On Higher Arthur-Merlin Classes

DENIS CHARLES [1] A. PAVAN [2] SAMIK SENGUPTA [3]

[1]Department of Computer Science and Engineering, State University of New York at Buffalo, Buffalo, NY 14260. Research supported in part by NSF grant CCR-9820140. Email: cdx@cse.buffalo.edu
[2]Department of Computer Science and Engineering, State University of New York at Buffalo, Buffalo, NY 14260. Email: aduri@cse.buffalo.edu
[3]Department of Computer Science and Engineering, State University of New York at Buffalo, Buffalo, NY 14260. Email: samik@cse.buffalo.edu

Abstract

We study higher Arthur-Merlin classes defined via several natural probabilistic operators BP, R and co-R. We investigate the complexity classes they define, and a number of interactions between these operators and the standard polynomial time hierarchy. We prove a hierarchy theorem for these higher Arthur-Merlin classes involving interleaving operators, and a theorem giving non-trivial upper bounds to the intersection of the complementary classes in the hierarchy.

1 Introduction

Arthur-Merlin Games were introduced by Bábai [B85] [BM88] to study the power of randomization in interaction. Goldwasser and Sipser [GS89]proved soon afterwards that these classes are equivalent in power to Interactive Proof Systems introduced by [GMR85]. In the last 15 years, this study has proved to be exceedingly successful in complexity theory [ZH86, BHZ87, ZF87, LFKN90, Sh90]. Eventually the study of these proof systems (and multi prover systems) led to perhaps the most spectacular achievement in the Theory of Computing in the last decade [BGKW88, LFKN90, Sh90, BFL91, BFLS91, FGLSM91, AS92, ALMSS92].

It is well known that some traditional complexity classes can be characterized by operators. For example $\mathrm{NP} = \exists \cdot \mathrm{P}, \Sigma_2 = \exists \cdot \forall \cdot \mathrm{P}$, using the existential and universal operators $\exists$ and $\forall$ respectively. They have been used fruitfully to prove (or to give simpler proofs of known) relations between complexity classes [ZF87, To91, WT92, VW93, VW95, VW97]. For example, Toda's Theorem was proved in this framework [To91]. In this approach, Zachos and Fürer [ZF87] showed that AM can also be characterized by the operator BP, i.e. $\mathrm{AM} = \mathrm{BP} \cdot \mathrm{NP}$. By successfully employing this operator machinery, they were able to give a simple and natural proof that the one-sided error version of AM coincides with the two-sided error version, and thus $\mathrm{AM} \subseteq \Pi_2$.

In this paper, we define higher Arthur-Merlin classes using several natural probabilistic operators BP, R and co-R. We consider the hierarchy of classes $\mathrm{BP} \cdot \Sigma_k$, for $k \geq 1$, and prove some intricate relations among these classes and Σ_ℓ and ZPP. The class $\mathrm{BP} \cdot \Sigma_k$ can also be thought of as an Arthur-Merlin game where Arthur has access to Σ_{k-1} oracle. By investigating the interactions between the BP operators and the polynomial-time hierarchy, we are able to obtain some non-trivial containments; for example, we show that $\Sigma_k^{\mathrm{AM}} = \Sigma_{k+1}$ for $k \geq 2$, whereas the naïve argument gives $\Sigma_k^{\mathrm{AM}} \subseteq \Sigma_{k+2}$. Similarly, by interleaving n levels of Σ_k classes and n levels of $\mathrm{BP} \cdot \Sigma_\ell$ classes, we obtain results that improve trivial containments by n levels.

Recently classes $\mathrm{ZPP}^{\mathrm{NP}}$ and $\mathrm{AM} \cap \text{co-AM}$ received much attention. Arvind and Köbler [AK97] and Goldreich and Zuckerman [GZ97] proved that MA is contained in $\mathrm{ZPP}^{\mathrm{NP}}$. Köbler and Watanabe [KW95] and Bshouty *et al.* [BCGKT95] proved that the polynomial-time hierarchy is in $\mathrm{ZPP}^{\mathrm{NP}}$, if NP has polynomial-size circuits. More recently Arvind and Köbler [AK00] proved that $\mathrm{AM} \cap \text{co-AM}$ is *low* for $\mathrm{ZPP}^{\mathrm{NP}}$, i.e., $\mathrm{ZPP}^{\mathrm{NP}^{\mathrm{AM} \cap \text{co-AM}}} \subseteq \mathrm{ZPP}^{\mathrm{NP}}$. We note that this containment is a significant improvement over the naïve bound.

We consider a generalization of the class $\mathrm{AM} \cap \text{co-AM}$. Let E_k be $\mathrm{BP} \cdot \Sigma_k \cap \mathrm{BP} \cdot \Pi_k$. We prove $\mathrm{NP}^{E_1} \subseteq \mathrm{ZPP}^{\mathrm{NP}}$ using the following technique: the ZPP machine sends the random bits to the NP oracle, which simulates $\mathrm{NP}^{\mathrm{AM} \cap \text{co-AM}}$ using those random bits. Arvind and Köbler's result follows as a simple corollary, and thereby, we obtain an alternative proof of their lowness theorem. We then prove a far reaching extension of this non-trivial upper bound. By interleaving n levels of E_k and n levels of Σ_l classes, we obtain an upper bound that improves over the trivial bound by n levels.

Our proofs illustrate the power of the operator machinery, when properly deployed. The apparent ease (even a tautness) with which these theorems on the hierarchy are revealed speaks volumes of its effectiveness. While the formalism of this operator machinery may appear austere and less vivid intuitively, it should also be pointed out that only through such a formalism can we even begin to state some of the delicate relations in this hierarchy.

2 Preliminaries

We give formal definitions in this section. An Arthur-Merlin game is a combinatorial game, played by Arthur–a probabilistic polynomial-time machine, and Merlin–a computationally unbounded Turing machine.

Given a string x, Merlin tries to convince Arthur that x belongs to some language L. The game consists of a finite number of moves that may depend on the length of x. The moves alternate between Arthur and Merlin. In each move Arthur (or Merlin) prints a finite string on a read-write communication tape. Arthur's moves can depend on his random bits. In the end Arthur either accepts or rejects x.

Bábai [B85, BM88] defines a language L to be in AM if for every string x of length n, the game consists of a random move by Arthur and a reply by Merlin. If $x \in L$, then there is a move by Merlin that makes Arthur accept with probability at least $\frac{3}{4}$; on the other hand, if $x \notin L$, then, for every possible move of Merlin, the probability that Arthur will accept is less than $\frac{1}{4}$.

This definition has error on both sides, i.e. if $x \in L$, Arthur may reject the string (with some small probability) and if $x \notin L$, Merlin may be able to convince Arthur that $x \in L$ with a small probability. One can define the one-sided error version, AM_1, which is defined similar to AM, except that when x is in the language then there exists a sequence of moves by Merlin that leads to the acceptance of x by Arthur *with probability one.*

Bábai [B85] [BM88] also defined the class MA. Here Merlin, instead of Arthur, moves first.

Proposition 1 *We know the following relationships about* AM.

1. $\mathrm{AM} = \mathrm{AM}_1$ *[ZF87].*
2. $\mathrm{AM} \subseteq \Pi_2$ *[BM88].*
3. $\mathrm{AM} \cap \text{co-AM} \subseteq \mathrm{ZPP}^{\mathrm{NP}}$.
4. $\mathrm{AM} \subseteq \text{co-RP}^{\mathrm{NP}} \subseteq \mathrm{BPP}^{\mathrm{NP}}$.

The following inclusions are known about MA: i) $\mathrm{MA} \subseteq \mathrm{ZPP}^{\mathrm{NP}}$ [AK97, GZ97], and ii)$\mathrm{NP}^{\mathrm{BPP}} \subseteq \mathrm{MA}$ [ZF87].

Now define the probabilistic operators BP and co-R.

Definition 1 *Given a class $\mathcal{C}$, a language L is in $\mathrm{BP} \cdot \mathcal{C}$ if there exists a language L' in $\mathcal{C}$ and a polynomial $p(\cdot)$ such that the following holds:*

$$x \in L \Longrightarrow \Pr_{r \in \{0,1\}^{p(n)}}[\langle x, r\rangle \in L'] \geq \frac{3}{4}$$

$$x \notin L \Longrightarrow \Pr_{r \in \{0,1\}^{p(n)}}[\langle x, r\rangle \in L'] \leq \frac{1}{4}$$

Zachos and Fürer [ZF87] showed that AM $=$ BP $\cdot$ NP. We can define the one-sided error version of BP $\cdot\, \mathcal{C}$ using the operator co-R. Again, the difference is if $x \in L$ then for every $r \in \{0,1\}^{p(n)}$ the tuple $\langle x, r\rangle$ is in L'. Then, by using the fact that AM $=$ AM$_1$ we obtain BP $\cdot$ NP $=$ co-R $\cdot$ NP. Similarly we can define the operator R. Note that for any complexity class $\mathcal{C}$, co-(R $\cdot\, \mathcal{C}$) $=$ co-R $\cdot$ co-$\mathcal{C}$.

We define higher Arthur-Merlin classes using these operators. First note that R $\cdot$ NP $=$ NP, in fact R $\cdot\, \Sigma_k = \Sigma_k$, for $k \geq 1$. Similarly, co-R $\cdot\, \Pi_k = \Pi_k$, for $k \geq 1$. So we do not obtain any new classes by applying the operator R (co-R) to Σ_k (Π_k respectively). Therefore, only co-R $\cdot\, \Sigma_k$ and R $\cdot\, \Pi_k$ are new classes, and since AM $=$ co-R $\cdot$ NP, co-R $\cdot\, \Sigma_k$ will be a generalization of AM. However, as the following proposition shows, we can equivalently consider BP $\cdot\, \Sigma_k$ as an extension of AM.

Proposition 2 *We extend Proposition 1 as follows:*

1. BP $\cdot\, \Sigma_k =$ co-R $\cdot\, \Sigma_k$.
2. co-R $\cdot\, \Sigma_k \subseteq \Pi_{k+1}$.
3. co-R $\cdot\, \Sigma_k \cap$ R $\cdot\, \Pi_k \subseteq$ ZPP$^{\Sigma_k}$.
4. BP $\cdot\, \Sigma_k \subseteq$ co-RP$^{\Sigma_k} \subseteq$ BPP$^{\Sigma_k}$.

Now, we consider the relativizations of the class AM. Given a class $\mathcal{C}$, AM$^{\mathcal{C}}$ is defined similar to the class AM where Arthur has access to some $L \in \mathcal{C}$ as the oracle. This generalization coincides with the classes we obtained by operators; namely, we can prove the following, given a class of languages $\mathcal{C}$,

Proposition 3 AM$^{\mathcal{C}} =$ co-R $\cdot$ NP$^{\mathcal{C}} =$ BP $\cdot$ NP$^{\mathcal{C}}$.

Hence, in particular AM$^{\Sigma_k} =$ BP $\cdot\, \Sigma_{k+1}$. Similarly, given class $\mathcal{C}$, we can define the class MA$^{\mathcal{C}}$.

Arvind and Köbler [AK00] proved a non-trivial result about AM $\cap$ co-AM. They showed that AM $\cap$ co-AM is *low* for ZPP$^{\rm NP}$, i.e, $\mathrm{ZPP}^{\mathrm{NP}^{\mathrm{AM}\cap\mathrm{co\text{-}AM}}} \subseteq \mathrm{ZPP}^{\mathrm{NP}}$. Note that a naïve attempt, that just uses the fact AM $\cap$ co-AM $\subseteq$ ZPP$^{\rm NP}$, yields $\mathrm{ZPP}^{\mathrm{NP}^{\mathrm{AM}\cap\mathrm{co\text{-}AM}}} \subseteq \mathrm{ZPP}^{\Sigma_2}$.

Theorem 1 *[AK00] For every language L in* AM $\cap$ co-AM, $\mathrm{ZPP}^{\mathrm{NP}^L} = \mathrm{ZPP}^{\mathrm{NP}}$.

The rest of the paper is organized as follows. In section 3, we shall prove results about BP $\cdot\, \Sigma_k$, culminating in Theorem 3 about the hierarchy with interleaving levels of BP $\cdot\, \Sigma_l$ and Σ_k. In section 4, we concentrate on BP $\cdot\, \Sigma_k \cap$ BP $\cdot\, \Pi_k$. We extend the lowness results about AM $\cap$ co-AM and prove Theorem 6 about interleaving levels of BP $\cdot\, \Sigma_l \cap$ BP $\cdot\, \Pi_l$ and Σ_k.

3 On BP $\cdot\, \Sigma_k$

We begin with the following result and generalize it later.

Lemma 1 $\mathrm{NP}^{\mathrm{AM}} \subseteq \mathrm{MA}^{\mathrm{NP}}$.

Proof : Let $L \in \mathrm{NP}^{\mathrm{AM}}$. Then there is a language $A \in \mathrm{AM}$ and a polynomial-time bounded non-deterministic oracle Turing machine N^A, that accepts the language L. Consider the following $\mathrm{MA}^{\mathrm{NP}}$ protocol: Merlin provides an accepting computation of N^A with query answers filled in. Arthur, here, is a $\mathrm{BPP}^{\mathrm{NP}}$ machine. Since both AM and co-AM are in $\mathrm{BPP}^{\mathrm{NP}}$, Arthur can verify that the path given by Merlin is indeed a correct accepting computation.

The following theorem is a natural extension of the above Lemma.

Theorem 2

$$\mathrm{NP}^{\mathrm{BP}\cdot\Sigma_l} \subseteq \mathrm{MA}^{\Sigma_l} \subseteq \mathrm{ZPP}^{\Sigma_{l+1}}, \textit{ for } l \geq 0.$$

Proof : Note that when $l = 0$, the theorem is saying $\mathrm{NP}^{\mathrm{BPP}} \subseteq \mathrm{MA} \subseteq \mathrm{ZPP}^{\mathrm{NP}}$. All these inclusions are known. The proof of the case $l \geq 1$ is similar to the proof of previous lemma. For the first containment, Merlin gives an accepting computation of the NP machine with query answers filled in. Arthur, now a BPP^{Σ_l} machine can verify the all the query answers are correct, as $\mathrm{BP}\cdot\Sigma_l$ and co-$\mathrm{BP}\cdot\Sigma_l$ are subsets of BPP^{Σ_l}. The second inclusion follows from modifying the proof of $\mathrm{MA} \subseteq \mathrm{ZPP}^{\mathrm{NP}}$.

The following two equalities can be easily proved using the fact that $\mathrm{NP}^{\mathrm{ZPP}} = \mathrm{NP}$.

Lemma 2

$$\Sigma_k^{\mathrm{ZPP}^{\Sigma_l}} = \Sigma_{k+l}, \textit{ for } k \geq 1, l \geq 0.$$
$$\mathrm{BP}\cdot\Sigma_k^{\mathrm{ZPP}^{\Sigma_l}} = \mathrm{BP}\cdot\Sigma_{k+l}, \textit{ for } k \geq 1, l \geq 0.$$

Next, we consider a hierarchy with interleaving levels of $\mathrm{BP}\cdot\Sigma_l$. The upper bound in this theorem is an improvement of n levels over the trivial bounds. and Σ_k.

Theorem 3 *1. For $k_1, \ldots, k_n \geq 1$ and $l_1, \cdots l_n \geq 0$, where $n \geq 1$*

$$\Sigma_{k_1}^{\mathrm{BP}\cdot\Sigma_{l_1}^{\cdot^{\cdot^{\cdot^{\Sigma_{k_n}^{\mathrm{BP}\cdot\Sigma_{l_n}}}}}}} \subseteq \mathrm{ZPP}^{\Sigma_{k_1+k_2+\cdots+k_n+l_1+l_2+\cdots+l_n}}.$$

2. For $k_1 \geq 2$, $k_2, \ldots, k_n \geq 1$, and $l_1, \cdots l_n \geq 0$, where $n \geq 1$

$$\Sigma_{k_1}^{\mathrm{BP}\cdot\Sigma_{l_1}^{\cdot^{\cdot^{\cdot^{\Sigma_{k_n}^{\mathrm{BP}\cdot\Sigma_{l_n}}}}}}} = \Sigma_{k_1+k_2+\cdots+k_n+l_1+l_2+\cdots+l_n}.$$

Proof :

We prove the first equality, by induction on n, the number of levels. Our base case is

$$\Sigma_k^{\mathrm{BP}\cdot\Sigma_l} \subseteq \mathrm{ZPP}^{\Sigma_{k+l}}, \text{ for } k \geq 1, l \geq 0,$$

which we shall prove by induction on k. We know, by Theorem 2, that $\mathrm{NP}^{\mathrm{BP}\cdot\Sigma_l} \subseteq \mathrm{ZPP}^{\Sigma_{l+1}}$. So when $k = 1$ the base case is true. Now consider the case $k \geq 2$. Assume $\Sigma_{k-1}^{\mathrm{BP}\cdot\Sigma_l} \subseteq \mathrm{ZPP}^{\Sigma_{k+l-1}}$, for $k \geq 2$. Now,

$$\begin{aligned} \Sigma_k^{\mathrm{BP}\cdot\Sigma_l} &= \mathrm{NP}^{\Sigma_{k-1}^{\mathrm{BP}\cdot\Sigma_l}} \\ &\subseteq \mathrm{NP}^{\mathrm{ZPP}^{\Sigma_{k+l-1}}} \text{(by assumption)} \\ &= \Sigma_{k+l} \subseteq \mathrm{ZPP}^{\Sigma_{k+l}} \text{ (by Lemma 2).} \end{aligned}$$

Let us assume that, for $k_2, \ldots, k_n \geq 1$ and $l_2, \ldots l_n \geq 0$

$$\Sigma_{k_2}^{\mathrm{BP}\cdot\Sigma_{l_2}^{\cdot^{\cdot^{\cdot^{\Sigma_{k_n}^{\mathrm{BP}\cdot\Sigma_{l_n}}}}}}} \subseteq \mathrm{ZPP}^{\Sigma_{k_2+\cdots+k_n+l_2+\cdots+l_n}}.$$

The following inclusions prove item 1.

$$\begin{aligned} \Sigma_{k_1}^{\mathrm{BP}\cdot\Sigma_{l_1}^{\cdot^{\cdot^{\cdot^{\Sigma_{k_n}^{\mathrm{BP}\cdot\Sigma_{l_n}}}}}}} &\subseteq \Sigma_{k_1}^{\mathrm{BP}\cdot\Sigma_{l_1}^{\mathrm{ZPP}^{\Sigma_{k_2+\cdots+k_n+l_2+\cdots+l_n}}}} \text{(by assumption)} \\ &= \Sigma_{k_1}^{\mathrm{BP}\cdot\Sigma_{k_2+\cdots+k_n+l_1+l_2+\cdots+l_n}} \text{(by Lemma 2)} \\ &\subseteq \mathrm{ZPP}^{\Sigma_{k_1+k_2+\cdots+k_n+l_1+l_2+\cdots+l_n}} \text{(By base case)} \end{aligned}$$

Now we treat the case where $k_1 \geq 2$. We first prove that $\Sigma_2^{\mathrm{BP}\cdot\Sigma_l} = \Sigma_{l+2}$. We know, by Theorem 2, that $\mathrm{NP}^{\mathrm{BP}\cdot\Sigma_l} \subseteq \mathrm{ZPP}^{\Sigma_{l+1}}$. So $\Sigma_2^{\mathrm{BP}\cdot\Sigma_l} \subseteq \mathrm{NP}^{\mathrm{ZPP}^{\Sigma_{l+1}}} = \Sigma_{l+2}$, by Lemma 2. Since $\Sigma_{l+2} \subseteq \Sigma_2^{\mathrm{BP}\cdot\Sigma_l}$ we obtain $\Sigma_2^{\mathrm{BP}\cdot\Sigma_l} = \Sigma_{l+2}$. If $k > 2$ then

$$\begin{aligned} \Sigma_k^{\mathrm{BP}\cdot\Sigma_l} &= \mathrm{NP}^{\mathrm{NP}^{\Sigma_{k-2}^{\mathrm{BP}\cdot\Sigma_l}}}, k-2 \geq 1 \\ &\subseteq \mathrm{NP}^{\mathrm{NP}^{\mathrm{ZPP}^{\Sigma_{k+l-2}}}} \text{ by item 1} \\ &\subseteq \Sigma_{k+l} \text{ by Lemma 2} \end{aligned}$$

Since the other inclusion is clear, we have $\Sigma_k^{\mathrm{BP}\cdot\Sigma_l} = \Sigma_{k+l}$ for $k \geq 2$ and $l \geq 0$.

Now,

$$\begin{aligned} \Sigma_{k_1}^{\mathrm{BP}\cdot\Sigma_{l_1}^{\cdot^{\cdot^{\cdot^{\Sigma_{k_n}^{\mathrm{BP}\cdot\Sigma_{l_n}}}}}}} &\subseteq \Sigma_{k_1}^{\mathrm{BP}\cdot\Sigma_{l_1}^{\mathrm{ZPP}^{\Sigma_{k_2+\cdots+k_n+l_2+\cdots+l_n}}}} \text{(by item 1)} \\ &= \Sigma_{k_1}^{\mathrm{BP}\cdot\Sigma_{k_2+\cdots+k_n+l_1+l_2+\cdots+l_n}} \text{(by Lemma 2)} \\ &= \Sigma_{k_1+k_2+\cdots+k_n+l_1+l_2+\cdots+l_n} \text{(by base case)} \end{aligned}$$

The other inclusion is obvious.

4 On $\mathrm{BP} \cdot \Sigma_k \cap \mathrm{BP} \cdot \Pi_k$

Definition 2 *Let* $E_k \equiv \mathrm{BP} \cdot \Sigma_k \cap \mathrm{BP} \cdot \Pi_k$, *and if* $\mathcal{C}$ *is a class of languages we define* $E_k^{\mathcal{C}} \equiv \mathrm{BP} \cdot \Sigma_k^{\mathcal{C}} \cap \mathrm{BP} \cdot \Pi_k^{\mathcal{C}}$.

Note that $E_k^{\Sigma_l} = E_{k+l}$. In this section we study the interaction of the class E_k with Σ_k classes. Recall that $\mathrm{AM} \cap \text{co-AM} \subseteq \mathrm{ZPP}^{\mathrm{NP}}$; in fact Arvind and Köbler [AK00] proved that $\mathrm{AM} \cap \text{co-AM}$ is low for $\mathrm{ZPP}^{\mathrm{NP}}$. By using the following theorem, we offer a different proof of their result, which we believe is intuitively clearer.

Theorem 4

$$\mathrm{NP}^{\mathrm{AM} \cap \text{co-AM}} \subseteq \mathrm{ZPP}^{\mathrm{NP}}$$

Proof : Let $L \in E_1 = \mathrm{AM} \cap \mathrm{coAM}$. By definition there exist two deterministic polynomial-time computable predicates $A(\cdot,\cdot,\cdot)$ and $B(\cdot,\cdot,\cdot)$ and a polynomial $p(\cdot)$ such that the following holds: $\forall x \in \{0,1\}^n$: let $m = p(n)$

$$\begin{array}{rcl} x \in L & \Rightarrow & \forall r \in \{0,1\}^m : \exists w \in \{0,1\}^m : A(x,w,r) \\ & \text{AND} & \Pr_{r \in \{0,1\}^m}[\forall w \in \{0,1\}^m : \neg B(x,w,r)] \geq \dfrac{3}{4} \\ x \notin L & \Rightarrow & \Pr_{r \in \{0,1\}^m}[\forall w \in \{0,1\}^m : \neg A(x,w,r)] \geq \dfrac{3}{4} \\ & \text{AND} & \forall r \in \{0,1\}^m : \exists w \in \{0,1\}^m : B(x,w,r) \end{array}$$

We will show that $\mathrm{NP}^L \subseteq \mathrm{ZPP}^{\mathrm{NP}}$. Let $S \in \mathrm{NP}^L$ and let N be an oracle Turing machine which witnesses this membership. Let $T(n)$ be the bound on running time of N. Hence, N can query strings of length at most $T(n)$. We want to amplify the success probability for A and B so that for most of the random strings r, for all queries q and for all w, if $q \in L$ then $B(q,w,r)$ doesn't hold, and if $q \notin L$, then $A(q,w,r)$ doesn't hold. Let $l(n)$ be the bound on the length of the random strings that achieves such amplification.

Now we define a non-deterministic Turing machine N'. Let $|x| = n$ and ν be a string of length $l(n) \times T(n)$. Clearly $|\nu|$ is a polynomial in n. We shall treat ν as $T(n)$ strings of length $l(n)$ each. N' on input $\langle x, \nu \rangle$ operates as follows. It simulates N on input x. Whenever N poses a query q to the oracle L, N' non-deterministically guesses an answer $a_q \in \{\mathrm{Yes}, \mathrm{No}\}$ and then uses r, a segment of ν, as random bits and also guesses a proof w and verifies that the following holds:

$$\begin{array}{rl} a_q = \mathrm{Yes} & \Rightarrow A(q,w,r) \\ a_q = \mathrm{No} & \Rightarrow B(q,w,r). \end{array}$$

Note that due to our amplification, if $q \notin L$ then for every w $A(q,w,r)$ holds with miniscule probability; and if $q \in L$, similarly, for every w, it is highly unlikely that $B(q,w,r)$ holds. N' accepts $\langle x, \nu \rangle$ at the end of a path if N accepts x; therefore, an accepting computation of N' consists of queries to L along with the guessed answers and the proofs. Note that if N^L accepts x, then $\forall \nu$, N' accepts $\langle x, \nu \rangle$. Moreover, most of the accepting computations of N' correspond to an accepting computation of N^L by our choice of ν. And also, if N^L rejects x, N' accepts $\langle x, \nu \rangle$ with a small probability.

Now we construct a probabilistic oracle Turing machine M with oracle access to **SAT** that recognizes S. Given an x with $|x| = n$, it generates a random string ν of length $l(n) \times T(n)$. Then, M poses the query to the **SAT** oracle asking (using Cook reduction) whether there is an accepting path of N' on input $\langle x, \nu \rangle$ and if so, M finds such a path C using the self-reducibility of **SAT**. If the answer was "No" then M rejects x. If the answer was "Yes" then M verifies that C is indeed a correct accepting computation of N' on $\langle x, \nu \rangle$. M can verify that the answers to the queries in C are correct since both L and $\overline{L}$ are in $\mathrm{AM} \cap \text{co-AM} \subseteq \mathrm{ZPP}^{\mathrm{NP}}$ and M itself is a $\mathrm{ZPP}^{\mathrm{NP}}$ machine. If M successfully verifies all the answers then it accepts x, and otherwise outputs "?".

If $x \in S$ then there exists an accepting computation of N^L, and so, for every ν, N' accepts $\langle x, \nu \rangle$. Clearly, M never rejects in this case; it outputs "?" only if the computation C happens to be a accepting computation of N' that doesn't correspond to an accepting computation of N^L, which can happen only with a negligible probability. On the other hand, if $x \notin S$, the first query of M will be answered "No" with high probability, and M rejects x in that case; if the answer to the query was "Yes", then C has some queries that are answered wrong, and during the verification of C by M, this will be detected and M outputs "?".

Now $\mathrm{ZPP}^{\mathrm{NP}^{\mathrm{AM} \cap \text{co-AM}}} \subseteq \mathrm{ZPP}^{\mathrm{ZPP}^{\mathrm{NP}}} = \mathrm{ZPP}^{\mathrm{NP}}$. Thus we obtain an alternate proof of Arvind and Köbler's result.

Corollary 1 *[AK00]* $\mathrm{AM} \cap \text{co-AM}$ *is low for* $\mathrm{ZPP}^{\mathrm{NP}}$.

Next we try to generalize the previous theorem.

Lemma 3

$$\mathrm{NP}^{\mathrm{E}_l} \subseteq \mathrm{ZPP}^{\Sigma_l}, \textit{ for } l \geq 1.$$

Proof : It is clear that the above lemma relativizes. So we have

$$\begin{aligned} \mathrm{NP}^{\mathrm{E}_l} &= \mathrm{NP}^{\mathrm{E}_1^{\Sigma_{l-1}}} \\ &\subseteq \mathrm{ZPP}^{\mathrm{NP}^{\Sigma_{l-1}}} \\ &= \mathrm{ZPP}^{\Sigma_l}. \end{aligned}$$

Theorem 5 *For* $k \geq 2, l \geq 1$

$$\Sigma_k^{\mathrm{E}_l} = \Sigma_{k+l-1}$$

Proof :

We again prove this by induction. Base case is $\mathrm{NP}^{\mathrm{NP}^{\mathrm{E}_l}} = \Sigma_{l+1}$.

$$\begin{aligned} \mathrm{NP}^{\mathrm{NP}^{\mathrm{E}_l}} &\subseteq \mathrm{NP}^{\mathrm{ZPP}^{\Sigma_l}} \text{(by previous lemma)} \\ &= \Sigma_{l+1} \text{(by Lemma 2)}. \end{aligned}$$

Let us assume $\Sigma_{k-1}^{\mathrm{E}_l} \subseteq \mathrm{ZPP}^{\Sigma_{k+l-2}}$, for $k \geq 3$. Now,

$$\begin{aligned}\Sigma_k^{\mathrm{E}_l} &= \mathrm{NP}^{\Sigma_{k-1}^{\mathrm{E}_l}} \\ &\subseteq \mathrm{NP}^{\mathrm{ZPP}^{\Sigma_{k+l-2}}} \text{(by assumption)} \\ &= \Sigma_{k+l-1} \text{ (by Lemma 2)}\end{aligned}$$

Since E_l clearly contains $Sigma_{l-1}$ the other inclusion also holds.

We obtain following corollary.

Corollary 2 AM ∩ co-AM *is low for* Σ_k, $k \geq 2$.

Theorem 6 *For* $k \geq 1$ *and* $l \geq 1$

$$E_k^{\mathrm{ZPP}^{\Sigma_l}} = E_{k+l}$$

Proof :

$$\begin{aligned}E_k^{\mathrm{ZPP}^{\Sigma_l}} &= \mathrm{BP}\cdot\Sigma_k^{\mathrm{ZPP}^{\Sigma_l}} \cap \mathrm{BP}\cdot\Pi^{\mathrm{ZPP}^{\Sigma_l}} \\ &= \mathrm{BP}\cdot\Sigma_{k+l} \cap \mathrm{BP}\cdot\Pi_{k+l}\text{by Lemma2}\end{aligned}$$

Theorem 7 *1. For* $l_1, l_2, \ldots, l_n, k_1, k_2, \ldots, k_n \geq 1$, $n \geq 1$,

$$\Sigma_{l_1}^{E_{k_1}^{\Sigma_{l_2}^{\cdot^{\cdot^{\cdot^{\Sigma_{l_n}^{E_{k_n}}}}}}}} \subseteq \mathrm{ZPP}^{\Sigma_{l_1+l_2+\cdots+l_n+k_1+k_2+\cdots+k_n-n}}.$$

2. For $l_1 \geq 2$ *and* $l_2, \ldots, l_n, k_1, k_2, \ldots, k_n \geq 1$, $n \geq 1$,

$$\Sigma_{l_1}^{E_{k_1}^{\Sigma_{l_2}^{\cdot^{\cdot^{\cdot^{\Sigma_{l_n}^{E_{k_n}}}}}}}} = \Sigma_{l_1+l_2+\cdots+l_n+k_1+k_2+\cdots+k_n-n}.$$

Proof :

We prove first inclusion by induction. Our base case $\Sigma_l^{E_k} \subseteq \mathrm{ZPP}^{\Sigma_{k+l-1}}$ is due to Theorem 5 and Lemma 3. Now assume

$$\Sigma_{l_2}^{E_{k_2}^{\Sigma_{l_3}^{\cdot^{\cdot^{\cdot^{\Sigma_{l_n}^{E_{k_n}}}}}}}} \subseteq \mathrm{ZPP}^{\Sigma_{l_2+\cdots+l_n+k_2+\cdots+k_n-(n-1)}}.$$

Now,

$$
\begin{aligned}
\Sigma_{l_1}^{E_{k_1}^{\Sigma_{l_2}^{\cdot^{\cdot^{\cdot^{\Sigma_{l_n}^{E_{k_n}}}}}}}} &\subseteq \Sigma_{l_1}^{E_{k_1}^{\mathrm{ZPP}^{\Sigma_{l_2+\cdots+l_n+k_2+\cdots+k_n-(n-1)}}}} && \text{(by assumption)} \\
&= \Sigma_{l_1}^{E_{l_2+\cdots+l_n+k_1+k_2+\cdots+k_n-(n-1)}} && \text{(by previous theorem)} \\
&\subseteq \mathrm{ZPP}^{\Sigma_{k_1+k_2+\cdots+k_n+l_1+\cdots l_n-n}} && \text{(by Theorem 5)}
\end{aligned}
$$

Now, for the second equality the base case, $\Sigma_l^{E_k} = \Sigma_{k+l-1}$ where $l \geq 2$, is true due to Theorem 5. The following inclusions prove the theorem.

$$
\begin{aligned}
\Sigma_{l_1}^{E_{k_1}^{\Sigma_{l_2}^{\cdot^{\cdot^{\cdot^{\Sigma_{l_n}^{E_{k_n}}}}}}}} &\subseteq \Sigma_{l_1}^{E_{k_1}^{\mathrm{ZPP}^{\Sigma_{l_2+\cdots+l_n+k_2+\cdots+k_n-(n-1)}}}} && \text{(by item 1)} \\
&= \Sigma_{l_1}^{E_{l_2+\cdots+l_n+k_1+k_2+\cdots+k_n-(n-1)}} && \text{(by Theorem 6)} \\
&= \Sigma_{l_1+l_2+\cdots+l_n+k_1+k_2+\cdots+k_n-n} && \text{(by Theorem 5)}
\end{aligned}
$$

The other inclusion is trivial.

5 Conclusions

We have considered natural extensions of the class AM using the BP operator. We have established several non-trivial relations involving these classes and the polynomial hierarchy. We note that by extending a result of Agrawal and Thierauf [AT97] we get problems in $\mathrm{BP} \cdot \Sigma_k \cap \Pi_k$. This can be achieved by considering *Circuit Isomorphism problem* with Σ_{k-2} oracle gates. Observe that these languages can not be complete for Π_k unless hierarchy collapses. However, it would be interesting to give natural examples of languages in $\mathrm{BP} \cdot \Sigma_k \cap \Pi_k$.

Another possible extension will be to obtain a similar operator characterization of MA, and to shed some light on their relationships with the hierarchy.

References

[AK97] V. Arvind and J. Köbler, *On Pseudorandomness and Resource-Bounded Measure*, Proc. 17th FST and TCS, Springer-Verlag, LNCS 1346, 235-249, 1997.

[AK00] V. Arvind and J. Köbler, *Graph isomorphism is low for ZPP^{NP} and other lowness results*, STACS 2000.

[ALMSS92] S. Arora, C. Lund, R. Motwani, M. Sudan and M. Szegedy, *Proof verification and hardness of approximation problems.* Proceedings of the 33rd IEEE Symposium on Foundations of Computer Science, 14–23, 1992.

[AS92] S. Arora and S. Safra, *Approximating clique is NP-complete.*, Proceedings of the 33rd IEEE Symposium on Foundations on Computer Science, 2–13, 1992.

[AT97] M. Agrawal and T. Thierauf, *The Boolean isomorphism problem*, Proc. 37th Annual Symposium on Foundations of Computer Science, 422–430.

[B85] L. Bábai, *Trading group theory for randomness*, STOC 17:421–429(85).

[BFL91] L. Bábai, L. Fortnow and C. Lund, *Nondeterministic exponential time has two-prover interactive protocols.* Computational Complexity, 1(1):3–40, 1991.

[BFLS91] L. Bábai, L. Fortnow, L. Levin and M. Szegedy, *Checking computations in polylogarithmic time.* Proceedings of the 23rd ACM Symopsium on Theory of COmputing, 21–31, 1991.

[BM88] L. Bábai and S. Moran, *Arthur-Merlin Games : a randomized proof system, and a hierarchy of complexity classes*, Journal of Computer and System Sciences, 36:254-276, 1988.

[BGKW88] M. Ben-Or, S. Goldwasser, J. Kilian, and A. Wigderson, *Multiprover interactive proofs: How to remove the intractability assumptions*, in Proc. 20th Ann. ACM Symp. Theory of Computing, 1988, 113-131.

[BHZ87] R. Boppana, J. Hastad and S. Zachos, *Does* co-NP *have short interactive proofs?*, Information Processing Letters, 25:127-132, 1987.

[BCGKT95] N. Bshouty, R. Cleve, S. Kannan and C. Tamon, *Oracles and Queries that are sufficient for Exact Learning*, Proceedings of the 17th Annual ACM conference on Computational Learning Theory, 130–19 (1994).

[FGLSM91] U. Feige, S. Goldwasser, L. Lovász, S. Safra, M. Szegedy, *Aprroximating clique is akmost NP-complete.* Proceedings of the 32nd 32nd IEEE Symposium on Foundations of Computer Science, 2–12, 1991.

[GMR85] S. Goldwasser, S. Micali and C. Rackoff, *The Knowledge Complexity of Interactive Proofs*, Proc. 17th ACM Symp. om Computing, Providence, RI, 1985, pp. 291-304.

[GS89] S. Goldwasser and M. Sipser, *Private coins versus public coins in interactive proof systems*, STOC 18:59–68(1986).

[GZ97] O.Goldreich and D.Zuckerman, *Another Proof that BPP $\subseteq$ PH (and more)*, ECCC, TR97-045, October 1997.

[HW00] H. Hempel and G. Wechsung, *The Operators min and max on the Polynomial Hierarchy*, IJFCS, 11:315-342, 2000.

[KW95] J. Köbler and O. Watanabe, *New collapse consequences of NP having small circuits* ICALP, LNCS 944:196–207(1995).

[LFKN90] C. Lund, L. Fortnow, H. Karloff and N. Nisan, *Algebraic Methods for Interactive Proof Systems*, Journal of the ACM, 39(4):859-868, October 1992.

[OH93] M. Ogihara and L. Hemachandra, *A complexity theory for closure properties.* Journal of Computer Systems and Sciences, 46(3):295–325, 1993.

[Sh90] A. Shamir, *IP = PSPACE*, Journal of the ACM, 39(4):869-877, October 1992.

[To91] S. Toda, *PP is as hard as polynomial-time hierarchy.* SIAM Journal on Computing, 20(5):865–877, 1991.

[VW93] H. Vollmer and K. Wagner, *The complexity of finding middle elements.* International Journal of Foundations of Computer Science, 4:293–307, 1993.

[VW95] H. Vollmer and K. Wagner, *Complexity classes of optimization functions.* Information and Computation, 120(2):198–219, 1995.

[VW97] H. Vollmer, K. W. Wagner, *On Operators of higher types.* Proc. 12th Conf on computational Complexity, pages 174-184. IEEE, 1997.

[WT92] O. Watanabe and S. Toda, *Polynomial time 1-Turing reductions from #PH to #P.* Theoritical Computer Science, 100(1):205–221, 1992.

[ZH86] S. Zachos and H. Heller, *A Decisive characterization of BPP*, Information and Control, 69:125–135(1986).

[ZF87] S. Zachos and M. Fürer, *Probabilistic quantifiers vs Distrustful adversaries*, FSTTCS 1987, LNCS-287:449–455.