|\mathrm{DELTA}(n,q)\| \leq q(q+1)(144eq)^q \cdot 2^{2^n} 2^{-c2^{(1-2\alpha)n}}$$

distinct n-ary boolean functions that are not $\mathcal{NCIR}^A(q)$-hard. Hence, using the fact that $0 < \alpha < 1/3$ we can easily find a constant n_0 such that for $n \geq n_0$ the above number is bounded above by $2^{2^n} e^{-2^{n/4}}$ as required. ■

We further need the important Borel-Cantelli-Lutz Lemma [Lut92]. A series $\sum_{k=0}^{\infty} a_k$ of nonnegative reals is said to be p-*convergent* if there is a polynomial q such that for all $r \in \mathcal{N}$, $\sum_{k=q(r)}^{\infty} a_k \leq 2^{-r}$.

Theorem 15 [Lut92] *Assume that $d : \mathcal{N} \times \Sigma^* \to \mathcal{R}^+$ is a function with the following properties:*

1. *d is* p-*computable.*
2. *For each $k \in \mathcal{N}$, the function d_k, defined by $d_k(w) = d(k,w)$ is a supermartingale.*
3. *The series $\sum_{k=0}^{\infty} d_k(\lambda)$ is* p-*convergent.*

Then $\mu_{\rm p}(\bigcap_{j=0}^{\infty}\bigcup_{k=j}^{\infty} {\rm S}^1[d_k]) = 0$.

Now we are ready to extend Lutz's Lemma 5 to the case of nondeterministic circuits.

Theorem 16 *For all* $0 < \alpha < 1/3$ *and all oracles* $B \in {\rm E}$,

$$\mu_{\rm p}\{A \mid {\rm E}^A \textit{ is not } \mathcal{NCIR}^{A\oplus B}(2^{\alpha n})\textit{-hard}\} = 0.$$

Proof. Let $0 < \alpha < 1/3$ and $B \in {\rm E}$. For each language A define the test language[1]

$$C(A) = \{x \mid 0^{num(x)} \in A\}$$

and consider the language class ${\rm X} = \{A \mid C(A) \text{ is not } \mathcal{NCIR}^{A\oplus B}(2^{\alpha n})\text{-hard}\}$. Notice that since $C(A) \in {\rm E}^A$, the theorem follows from the following claim.

Claim. $\mu_{\rm p}({\rm X}) = 0$.

Proof of Claim. The proof follows the same lines as in [Lut97, Theorem 3.2] except for minor changes to take care of the fact that we are dealing with nondeterministic circuits. For each $k > 0$, let

$${\rm X}_k = \begin{cases} \{A \mid C(A)^{=n} \text{ is not } \mathcal{NCIR}^{A\oplus B}(2^{\alpha n})\text{-hard}\}, & \text{if } k = 2^n \text{ for some } n,\\ \emptyset, & \text{otherwise.}\end{cases}$$

It follows immediately that

$${\rm X} = \bigcap_{j\geq 0}\bigcup_{k\geq j} {\rm X}_k.$$

We will show that $\mu_{\rm p}({\rm X}) = 0$ by applying the Borel-Cantelli-Lutz Lemma (Theorem 15). Let n_0 be the constant provided by Lemma 14 and let $k_0 = 2^{n_0}$. In order to apply Theorem 15 we define $d : \mathcal{N} \times \Sigma^* \to \mathcal{R}^+$ as follows (exactly as in [Lut97]):

1. If $k < k_0$ or k is not a power of 2, then $d_k(w) = 0$.
2. If $k = 2^n \geq k_0$ and $|w| < 2^{k+1}$, then $d_k(w) = e^{-k^{1/4}}$.
3. If $k = 2^n \geq k_0$ and $|w| \geq 2^{k+1}$, then

$$d_k(w) = \sum_{\substack{g\in\mathcal{NCIR}^{L_w\oplus B}(n,2^{\alpha n}),\\ D\in{\rm DELTA}(n,2^{\alpha n})}} Prob[L_g = C(A)^{=n}\triangle D \mid A \in {\rm C}_w]$$

where $d_k(w) = d(k, w)$ and the conditional probabilities are taken by deciding the membership of each string $x \in \Sigma^*$ to the random language A by an independent toss of a fair coin.

Now, the following three properties of d can be proved along similar lines as in [Lut97]:

[1] A similar test language has been used in [AS94] and later in [Lut97].

1. d is p-computable.
2. For each $k > 0$, d_k is a supermartingale with $d_k(\lambda) \leq e^{-k^{1/4}}$.
3. For all $k \geq k_0$, $\mathrm{X}_k \subseteq \mathrm{S}^1[d_k]$.
4. $\mathrm{X} \subseteq \bigcup_{j\geq 0} \bigcap_{k\geq j} \mathrm{S}^1[d_k]$.

The only point where a different argument is required is in showing that d is p-computable because the circuits used to define $d_k(w)$ are nondeterministic. Nevertheless, notice that the only nontrivial case to be handled in the definition of d_k is when $k = 2^n \geq k_0$ and $|w| \geq 2^{k+1}$. In this case, the size of the considered nondeterministic oracle circuits is bounded by $2^{\alpha n} \leq k$. Therefore, in time polynomial in $2^k < |w|$ it is possible to evaluate these circuits by exhaustive search. ∎

It is now easy to derandomize $\mathrm{BP}\cdot\Sigma_k^{\mathrm{P}}$ under the assumption that $\Sigma_k^{\mathrm{P}} \cap \Pi_k^{\mathrm{P}}$ has non-zero p-measure.

Corollary 17 *For all $k \geq 1$, if $\mu_{\mathrm{p}}(\Sigma_k^{\mathrm{P}} \cap \Pi_k^{\mathrm{P}}) \neq 0$, then* $\mathrm{BP}\cdot\Sigma_k^{\mathrm{P}} = \Sigma_k^{\mathrm{P}}$.

Proof. Assume the hypothesis and let B be a fixed $\Sigma_{k-1}^{\mathrm{P}}$-complete set. We know from Theorem 16 that for $\alpha = 1/4$,

$$\mu_{\mathrm{p}}\{A \mid \mathrm{E}^A \text{ is not } \mathcal{NCIR}^{A\oplus B}(2^{\alpha n})\text{-hard}\} = 0.$$

On the other hand, $\mu_{\mathrm{p}}(\Sigma_k^{\mathrm{P}} \cap \Pi_k^{\mathrm{P}}) \neq 0$. Hence, there is a set $A \in \Sigma_k^{\mathrm{P}} \cap \Pi_k^{\mathrm{P}}$ such that E^A (and thus also $\mathrm{E}^{A\oplus B}$) is $\mathcal{NCIR}^{A\oplus B}(2^{\alpha n})$-hard. Applying Theorem 11 we get

$$\mathrm{BP}\cdot\Sigma_k^{\mathrm{P}} = \mathrm{BP}\cdot\mathrm{NP}^{A\oplus B} = \mathrm{NP}^{A\oplus B} = \Sigma_k^{\mathrm{P}},$$

which completes the proof. ∎

Furthermore, we obtain the following interesting consequence.

Corollary 18 If $\mu_{\mathrm{p}}(\Sigma_k^{\mathrm{P}}) \neq 0$, then $\mathrm{BP}\cdot\Sigma_k^{\mathrm{P}} \subseteq \Theta_{k+1}^{\mathrm{P}} \cap \Sigma_k^{\mathrm{P}}/\log$.

Proof. Let B be a fixed $\Sigma_{k-1}^{\mathrm{P}}$-complete set. If $\mu_{\mathrm{p}}(\Sigma_k^{\mathrm{P}}) \neq 0$, then it follows from Theorem 16 that there is a set $A \in \Sigma_k^{\mathrm{P}}$ such that E^A is $\mathcal{NCIR}^{A\oplus B}(2^{\alpha n})$-hard (and thus also $\mathcal{NCIR}^{B}(2^{\alpha n})$-hard). Actually, from the proof of Theorem 16 we know something stronger. Namely, we know that the test language

$$C(A) = \{x \mid 0^{num(x)} \in A\}$$

is $\mathcal{NCIR}^{B}(2^{\alpha n})$-hard. Hence, we can assume that A is a tally set in Σ_k^{P} and by Theorem 11 it follows that

$$\mathrm{BP}\cdot\Sigma_k^{\mathrm{P}} = \mathrm{BP}\cdot\mathrm{NP}^B \subseteq \mathrm{NP}^B/\mathrm{FP}^A \subseteq \Sigma_k^{\mathrm{P}}/\mathrm{FP}^{\Sigma_k^{\mathrm{P}}\cap\mathrm{Tally}} \subseteq \Theta_{k+1}^{\mathrm{P}} \cap \Sigma_k^{\mathrm{P}}/\log,$$

where the inclusion in $\Sigma_k^{\mathrm{P}}/\log$ follows by a census argument [Kad89] (see also [KT94]). ∎

Also, by combining Theorem 16 with Theorem 10 we easily get the following result.

Corollary 19 *Let* D *be a complexity class. Then* $\mu_{\mathrm{p}}(\mathrm{D}) \neq 0$ *implies that for every oracle* $B \in \mathrm{E}$ *there is a set* A *in* D *and an* $\mathcal{NCIR}^{A\oplus B}(n^2)$*-secure pseudorandom generator* $g_n : \{0,1\}^{l(n)} \to \{0,1\}^n$, $n \geq 1$, *such that* $l(n) = O(\log n)$ *and the set* $\{\langle 0^n, 0^j, s\rangle \mid s \in \{0,1\}^{l(n)}$ *and the* j*-th bit of* $g_n(s)$ *is* $1\}$ *polynomial-time many-one reduces to the tally set* $A \cap 0^*$.

Proof. By Theorem 16 the assumption $\mu_{\mathrm{p}}(\mathrm{D}) \neq 0$ implies that for every oracle $B \in \mathrm{E}$ there is a set A in D such that $C(A)$ is $\mathcal{NCIR}^{A\oplus B}(2^{n/4})$-hard. Thus, the corollary follows by Theorem 10. ∎

5 Derandomizing BP$\cdot\Theta_k^{\mathrm{P}}$ if Θ_k^{P} is Not Small

In [Lut97] it was an open question whether $\mathrm{BP}\cdot\Theta_2^{\mathrm{P}} = \Theta_2^{\mathrm{P}}$ can be proven as a consequence of $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$. We answer this question by deriving $\mathrm{BP}\cdot\Theta_2^{\mathrm{P}} = \Theta_2^{\mathrm{P}}$ from an assumption that is possibly weaker than $\mu_{\mathrm{p}}(\mathrm{NP}) \neq 0$.

For a complexity class $\mathrm{K} \in \{\mathrm{P}, \mathrm{FP}, \mathrm{BPP}, \mathrm{E}\}$ and oracle A, let $\mathrm{K}_{\|}^{A}$ denote the respective relativized class where only *parallel queries* to A are allowed.

A deterministic oracle circuit with *parallel queries* is a usual deterministic oracle circuit with the additional constraint that there is no *directed* path between any two oracle gates.

Definition 20 *Let* $A \subseteq \Sigma^*$ *be an oracle set. Let* $\mathcal{CIR}_{\|}^{A}(n,s)$ *denote the class of boolean functions* $f : \{0,1\}^n \to \{0,1\}$ *that can be computed by some oracle circuit* c *of size at most* s *that makes only* parallel queries *to oracle* A*. Furthermore, for a function* $s : \mathcal{N} \to \mathcal{N}^+$ *let* $\mathcal{CIR}_{\|}^{A}(s) = \bigcup_{n\geq 0} \mathcal{CIR}_{\|}^{A}(n, s(n))$.

It is not hard to verify that Nisan and Wigderson's result (Theorem 2) also holds in the parallel setting.

Theorem 21 *For all* $\alpha > 0$ *and all oracles* A *and* B*, if* $\mathrm{E}_{\|}^{A}$ *is* $\mathcal{CIR}_{\|}^{B}(2^{\alpha n})$*-hard, then* $\mathrm{BP}\cdot\mathrm{P}_{\|}^{B} \subseteq \mathrm{P}_{\|}^{B}/\mathrm{FP}_{\|}^{A}$.

Corollary 22 For all $k \geq 2$, if $\mu_{\mathrm{p}}(\Theta_k^{\mathrm{P}}) \neq 0$, then $\mathrm{BP}\cdot\Theta_k^{\mathrm{P}} = \Theta_k^{\mathrm{P}}$.

Proof. Assume the hypothesis and let B be a fixed $\Sigma_{k-1}^{\mathrm{P}}$-complete set. Observe that if $\mu_{\mathrm{p}}(\Theta_k^{\mathrm{P}}) \neq 0$, then it follows from the proof of Lemma 5 (as given in [Lut97]) that for $\alpha = 1/4$ there is a set $A \in \Theta_k^{\mathrm{P}}$ such that $C(A)$ is $\mathcal{CIR}^{A\oplus B}(2^{\alpha n})$-hard. Since $C(A) \in E_{\|}^{A} \subseteq E_{\|}^{A\oplus B}$ and since $\mathcal{CIR}_{\|}^{A\oplus B}(2^{\alpha n}) \subseteq \mathcal{CIR}^{A\oplus B}(2^{\alpha n})$, it follows that $E_{\|}^{A\oplus B}$ is $\mathcal{CIR}_{\|}^{A\oplus B}(2^{\alpha n})$-hard, implying that

$$\mathrm{BP}\cdot\Theta_k^{\mathrm{P}} = \mathrm{BP}\cdot\mathrm{P}_{\|}^{A\oplus B} = \mathrm{P}_{\|}^{A\oplus B} = \Theta_k^{\mathrm{P}},$$

where the second equality follows by Theorem 21. ∎

Corollary 22 has the following immediate lowness consequence.

Corollary 23 If $\mu_{\rm p}(\Theta_2^{\rm P}) \neq 0$ then AM$\cap$coAM (and hence the graph isomorphism problem) is low for $\Theta_2^{\rm P}$.

Corollary 22 can easily be extended to further complexity classes.

Corollary 24 For any complexity class C $\subseteq$ EXP closed under join and polynomial-time truth-table reducibility, $\mu_{\rm p}({\rm C}) \neq 0$ implies that BP $\cdot$ C $\subseteq$ C.

Proof. Assume the hypothesis and let L be a set in BP $\cdot$ C, witnessed by some set $B \in$ C. Since C is closed under many-one reducibility we can define a suitably padded version $\hat{B}$ of B in C$\cap$E such that L belongs to BP $\cdot \{\hat{B}\}$. Now, exactly as in the proof of Corollary 22 we can argue that there is a set $A \in$ C with the property that $E_{\|}^{A\oplus\hat{B}}$ is $\mathcal{CIR}_{\|}^{A\oplus\hat{B}}(2^{\alpha n})$-hard. Hence, by Theorem 21 it follows that

$$L \in {\rm BP} \cdot \{\hat{B}\} \subseteq {\rm BP} \cdot {\rm P}_{\|}^{A\oplus\hat{B}} = {\rm P}_{\|}^{A\oplus\hat{B}} \subseteq {\rm C}.$$

■

For example, using the fact that PP is closed under polynomial-time truth-table reducibility [FR96], it follows that if $\mu_{\rm p}({\rm PP}) \neq 0$, then BP $\cdot$PP = PP.

6 MA is Contained in ZPP$^{\rm NP}$

In this section we apply the Nisan-Wigderson generator to show that MA is contained in ZPP$^{\rm NP}$ and that MA$\cap$coMA is low for ZPP$^{\rm NP}$. This improves on a result of [ZF87] where a quantifier simulation technique is used to show that NP$^{\rm BPP}$ (a subclass of MA) is contained in ZPP$^{\rm NP}$. We notice that the result MA $\subseteq$ ZPP$^{\rm NP}$ has been shown independently using different techniques [GZ97].

The proof of the next theorem makes use of the fact that there are many n-ary boolean functions that are $\mathcal{CIR}(2^{\alpha n})$-hard (Lemma 12).

Theorem 25 MA *is contained in* ZPP$^{\rm NP}$*.*

Proof. Let L be a set in MA. Then there exist a polynomial p and a set $B \in$ P such that for all x, $|x| = n$,

$$\begin{aligned} x \in A &\Rightarrow \exists y, |y| = p(n) : Prob_{r\in_R\{0,1\}^{p(n)}}[\langle x, y, r\rangle \in B] \geq 2/3, \\ x \notin A &\Rightarrow \forall y, |y| = p(n) : Prob_{r\in_R\{0,1\}^{p(n)}}[\langle x, y, r\rangle \in B] \leq 1/3. \end{aligned}$$

For fixed strings x and y, the decision procedure for B on input x, y, r can be simulated by some circuit $c_{x,y}$ with inputs $r_1, \ldots, r_{p(n)}$, implying that

$$\begin{aligned} x \in A &\Rightarrow \exists y, |y| = p(n) : Prob_{r\in_R\{0,1\}^{p(n)}}[c_{x,y}(r) = 1] \geq 2/3, \\ x \notin A &\Rightarrow \forall y, |y| = p(n) : Prob_{r\in_R\{0,1\}^{p(n)}}[c_{x,y}(r) = 1] \leq 1/3 \end{aligned}$$

where w.l.o.g. we can assume that the size of $c_{x,y}$ is bounded by $p^2(|x|)$. It follows by the deterministic version of Lemma 8 that for any (p,l,m,k)-design $\mathcal{D}$ and any set C for which $C^{=m}$ is p^2-hard for $\mathcal{CIR}(m, p^2 + p2^k)$,

$$\left| Prob_{y \in_R \{0,1\}^p}[c(y) = 1] - Prob_{s \in_R \{0,1\}^l}[c(g_{\mathcal{D}}^C(s)) = 1] \right| \leq 1/p$$

holds for every p-input circuit c of size at most p^2.

Now let $m(n) = 12 \log p(n)$, $l(n) = 2 \cdot 12^2 \log p(n)$, and $k(n) = \log p(n)$. Then, by Lemma 12 we know that for all sufficiently large n, a randomly chosen set $C \subseteq \{0,1\}^{m(n)}$ has the property that $C^{=m(n)}$ is $\mathcal{CIR}(2^{m(n)/4})$-hard (and thus $p(n)^2$-hard for $\mathcal{CIR}(m(n), p(n)^2 + p(n)2^{k(n)})$) with probability at least $1 - e^{-2^{m(n)/4}}$. Hence, the following algorithm together with the NP oracle set B defined as the join of the two sets

$$\{\langle C, 0^n \rangle \mid C^{=m(n)} \text{ is not } \mathcal{CIR}(2^{m(n)/4})\text{-hard}\}$$

and

$$\{\langle x, r_1, \ldots, r_k \rangle \mid \exists y \in \Sigma^{p(|x|)} : \sum_{i=1}^{k} c_{x,y}(r_i) \geq k/2\}$$

witnesses $L \in \mathrm{ZPP}^{\mathrm{NP}}$:

> **input** x, $|x| = n$;
> compute a $(p(n), l(n), m(n), k(n))$-design $\mathcal{D}$;
> **choose randomly** $C \subseteq \{0,1\}^{m(n)}$;
> **if** $0\langle C, 0^n \rangle \notin B$ **then**
>   compute the pseudorandom strings $r_1, \ldots, r_{2^{l(n)}}$ of $g_{\mathcal{D}}^C$ on all seeds;
>   **if** $1\langle x, r_1, \ldots, r_{2^{l(n)}} \rangle \in B$ **then accept else reject**
> **else output** ?

■

Notice that the ZPP algorithm in the above proof actually asks only two queries to its NP oracle.

We also note that Theorem 25 cannot be further improved to $\mathrm{AM} \subseteq \mathrm{ZPP}^{\mathrm{NP}}$ by relativizing techniques since there is an oracle relative to which AM is not contained in Σ_2^{P} [San89].

From the closure properties of MA (namely that MA is closed under conjunctive truth-table reductions) it easily follows that $\mathrm{NP}^{\mathrm{MA} \cap \mathrm{coMA}} \subseteq \mathrm{MA}$. From Theorem 25 we have $\mathrm{MA} \subseteq \mathrm{ZPP}^{\mathrm{NP}}$. Hence, $\mathrm{NP}^{\mathrm{MA} \cap \mathrm{coMA}} \subseteq \mathrm{ZPP}^{\mathrm{NP}}$, implying that $\mathrm{ZPP}^{\mathrm{NP}^{\mathrm{MA} \cap \mathrm{coMA}}} \subseteq \mathrm{ZPP}^{\mathrm{ZPP}^{\mathrm{NP}}} = \mathrm{ZPP}^{\mathrm{NP}}$. We have proved the following corollary.

Corollary 26 $\mathrm{MA} \cap \mathrm{coMA}$ is low for $\mathrm{ZPP}^{\mathrm{NP}}$ and, consequently, BPP is low for $\mathrm{ZPP}^{\mathrm{NP}}$.

Acknowledgment

We would like to thank Lance Fortnow for interesting discussions on the topic of this paper.

References

[ACR96] A. Andreev, A. Clementi, and J. Rolim. Hitting sets derandomize BPP. In *Proc. 23rd International Colloquium on Automata, Languages, and Programming*, Lecture Notes in Computer Science #1099, 357–368. Springer-Verlag, 1996.

[ACR97] A. Andreev, A. Clementi, and J. Rolim. Worst-case hardness suffices for derandomization: a new method for hardness-randomness trade-offs. In *Proc. 24th International Colloquium on Automata, Languages, and Programming*, Lecture Notes in Computer Science #1256, 177–187. Springer-Verlag, 1997.

[AK97a] V. Arvind and J. Köbler. On pseudorandomness and resource-bounded measure. Technical Report UIB-97-05, University of Ulm, March 1997.

[AK97b] V. Arvind and J. Köbler. On resource-bounded measure and pseudorandomness. In *Proc. 17th Conference on Foundations of Software Technology and Theoretical Computer Science*, Lecture Notes in Computer Science #1346, 235–249. Springer-Verlag, 1997. Erscheint bei Theoretical Computer Science.

[AS94] E. Allender and M. Strauss. Measure on small complexity classes with applications for BPP. In *Proc. 35th IEEE Symposium on the Foundations of Computer Science*, 807–818. IEEE Computer Society Press, 1994.

[Bab85] L. Babai. Trading group theory for randomness. In *Proc. 17th ACM Symposium on Theory of Computing*, 421–429. ACM Press, 1985.

[BDG90] J. L. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity II.* EATCS Monographs on Theoretical Computer Science. Springer-Verlag, 1990.

[BDG95] J. L. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity I.* EATCS Monographs on Theoretical Computer Science. Springer-Verlag, second edition, 1995.

[BG94] M. Bellare and S. Goldwasser. The complexity of decision versus search. *SIAM Journal on Computing*, **23**:97–119, 1994.

[FR96] L. Fortnow and N. Reingold. PP is closed under truth-table reductions. *Information and Computation*, **124**(1):1–6, 1996.

[GZ97] O. Goldreich and D. Zuckerman. Another proof that BPP$\subseteq$PH (and more). Technical Report TR97-045, Electronic Colloquium on Computational Complexity, October 1997.

[IW97] R. Impagliazzo and A. Wigderson. P=BPP unless E has sub-exponential circuits: derandomizing the XOR lemma. In *Proc. 29rd ACM Symposium on Theory of Computing*, 220–229. ACM Press, 1997.

[Kad89] J. Kadin. $\mathrm{P}^{\mathrm{NP}[\log n]}$ and sparse Turing-complete sets for NP. *Journal of Computer and System Sciences*, **39**:282–298, 1989.

[KL80] R. M. Karp and R. J. Lipton. Some connections between nonuniform and uniform complexity classes. In *Proc. 12th ACM Symposium on Theory of Computing*, 302–309. ACM Press, 1980.

[KT94] J. Köbler and T. Thierauf. Complexity-restricted advice functions. *SIAM Journal on Computing*, **23**(2):261–275, 1994.

[LM96] J. H. Lutz and E. Mayordomo. Cook versus Karp-Levin: separating reducibilities if NP is not small. *Theoretical Computer Science*, **164**:141–163, 1996.

[LS93] J. H. Lutz and W. J. Schmidt. Circuit size relative to pseudorandom oracles. *Theoretical Computer Science*, **107**:95–120, 1993.

[Lut92] J. H. Lutz. Almost everywhere high nonuniform complexity. *Journal of Computer and System Sciences*, **44**:220–258, 1992.

[Lut93] J. H. Lutz. A pseudorandom oracle characterization of BPP. *SIAM Journal on Computing*, **22**:1075–1086, 1993.

[Lut97] J. H. Lutz. Observations on measure and lowness for Δ_2^{P}. *Theory of Computing Systems*, **30**:429–442, 1997.

[NW94] N. Nisan and A. Wigderson. Hardness vs randomness. *Journal of Computer and System Sciences*, **49**:149–167, 1994.

[Pap94] C. Papadimitriou. *Computational Complexity.* Addison-Wesley, 1994.

[Rud97] S. Rudich. Super-bits, demi-bits, and NQP-natural proofs. In *Proc. 1st Intern. Symp. on Randomization and Approximation Techniques in Computer Science (Random'97)*, Lecture Notes in Computer Science #1269, 85–93. Springer-Verlag, 1997.

[San89] M. Santha. Relativized Arthur-Merlin versus Merlin-Arthur games. *Information and Computation*, **80**(1):44–49, 1989.

[Sch89] U. Schöning. Probabilistic complexity classes and lowness. *Journal of Computer and System Sciences*, **39**:84–100, 1989.

[Sha81] A. Shamir. On the generation of cryptographically strong pseudo-random sequences. In *Proc. 8th International Colloquium on Automata, Languages, and Programming*, Lecture Notes in Computer Science #62, 544–550. Springer-Verlag, 1981.

[SV85] S. Skyum and L. G. Valiant. A complexity theory based on boolean algebra. *Journal of the ACM*, **32**:484–502, 1985.

[Tod91] S. Toda. PP is as hard as the polynomial-time hierarchy. *SIAM Journal on Computing*, **20**:865–877, 1991.

[Wil85] C. Wilson. Relativized circuit complexity. *Journal of Computer and System Sciences*, **31**(2):169–181, 1985.

[Yao82] A. C. Yao. Theory and applications of trapdoor functions. In *Proc. 23rd IEEE Symposium on the Foundations of Computer Science*, 80–91. IEEE Computer Society Press, 1982.

[ZF87] S. Zachos and M. Fürer. Probabilistic quantifiers vs. distrustful adversaries. In *Proc. 7th Conference on Foundations of Software Technology and Theoretical Computer Science*, Lecture Notes in Computer Science #287, 443–455. Springer-Verlag, 1987.