Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 88 (2018)

The Untold Story of SBP

Ilya Volkovich*

Abstract

In the seminal work of [Bab85], Babai have introduced *Arthur-Merlin Protocols* and in particular the complexity classes MA and AM as randomized extensions of the class NP. While it is easy to see that $\mathsf{NP} \subseteq \mathsf{MA} \subseteq \mathsf{AM}$, it has been a long standing open question whether these classes are actually different. In [BGM06], Böhler et al. introduced the probabilistic class of SBP and showed that $\mathsf{MA} \subseteq \mathsf{SBP} \subseteq \mathsf{AM}$. Indeed, this is the only known natural complexity class that lies between MA and AM. In this work we study the relations between these classes further, partially answering some open questions posed in [BGM06].

1 Introduction

For more than three decades, the question of whether the classes MA and AM are different had remained open. While it was shown that under widely-believed derandomization assumptions [KvM02, MV05] $\mathsf{MA} = \mathsf{AM}$ and, moreover, both to collapse to NP, there has been only a mild advancement on this front. In particular, Arvind et al. [AKSS95] showed that $\mathsf{AM} = \mathsf{MA}$ if $\mathsf{NP} \subseteq \mathsf{P/poly}$. Yet, the same premises imply a collapse of the Polynomial Hierarchy (see e.g. [KL80]) and hence are not *believed* to be true.

In [BGM06], Böhler et al. introduced the class of SBP, which stands for *small bounded-error probability*. They also showed that SBP lies between MA and AM. To the best of our knowledge, SBP is the only natural class with this property. However, the only known conditional collapse results of either AM to SBP or SBP to MA are actually those that collapse AM all the way to MA.

SZK (Statistical Zero Knowledge) is the class of decision problems for which a "yes" answer can be verified by a statistical zero-knowledge proof protocol. Rather than providing a formal definition, the class can be captured by its complete (promise) problem known as *Statistical Difference* [SV03]: given two polynomial-size circuits, C_0 and C_1 on n variables, decide if the statistical distance between the induced probability distributions is either at most $1/3$ or at least $2/3$. This problem is denoted as $\mathrm{SD}^{(2/3,1/3)}$. Similarly to SBP, $\mathsf{SZK} \subseteq \mathsf{AM}$ (see e.g. [For89]).

A different line of work [Val76, All86, Mor82] has been involved with the study of the computational power of NP machines with bounded number of accepting paths (or witnesses). In [Val76], Valiant introduced the complexity class UP that consists of NP problems with unique solutions. For instance, UNIQUE-SAT stands for a version of the SAT problem in which the given Boolean formula φ is either unsatisfiable or contains **exactly** one satisfying assignment. Another natural example of such class is FewP, introduced by Allender in [All86], which consists of NP problems with polynomially-many solutions. More generally, we consider the class $\mathsf{SOLUTIONS}[f(n)]$ that consists of NP problems with at most $f(n)$ accepting paths or solution, for inputs of size of n. For a formal definition, see Definition 2.15.

*Department of EECS, CSE Division, University of Michigan, Ann Arbor, MI. Email: ilyavol@umich.edu.

ISSN 1433-8092

1.1 Our Results

Our first main result links the aforementioned lines of work:

Theorem 1. *Suppose there exists* $\varepsilon > 0$ *such that* 3-SAT $\in \mathsf{SOLUTIONS}[2^{n^{1-\varepsilon}}]$. *Then* $\mathsf{AM} = \mathsf{SBP}$.

In other words, if there exists an NP machine that decides 3-SAT with somewhat less than trivial number of accepting paths, then AM collapses to SBP. In particular, the result holds if 3-SAT $\in$ UP or even if 3-SAT $\in$ FewP. To put the result in the correct context, note that even a subexponential number of accepting paths is not known to imply a (deterministic) subexponential-time algorithm. In fact, such an implication is not even known for the case of a unique path (i.e. SAT $\in$ UP).

We now would like to elaborate on the premises. For a 3-CNF φ of size s, the NP machine is required to have at most $2^{s^{1-\varepsilon}}$ accepting paths for some $\varepsilon > 0$. This requirement is trivially met when $s = n^{1+\delta}$, for $\delta > 0$. Indeed, the main challenge is to satisfy the requirement for formulas of linear and slightly super-linear sizes (i.e. when $s = \mathcal{O}(n)$ or $s = n \cdot \mathrm{polylog}(n)$). Furthermore, we observe that the requirement is met for formulas of size n if and only if it is met for formulas of size $n \cdot \mathrm{polylog}(n)$. This in turn allows to define the size of a formula as a number of clause as opposed to the encoding (i.e. bit) size, as these two notions are within poly-logarithmic factor from each other. For more details see Section 2.3

In terms of oracle separation, in [Ver92], Vereshchagin have shown that while MA $\subseteq$ PP for every oracle, there exists an oracle that separates AM from PP. In [BGM06], Böhler et al. have extended this inclusion to MA $\subseteq$ SBP $\subseteq$ PP $\cap$ AM. As a corollary, they have concluded that the same oracle also separates SBP from PP. Furthermore, it is an easy exercise to see that AM is closed under union and intersection. Yet, whether SBP is closed under intersection remains an open question. In [GLM$^+$16], Göös et al. have shown an oracle relative to which SBP is not closed under intersection. In conclusion, the collapse of AM to SBP should evade numerous relativization barriers. In [Rub88], Rubinstein have shown an oracle relative to which SAT is not in UP and FewP. Since the proof of Theorem 1 is relativizable, we obtain a further oracle separation as a corollary:

Corollary 1.1. *There exist an oracle relative to which for any* $\varepsilon > 0$*,* SAT $\notin \mathsf{SOLUTIONS}[2^{n^{1-\varepsilon}}]$.

This result partially answers an open question posed in [BGM06], whether one could extend the oracle separations to collapse consequences.

1.1.1 Relations Between SBP and SZK

Our next result studies the relation between SBP and SZK. To that end, we consider the *general Statistical Difference* problem: for functions $\alpha(n) > \beta(n)$, $\mathrm{SD}^{(\alpha(n),\beta(n))}$ is the (promise) problem of deciding whether the statistical distance is either at most $\beta(n)$ or at least $\alpha(n)$ (for a formal definition, see Definition 2.13). Our next main result exhibits a non-trivial problem in the intersection of the promised versions of SZK and SBP.

Theorem 2. $\overline{\mathrm{SD}}^{\left(1-\frac{1}{2^{n+3}}\,,\,\frac{1}{2^{n+3}}\right)} \in \mathsf{PromiseSBP}$.

First of all, it is to be noted that since PromiseSZK is closed under complement (see e.g. [Oka00]), $\overline{\mathrm{SD}}^{\left(1-\frac{1}{2^{n+3}}\,,\,\frac{1}{2^{n+3}}\right)} \in \mathsf{PromiseSZK}$. Furthermore, the problem represents a somewhat more general version of $\overline{\mathrm{SD}}^{(1\,,\,0)}$, which is complete for the class of the so-called problems with "V-bit" perfect zero knowledge protocols [KMS15]. And while, $\overline{\mathrm{SD}}^{(1\,,\,0)} \subseteq \mathsf{PromiseNP}$ and hence is clearly in

PromiseSBP, to the best of our knowledge, $\overline{\mathrm{SD}}^{\left(1-\frac{1}{2^{n+3}}\,,\,\frac{1}{2^{n+3}}\right)}$ is not known to lie in any subclass of PromiseSBP (not even PromiseMA). In that sense, the proposed problem constitutes the first known non-trivial problem in PromiseSZK∩PromiseSBP. Indeed, this result partially answers another open question posed in [BGM06], whether there is a natural problem in SBP that is not contained in MA. It is to be noted that Watson [Wat16] has shown another natural problem complete for PromiseSBP.

1.1.2 Relation to Polarization

The *polarization lemma*, introduced by Sahai and Vadhan in [SV03], is an efficient transformation that takes as input a pair of Boolean circuits (C_0, C_1) and an integer k and coverts them into a new pair of circuits (D_0, D_1) such that:

$$\begin{aligned} \Delta(C_1, C_2) \geq 2/3 \quad &\Longrightarrow \Delta(D_1, D_2) \geq 1 - 2^k \\ \Delta(C_1, C_2) \leq 1/3 \quad &\Longrightarrow \Delta(D_1, D_2) \leq 2^k \end{aligned}$$

We would like to highlight one important aspect of this transformation: if the input circuits C_1 and C_2 are defined on n variables - i.e. the distributions are samplable using n random bits, the resulting circuits D_1 and D_2 are defined on $\mathrm{poly}(k) \cdot n$ variables, thus requiring more random bits. Similar phenomenon occurs when one tries to naively amplify the success probability of a BPP algorithm by a simple repetition. Indeed, if a given BPP algorithm achieves an error probability of $1/3$ using r random bits, one could drive down the error probability to 2^{-t} using $\mathcal{O}(t) \cdot r$ random bits. More efficient amplification procedures (see e.g. [Zuc96, Gol11]) allow us to achieve a similar probability bound using only $\mathcal{O}(t) + r$ random bits. This raises a natural question: could we obtain a "randomness-efficient" polarization procedure? Our Theorem 2 suggests that in a very efficient regime of parameters, the existence of such a procedure implies that SZK ⊆ SBP.

Corollary 1.2 (Informal)**.** *If there exists a randomness-efficient polarization, then* SZK ⊆ SBP*.*

Nonetheless, we believe that this result should be regarded as evidence that a "randomness-efficient" polarization may not be possible. Since while polarization is an inherently relativizable procedure, there exist an oracle that separates SZK from SBP (and, in fact, from PP. See [BCH+17]).

1.2 Ideas and Techniques

We show the collapse of AM to SBP by identifying complete sets of AM and SBP[1]. In [GS86], Goldwasser & Sipser considered the problem of determining whether a set S is of size at least m or at most $m/2$, where membership of x in S can be efficiently determined given a witness w. They show an AM protocol for the problem. Our first observation is that this problem is, in fact, hard for the class AM. In conclusion, we obtain a natural AM-complete problem - WSSE (see Definition 2.8 for more details). Next, we observe that the class SBP corresponds to a simpler version of the problem - SSE. As before, we would like to determine whether a set S is of size at least m or at most $m/2$. Yet, in this version of the problem, the membership of x can be efficiently determined given (just) x (see Definition 2.10 for more details).

In what follows, we show a polynomial-time reduction from WSSE to SSE. The natural approach would be to regard the set S as a set of tuples (x, w) such that w is a witness for membership of x in S. By definition, each $x \in S$ has at least one witness w associated with it. Yet, the actual number of such witnesses could be arbitrary. To illustrate this, consider the following two sets: S_1 contains

[1] Technically, we are looking at the promise versions of AM and SBP.

only one element x_1 with $K \gg 2$ witnesses of membership; S_2 contains two elements element e_1, e_2 with 1 witnesses of membership each. Suppose $m = 2$. Viewing S_1 and S_2 as above introduces order inversion between S_1 and S_2 as we will obtain sets with K and 2 elements, respectively. One approach to overcome this issue could be to actually count the number of witnesses. However this task turns out to be a #P-hard problem. We take a slightly different approach.

Rather than counting witnesses, we would like to ensure that each element x has only a "small" number of witnesses. For the sake of intuition, let us assume that SAT $\in$ UP. Fix x and consider the set W_x of witnesses associated with x. By definition, if $x \notin S$ then $W_x = \emptyset$; otherwise, if $x \in S$ then $|W_x| \geq 1$. Moreover, observe that the membership of w in W_x can be efficiently determined given (just) w. Will now run the unique-solution NP machine A on the predicate (formula) that corresponds to W_x. Observe that in the former case (i.e. $W_x = \emptyset$) A has zero accepting paths and in the latter case A has one exactly accepting path. In other words, every $x \in S$ will have a unique witness w of its membership in S. To handle the more general case of SAT $\notin \mathsf{SOLUTIONS}[2^{n^{1-\varepsilon}}]$ we "preprocess" the circuit by applying sequential repetition thus increasing the gap between number of witnesses in the "yes" and the "no" cases. See Lemma 3.1 for the formal proof.

In order to related SZK and SBP we study the relation between Statistical and the Collision Distances. See Lemma 2.4 for the formal proof.

1.3 Organization

We start by some basic definitions and notation in Section 2. In Section 3 we prove our main results. In fact, we prove somewhat more general and technical statements. Finally, we discuss some open questions in Section 4.

2 Preliminaries

For a unary relation $R(x)$, we define $\#_x R \triangleq |\{x \mid x \in R\}|$. For a binary relation $R(x, w)$, we define $\#_x \exists_w R \triangleq |\{x \mid \exists w \text{ s.t. } (x, w) \in R\}|$. For $k \in \mathbb{N}$, we define $R^{\otimes k}$ - the *tensor power of* R as

$$R^{\otimes k} \triangleq R(x_1, w_1) \wedge R(x_2, w_2) \wedge \ldots \wedge R(x_k, w_k)$$

where $x_1, \ldots, x_k$ and $w_1, \ldots w_k$ are k disjoint copies of x and w, respectively.

Observation 2.1. *Let* $\bar{x} = (x_1, \ldots, x_k)$ *and* $\bar{w} = (w_1, \ldots, w_k)$*. Then* $\#_{\bar{x}} \exists_{\bar{w}} R^{\otimes k} = (\#_x \exists_w R)^k$.

We will require the following technical lemma.

Lemma 2.2. *For any* $s > 1$ *and* $0 < \varepsilon < 1$ *it holds:*

1. $s^{-\varepsilon} \leq (s^{-1} - 1)\varepsilon + 1$.
2. $s^{\frac{1}{\varepsilon}} \geq 1 + \ln s \cdot \frac{1}{\varepsilon}$.

2.1 Probability Distributions and Circuits

Let X and Y be two random variables taking values in some finite domain $\mathcal{U}$.
We define the *support* of a random variable X as $\mathrm{Supp}(X) \triangleq \{a \in \mathcal{U} \mid \Pr[X = a] > 0\}$.

Definition 2.3 (Distances Between Distributions)**.** *The* Statistical Distance *between X and Y is defined as*

$$\Delta(X,Y) = \max_{\mathcal{U}' \subseteq \mathcal{U}} \Pr[X \in \mathcal{U}'] - \Pr[Y \in \mathcal{U}'].$$

The equality is attained for $\mathcal{U}' = \mathcal{U}_X \stackrel{\Delta}{=} \{a \in \mathcal{U} \mid \Pr[X = a] \geq \Pr[Y = a]\}$.
The Collision Distance *between X and Y is defined as* $\mathrm{Col}(X,Y) \stackrel{\Delta}{=} \Pr[X = Y]$.

We prove two properties relating the Statistical and the Collision Distances.

Lemma 2.4. *Let $k = |\mathrm{Supp}(X) \cup \mathrm{Supp}(Y)|$. Then $1/k \leq \Delta(X,Y) + \mathrm{Col}(X,Y) \leq 1$.*

Proof. Let $\mathcal{U}' = \mathrm{Supp}(X) \cup \mathrm{Supp}(Y)$, $\mathcal{U}_X = \{a \in \mathcal{U} \mid \Pr[X = a] \geq \Pr[Y = a]\}$ and $\mathcal{U}_Y = \mathcal{U}' \setminus \mathcal{U}_X$. For the first inequality:

$$\begin{aligned}
\mathrm{Col}(X,Y) = \sum_{a \in \mathcal{U}'} \Pr[X = a] \Pr[Y = a] = \sum_{a \in \mathcal{U}'} (\Pr[X = a])^2 - \sum_{a \in \mathcal{U}'} \Pr[X = a](\Pr[X = a] - \Pr[Y = a]) \geq \\
\geq \frac{\left(\sum_{a \in \mathcal{U}'} \Pr[X = a]\right)^2}{|\mathcal{U}'|} - \sum_{a \in \mathcal{U}_X} \Pr[X = a](\Pr[X = a] - \Pr[Y = a]) \geq \\
\geq \frac{1}{|\mathcal{U}'|} - \sum_{a \in \mathcal{U}_X} (\Pr[X = a] - \Pr[Y = a]) = \frac{1}{|\mathcal{U}'|} - \Delta(X,Y).
\end{aligned}$$

We now move to the second inequality.

$$\begin{gathered}
\mathrm{Col}(X,Y) + \Delta(X,Y) - 1 = \sum_{a \in \mathcal{U}'} \Pr[X = a] \Pr[Y = a] + \sum_{a \in \mathcal{U}_X} \Pr[X = a] - \Pr[Y = a] - 1 \leq \\
\Pr[X \in \mathcal{U}_X] \Pr[Y \in \mathcal{U}_X] + \Pr[X \in \mathcal{U}_Y] \Pr[Y \in \mathcal{U}_Y] + \Pr[X \in \mathcal{U}_X] - \Pr[Y \in \mathcal{U}_X] - 1 = \\
= (\Pr[X \in \mathcal{U}_X] - 1)(\Pr[Y \in \mathcal{U}_X] + 1) + (1 - \Pr[X \in \mathcal{U}_X])(1 - \Pr[Y \in \mathcal{U}_X]) = \\
= 2(\Pr[X \in \mathcal{U}_X] - 1) \Pr[Y \in \mathcal{U}_X] \leq 0.
\end{gathered}$$

Observe that $\Pr[X \in \mathcal{U}_Y] = 1 - \Pr[X \in \mathcal{U}_X]$ and $\Pr[Y \in \mathcal{U}_Y] = 1 - \Pr[Y \in \mathcal{U}_X]$. □

We complement our result by observing that for a pair of variables X and Y with disjoint supports it holds that: $\Delta(X,Y) = 1$ and $\mathrm{Col}(X,Y) = 0$, and hence $\Delta(X,Y) + \mathrm{Col}(X,Y) = 1$. In addition, for any $n \geq 1$ and $\varepsilon \geq 0$, consider a random variable X over $\{0,1\}^n$ defined as follows: For $\bar{a} \in \{0,1\}^n$:

$$\begin{array}{ll}
\Pr[X = \bar{a}] = \frac{1+\varepsilon}{2^n} & \text{if } a_n = 0 \\
\Pr[X = \bar{a}] = \frac{1-\varepsilon}{2^n} & \text{otherwise.}
\end{array}$$

Observe that $k = 2^n$, $\Delta(X, \bar{1} - X) = \varepsilon$ and $\mathrm{Col}(X, \bar{1} - X) = \frac{1-\varepsilon^2}{k}$.

A Boolean circuit $C : \{0,1\}^n \to \{0,1\}^m$ induces a probability distribution on $\{0,1\}^m$ by evaluating C on a uniformly chosen input in $\{0,1\}^n$. For two Boolean circuits, C_1 and C_2, we will use the notations $\Delta(C_1, C_2)$ and $\mathrm{Col}(C_1, C_2)$ to denote the corresponding distances between the induced distributions.

2.2 Complexity Classes and Promise Problems

We will be mostly concerned with the two following complexity classes. We refer the reader to [AB09] for the definitions of other standard complexity classes.

Definition 2.5 ([Bab85])**.** *A language L is in* AM *if there exists a polynomial-time computable predicate $A(x, r, w)$ such that:*

$$\begin{aligned} x \in L &\implies \Pr_r[\exists w : A(x, r, w) = 1] \geq 2/3 \\ x \notin L &\implies \Pr_r[\exists w : A(x, r, w) = 1] \leq 1/3. \end{aligned}$$

Definition 2.6 ([BGM06])**.** *A language L is in* SBP *if there exists $\varepsilon > 0, k \in \mathbb{N}$ and a polynomial-time computable predicate $B(x, r)$ such that:*

$$\begin{aligned} x \in L &\implies \Pr_r[B(x, r)) = 1] \geq (1 + \varepsilon) \cdot \tfrac{1}{2^{n^k}} \\ x \notin L &\implies \Pr_r[B(x, r)) = 1] \leq (1 - \varepsilon) \cdot \tfrac{1}{2^{n^k}}. \end{aligned}$$

where $n = |x|$.

For technical reasons we will need to consider promise problems. A *promise problem* is a relaxation of a language. Formally:

Definition 2.7 (Promise Problems)**.** $\Pi = (\Pi_{YES}, \Pi_{NO})$ *is a* promise problem *if* $\Pi_{YES} \cap \Pi_{NO} = \emptyset$*.*

In [GS86], Goldwasser & Sipser consider the problem of determining whether a set S is of size at least m or at most $m/2$, where membership of x can be efficiently determined given x and witness w. Formally, we define the following promise problem.

Definition 2.8 (Witnessed Set-Size Estimation)**.** $\text{WSSE} \triangleq (\text{WSSE}_{YES}, \text{WSSE}_{NO})$ *where,*
$\text{WSSE}_{YES} = \{(C, m) \mid \#_x \exists_w C \geq m\}, \text{WSSE}_{NO} = \{(C, m) \mid \#_x \exists_w C \leq m/2\}$*.*
Here $C(x, w)$ is a Boolean circuit and m is an integer given in binary representation.

In the same paper, an AM protocol for the problem was given. In other words, it was shown that $\text{WSSE} \in \mathsf{PromiseAM}$. We begin by observing that WSSE is also hard for the class AM. Recall Definition 2.5. Let $L \in \mathsf{AM}$ and suppose $r \in \{0, 1\}^\ell$. Furthermore, set $A_x(r, w) \triangleq A(x, r, w)$ and $m = 2^{\ell+1}/3$. We observe that:

$$\begin{aligned} x \in L &\implies \#_r \exists_w A_x \geq m \\ x \notin L &\implies \#_r \exists_w A_x \leq m/2. \end{aligned}$$

Corollary 2.9. WSSE *is* $\mathsf{PromiseAM}$*-complete.*

In this paper, we also study a simpler version of the problem. As before, we would like to determine whether a set S is of size at least m or at most $m/2$. Yet, in this version of the problem, the membership of x can be efficiently determined given (just) x. Formally, we define the following promise problem.

Definition 2.10 (Set-Size Estimation)**.** $\text{SSE} \triangleq (\text{SSE}_{YES}, \text{SSE}_{NO})$ *where,*
$\text{SSE}_{YES} = \{(C, m) \mid \#_x C \geq m\}, \text{SSE}_{NO} = \{(C, m) \mid \#_x C \leq m/2\}$*.*
Here $C(x)$ is a Boolean circuit and m is an integer given in binary representation.

Lemma 2.11 (Implicit in [BGM06])**.** SSE *is* $\mathsf{PromiseSBP}$*-complete.*

Indeed, SSE and WSSE capture the complexity classes SBP and AM, respectively. Indeed, AM corresponds to the class of all languages that reduce to WSSE. Likewise, SBP is the class of all languages that reduce to SSE. We now define the class SZK in a similar fashion.

Definition 2.12 (Statistical Difference - [SV03])**.** *Let $\alpha(n) : \mathbb{N} \to \mathbb{N}$ and $\beta(n) : \mathbb{N} \to \mathbb{N}$ be computable functions, such that $\alpha(n) > \beta(n)$.*
Then $\mathrm{SD}^{(\alpha(n)\,,\,\beta(n))} \triangleq (\mathrm{SD}_{YES}^{(\alpha(n)\,,\,\beta(n))}, \mathrm{SD}_{NO}^{(\alpha(n)\,,\,\beta(n))})$ where,
$\mathrm{SD}_{YES}^{(\alpha(n)\,,\,\beta(n))} = \{(C_1, C_2) \mid \Delta(C_1, C_2) \geq \alpha(n)\}, \mathrm{SD}_{NO}^{(\alpha(n)\,,\,\beta(n))} = \{(C_1, C_2) \mid \Delta(C_1, C_2) \leq \beta(n)\}$.

Here, C_1 and C_2 are Boolean circuits $C_1, C_2 : \{0,1\}^n \to \{0,1\}^m$ of size $\mathrm{poly}(n)$.

Definition 2.13 (Statistical Zero Knowledge)**.** *SZK is defined as class of all languages that reduce to $\mathrm{SD}^{(2/3\,,\,1/3)}$.*

We remark that originally SZK was defined in by Goldwasser et al. in [GMR89] as the class of decision problems for which a "yes" answer can be verified by a statistical zero-knowledge proof protocol. The alternate characterization via the complete problem was given in [SV03].

In order the explore the relation between SZK and SBP further, we define a sparse version of the Statistical Difference problem.

Definition 2.14 (Sparse Statistical Difference)**.** *For a computable function $t(n) : \mathbb{N} \to \mathbb{N}$, $t(n)$-$\mathrm{SSD}^{(\alpha(n)\,,\,\beta(n))}$ is a specialization of SD to the case where the support size of distributions induced by C_1 and C_2 is bounded by $t(n)$. Formally: $|\mathrm{Supp}(C_1)|, |\mathrm{Supp}(C_2)| \leq t(n)$.*

2.3 $\mathsf{SOLUTIONS}[f(n)]$

In this section we formally define the class $\mathsf{SOLUTIONS}[f(n)]$ and discuss some of its properties. Indeed, $\mathsf{SOLUTIONS}[f(n)]$ constitutes a subclass of NP with a bounded number of solutions.

Definition 2.15. *Let $f : \mathbb{N} \to \mathbb{N}$ be a computable function. We say that a language L in the class $\mathsf{SOLUTIONS}[f(n)]$, if there exists a polynomial-time computable predicate $A(x, y)$ such that:*

$$\begin{aligned} x \in L &\implies 1 \leq \#_y A_x \leq f(|x|) \\ x \notin L &\implies \#_y A_x = 0. \end{aligned}$$

where $A_x(y) = A(x, y)$.

In other words, $\mathsf{SOLUTIONS}[f(n)]$ is special case of NP where for each $x \in L$ there are at most $f(n)$ witnesses. Observe that: $\mathsf{UP} = \mathsf{SOLUTIONS}[1] \subseteq \mathsf{FewP} = \mathsf{SOLUTIONS}[\mathrm{poly}(n)] \subseteq \mathsf{NP}$.

Remark: We note the definition would not change if we relaxed the requirement "to have of at most $f(n)$ solutions" to hold only for sufficiently large values of n. Next, we would like to point out a property of the $\mathsf{SOLUTIONS}[f(n)]$ in a sub-exponential regime of parameters.

Observation 2.16. *Suppose there exists $\varepsilon > 0$ such that $L \in 2^{n^{1-\varepsilon}}$. Then there exists $\varepsilon' > 0$ and an NP machine that decides instances of size $n^{1+\varepsilon}$ of L with at most $2^{n^{1-\varepsilon'}}$ solutions.*

Proof. For instances of size $n^{1+\varepsilon}$, the number of solutions be at most $2^{(n^{1+\varepsilon})^{1-\varepsilon}} = 2^{n^{1-\varepsilon^2}}$. □

We conclude this section by presenting two facts about transforming Turing machine into Boolean circuits and Boolean circuits into Boolean formulas.

Fact 2.17. *There exists a polynomial-time algorithm that given a Turing machine M that computes a Boolean predicate $A(z)$ in time $t(|z|)$, and input length n, outputs a Boolean circuit C of size $\mathrm{poly}(t(n))$ on n inputs such that $C(z) = A(z)$ for every $z \in \{0,1\}^n$.*

Fact 2.18. *There exists a polynomial-time algorithm that given a Boolean circuit C of size s transforms it into a 3-CNF formula φ of size $\mathcal{O}(s)$ such that φ is satisfiable iff C is satisfiable.*

Combined with Observation 2.16, we obtain that wlog we can use various notions of size (i.e. number of gates in the circuit, number of clauses in a formula, bit-size complexity, etc..) interchangeably as they are with poly-log factor from each other and $s \cdot \mathrm{polylog}(s) = o(s^{1+\varepsilon})$ for any $\varepsilon > 0$.

Corollary 2.19. *There exists $\varepsilon > 0$ such that* CKT-SAT $\in \mathsf{SOLUTIONS}[2^{n^{1-\varepsilon}}]$ *iff there exists $\varepsilon' > 0$ such that* 3-SAT $\in \mathsf{SOLUTIONS}[2^{n^{1-\varepsilon'}}]$.

3 Proofs of the Main Results

In this section we prove our main results Theorems 1 and 2. In fact, we prove somewhat more general and technical results.

Lemma 3.1. *Suppose there exists $\varepsilon > 0$ such that* CKT-SAT $\in \mathsf{SOLUTIONS}[2^{n^{1-\varepsilon}}]$. *Then* $\mathsf{PromiseAM} = \mathsf{PromiseSBP}$.

Proof. We show that $\mathsf{PromiseAM} \subseteq \mathsf{PromiseSBP}$ by showing that WSSE $\leq_p$ SSE. In particular, let $C(x, w)$ be a circuit of size s. We map an instance $(C(x,w), m)$ of WSSE to $\left(\hat{C}(\bar{x}, y), m^k\right)$, where $\hat{C}(\bar{x}, y)$ is a circuit of size $\mathrm{poly}(sk)$, for $k = s^{\frac{1}{\varepsilon}}$.

Let $A(C', y)$ be a polynomial-time computable predicate that given a Boolean circuit $C'(z)$ of size s satisfies:

$$\begin{array}{lll} \#_z C' \geq 1 & \implies & 1 \leq \#_y A_{C'} \leq 2^{s^{1-\varepsilon}} \\ \#_z C' = 0 & \implies & \#_y A_{C'} = 0. \end{array}$$

where $A_{C'}(y) = A(C', y)$. Consider the following Boolean predicate $\hat{A}(\bar{x}, y)$, where $\bar{x} = (x_1, \ldots, x_k)$:

```
$C'_{\bar{x}}(\bar{w}) \leftarrow C^{\otimes k}(\bar{x}, \bar{w})$; /* Taking $k$-th tensor power of the circuit $C(x,w)$ and
    plugging in the value of $\bar{x}$.  Here $\bar{w} = (w_1, \ldots, w_k)$.                       */
return $A(C', y)$
```

Let $\hat{C}(\bar{x}, y)$ denote the circuit that results from converting $\hat{A}(\bar{x}, y)$ into a Boolean circuit (applying Fact 2.17). The claim about the runtime is clear. We now analyze the reduction.

- Suppose that $\#_x \exists_w C \geq m$. By Observation 2.1: $\#_{\bar{x}} \exists_{\bar{w}} C^{\otimes k} \geq m^k$. In other words, there exist at least m^k different inputs $\bar{x}$ for which $\#_{\bar{w}} C'_{\bar{x}} \geq 1$. By the properties of A, for each such $\bar{x}$ there exists y such that $\hat{C}(\bar{x}, y) = 1$. Therefore, $\#_{(\bar{x},y)} \hat{C} \geq m^k$.

- Suppose that $\#_x \exists_w C \leq m/2$. By Observation 2.1: $\#_{\bar{x}} \exists_{\bar{w}} C^{\otimes k} \leq (m/2)^k$. In other words, there exist at most $(m/2)^k$ different inputs $\bar{x}$ for which $\#_{\bar{w}} C'_{\bar{x}} \geq 1$. Since $C'_{\bar{x}}$ is a circuit of size at most sk, by the properties of A, for each such $\bar{x}$ there exists at most $2^{(sk)^{1-\varepsilon}}$ witnesses y such that $\hat{C}(\bar{x}, y) = 1$. Therefore, $\#_{(\bar{x},y)} \hat{C} \leq (m/2)^k \cdot 2^{(sk)^{1-\varepsilon}} \leq m^k/2$. To justify the last inequality, assume wlog that $s > 4$ and recall Lemma 2.2:

$$(sk)^{1-\varepsilon} - k = s^{(1+\frac{1}{\varepsilon})(1-\varepsilon)} - s^{\frac{1}{\varepsilon}} = s^{\frac{1}{\varepsilon}-\varepsilon} - s^{\frac{1}{\varepsilon}} \le s^{\frac{1}{\varepsilon}}[(s^{-1}-1)\varepsilon + 1 - 1] =$$
$$= s^{\frac{1}{\varepsilon}}(s^{-1}-1)\varepsilon \le (1 + \ln s \cdot \frac{1}{\varepsilon})(s^{-1}-1)\varepsilon \le (\varepsilon + \ln s)(s^{-1}-1) < -1$$

□

Theorem 1 follows from the lemma combined with Corollary 2.19

Lemma 3.2. *Let $\beta(n)$ and $t(n)$ be such that $\beta(n) \cdot t(n) \le 1/6$. Then $\overline{t(n)\text{-SSD}}^{(1-\beta(n)\ ,\ \beta(n))} \in$ PromiseSBP.*

Proof. Given two circuits $C_1, C_2 : \{0,1\}^n \to \{0,1\}^m$, the algorithm will try to find a collision. Namely, pick $x, x' \in \{0,1\}^n$ uniformly at randomly and accept iff $C_1(x) = C_2(x')$. Observe that the success probably of the algorithm is exactly $\mathrm{Col}(C_1, C_2)$. We now analyze this probability.

- Suppose $\Delta(C_1, C_2) \le \beta(n)$. Observe that $|\mathrm{Supp}(C_1) \cup \mathrm{Supp}(C_2)| \le 2t(n)$. Therefore, by Lemma 2.4, $\mathrm{Col}(C_1, C_2) \ge \frac{1}{2t(n)} - \beta(n) \ge 3\beta(n) - \beta(n) = 2\beta(n)$.
- Suppose $\Delta(C_1, C_2) \ge 1 - \beta(n)$. By Lemma 2.4, $\mathrm{Col}(C_1, C_2) \le \beta(n)$.

□

Theorem 2 follows by observing that for circuits defined over n bits we have:
$|\mathrm{Supp}(C_1)|, |\mathrm{Supp}(C_2)| \le 2^n$, and instantiating the lemma to $t(n) = 2^n$ and $\beta(n) = \frac{1}{2^{n+3}}$.

4 Discussion & Open Question

The major widely-believed derandomization assumption of [KvM02] that implies the collapse of AM and MA to NP is that some language in NE ∩ coNE requires SAT-oracle circuits of size $2^{\Omega(n)}$. Later in [MV05], the assumption of SAT-oracle circuits was relaxed to nondeterministic circuits. Can one prove that the premises of Theorem 1 are implies by a weaker assumption? For example, the assumption of [KvM02, MV05] that some language in E requires SAT-oracle circuits of size $2^{\Omega(n)}$ implies a deterministic version of the argument of [GS86]. Could one utilize this connection?

Another natural question is to identify a corresponding MA-complete problem in the flavor of WSSE for AM and SSE for SBP. Could the presented collapse, then, be extended to MA? Conversely, could one show that any collapse either AM, SBP or MA to a subclass implies the premises of Theorem 1? Perhaps under an even stronger assumption that NP ⊆ P/poly?

Finally, we note that setting $\beta(n) = 0$ in the statement of Lemma 3.2, will recover the class $\overline{\text{SD}}^{(1\ ,\ 0)}$. Could we identify a natural problem that reduces to $\overline{t(n)\text{-SSD}}^{(1-\beta(n)\ ,\ \beta(n))}$ that does not reduce to $\overline{\text{SD}}^{(1\ ,\ 0)}$ (with $\beta(n) \cdot t(n) \le 1/6$)? Such a problem will attest the non-triviality of the SSD problem.

Acknowledgment

The author would like to extend his gratitude to Thomas Watson and Ryan Williams for useful conversations. Finally, the author would like to thank the anonymous referees for their detailed comments and suggestions.

References

[AB09] S. Arora and B. Barak. *Computational complexity: a modern approach.* Cambridge University Press, 2009.

[AKSS95] V. Arvind, J. Köbler, U. Schöning, and R. Schuler. If NP has polynomial-size circuits, then ma=am. *Theor. Comput. Sci.*, 137(2):279–282, 1995.

[All86] E. Allender. The complexity of sparse sets in P. In *Structure in Complexity Theory*, pages 1–11, 1986.

[Bab85] L. Babai. Trading group theory for randomness. In *Proceedings of the 17th Annual ACM Symposium on Theory of Computing (STOC)*, pages 421–429, 1985.

[BCH$^+$17] A. Bouland, L. Chen, D. Holden, J. Thaler, and P. Vasudevan. On the power of statistical zero knowledge. In *58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017*, pages 708–719, 2017.

[BGM06] E. Böhler, C. Glaßer, and D. Meister. Error-bounded probabilistic computations between MA and AM. *J. Comput. Syst. Sci.*, 72(6):1043–1076, 2006.

[For89] L. Fortnow. The complexity of perfect zero-knowledge. *Advances in Computing Research*, 5:327–343, 1989.

[GLM$^+$16] M. Göös, Sh. Lovett, R. Meka, T. Watson, and D. Zuckerman. Rectangles are nonnegative juntas. *SIAM J. Comput.*, 45(5):1835–1869, 2016.

[GMR89] Sh. Goldwasser, S. Micali, and Ch. Rackoff. The knowledge complexity of interactive proof systems. *SIAM J. Comput.*, 18(1):186–208, 1989.

[Gol11] O. Goldreich. A sample of samplers: A computational perspective on sampling. In *Studies in Complexity and Cryptography. Miscellanea on the Interplay between Randomness and Computation*, pages 302–332. 2011.

[GS86] S. Goldwasser and M. Sipser. Private coins versus public coins in interactive proof systems. In *Proceedings of the 18th Annual ACM Symposium on Theory of Computing (STOC)*, pages 59–68, 1986.

[KL80] R. M. Karp and R. J. Lipton. Some connections between nonuniform and uniform complexity classes. In *Proceedings of the 12th Annual ACM Symposium on Theory of Computing, April 28-30, 1980, Los Angeles, California, USA*, pages 302–309, 1980.

[KMS15] B. M. Kapron, L. Malka, and V. Srinivasan. A framework for non-interactive instance-dependent commitment schemes (NIC). *Theor. Comput. Sci.*, 593:1–15, 2015.

[KvM02] Adam Klivans and Dieter van Melkebeek. Graph nonisomorphism has subexponential size proofs unless the polynomial-time hierarchy collapses. *SIAM J. Comput.*, 31(5):1501–1526, 2002.

[Mor82] Sh. Moran. On the accepting density hierarchy in NP. *SIAM J. Comput.*, 11(2):344–349, 1982.

[MV05] P. B. Miltersen and N. V. Vinodchandran. Derandomizing arthur-merlin games using hitting sets. *Computational Complexity*, 14(3):256–279, 2005.

[Oka00] T. Okamoto. On relationships between statistical zero-knowledge proofs. *J. Comput. Syst. Sci.*, 60(1):47–108, 2000.

[Rub88] R. Rubinstein. *Structural Complexity Classes of Sparse Sets: Intractability, Data Compression, and Printability.* Ph.D. thesis, Northeastern University, Department of computer Science, 1988.

[SV03] A. Sahai and S. P. Vadhan. A complete problem for statistical zero knowledge. *J. ACM*, 50(2):196–249, 2003.

[Val76] L. G. Valiant. Relative complexity of checking and evaluating. *Inf. Process. Lett.*, 5(1):20–23, 1976.

[Ver92] N. K. Vereshchagin. On the power of PP. In *Proceedings of the Seventh Annual Structure in Complexity Theory Conference*, pages 138–143, 1992.

[VV86] L. G. Valiant and V. V. Vazirani. NP is as easy as detecting unique solutions. *Theor. Comput. Sci.*, 47(3):85–93, 1986.

[Wat16] T. Watson. The complexity of estimating min-entropy. *Computational Complexity*, 25(1):153–175, 2016.

[Zuc96] D. Zuckerman. Simulating BPP using a general weak random source. *Algorithmica*, 16(4/5):367–391, 1996.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il