Electronic Colloquium on Computational Complexity, Report No. 30 (2001)

$S_2^p \subseteq ZPP^{NP}$

Jin-Yi Cai *

Abstract

We show that the class S_2^p is a subclass of ZPP^{NP}. The proof uses universal hashing, approximate counting and witness sampling. As a consequence, a collapse first noticed by Samik Sengupta that the assumption NP has small circuits collapses PH to S_2^p becomes the strongest version to date of the Karp-Lipton Theorem.

1 Introduction

The class S_2^p was introduced independently by Canetti [C96] and Russell and Sundaram [RS95] in the mid 1990's. Suppose there are two competing all powerful provers Y and Z. A string x is given, Y wishes to convince us that $x \in L$, and Z wishes to convince us the opposite $x \notin L$. We—the verifier—have only deterministic polynomial time computing power. A language L is in S_2^p iff there is a P-time predicate P such that the following holds:

> If $x \in L$ then there exists a y, such that for all z, $P(x, y, z)$ holds;
> If $x \notin L$ then there exists a z, such that for all y, $\neg P(x, y, z)$ holds, where both y and z are polynomially bounded in length of x.

In other words, if $x \in L$ then Y has irrefutable proof y which can withstand any challenge z from Z; and if $x \notin L$ then Z has irrefutable proof z which can withstand any challenge y from Y.

The motivation by both Canetti [C96] and Russell and Sundaram [RS95] was to provide a refinement of the Sipser-Lautemann Theorem that $BPP \subseteq \Sigma_2^p \cap \Pi_2^p$ [Si83, L83]. Indeed, Canetti [C96] extended Lautemann's proof to show that $BPP \subseteq S_2^p$, whereas Russell and Sundaram [RS95] showed further that $MA \subseteq S_2^p$. Note that $BPP \subseteq MA$ is trivial by definition, thus $MA \subseteq S_2^p$ implies $BPP \subseteq S_2^p$.

As to upper bound of S_2^p, the only known containment is by definition $S_2^p \subseteq \Sigma_2^p \cap \Pi_2^p$ (see Section 2). Goldreich and Zuckerman [GZ97] surveyed a number of interesting results for classes between P and the second level of the Polynomial-time Hierarchy Σ_2^p and Π_2^p. These classes include $ZPP, RP, BPP, NP, P^{NP}, MA, AM, ZPP^{NP}$ and S_2^p. They called the classes listed here upto P^{NP} "Traditional classes—classes of the 1970's", the class Arthur-Merlin

*Computer Sciences Department, University of Wisconsin, Madison, WI 53706, and Department of Computer Science and Engineering, State University of New York at Buffalo, Buffalo, NY 14260. Research supported in part by NSF CCR9820806 and a Guggenheim Fellowship. Email: jyc@cs.wisc.edu

ISSN 1433-8092

"a class of the 1980's", and the class S_2^p "a class of the 1990's", underscoring that not much is yet known about this class S_2^p. In their paper [GZ97] Goldreich and Zuckerman gave a number of elegant proofs of known results with the strikingly sharp amplification technique due to Zuckerman [Z96]. They also prove an interesting result MA $\subseteq$ ZPP$^{\rm NP}$. This last result was new in 1997 when [GZ97] appeared; it was independently obtained by Arvind and Köbler [AK97]. In the final diagram summarizing the known facts about all these classes between P and Σ_2^p and Π_2^p, Goldreich and Zuckerman used the letter X to stand for both S_2^p and ZPP$^{\rm NP}$, as they share all the known containment properties both below and above. They further state that it is unknown how these two classes are related.

The main result of this paper is

Theorem 1 $S_2^p \subseteq$ ZPP$^{\rm NP}$.

The proof uses universal hashing, approximate counting and witness sampling.

There is an interesting consequence of this result with respect to the well known Karp-Lipton Theorem concerning sparse sets (with contribution by Sipser) [KL80]. This theorem says, if NP is Cook-reducible ($\leq_T^p$) to sparse sets, or equivalently, if **SAT** has polynomial size circuits, then the Polynomial-time Hierarchy collapses to its second level: PH $= \Sigma_2^p \cap \Pi_2^p$. Many researchers have since tried to improve on this signature theorem—To simplify the proof and to strengthen the collapse. On the one hand, there emerged what I consider to be the "book" proof (as Erdös would say) of the theorem (As far as I know John Hopcroft [H81] was the first to give essentially this proof):

> To simulate Π_2^p by Σ_2^p, guess a poly-size circuit C for **SAT**, modify C via self-reducibility so that whenever $C(\phi) = 1$ it also produces a satisfying assignment to ϕ, then check all universal paths of the Π_2^p computation lead to a satisfiable formula.

Samik Sengupta [Se00] first noticed that this "book" proof actually gave the collapse to S_2^p ! (See Section 5.)

While the proof of Karp-Lipton Theorem becomes extremely transparent, more research effort went into trying to extend this beautiful result. Much work was done on the general theme (we mention some in Section 5). Over the years there have been steady improvements on the exact level of collapse of PH, assuming **SAT** has small circuits. In this regard, the best result so far is due to Bshouty et. al. [BCGKT94] and Köbler and Watanabe [KW95]. Their result states that if NP has polynomial size circuits, then the Polynomial-time Hierarchy collapses to ZPP$^{\rm NP}$. Admittedly the proofs of the theorem of Bshouty et. al. and Köbler-Watanabe are more involved than the "book" proof of the basic version of the Karp-Lipton Theorem and depend on previous interesting results by Jerrum, Valiant and V. Vazirani [JVV86] and others.

By the new theorem $S_2^p \subseteq$ ZPP$^{\rm NP}$ (unconditionally), the (currently) strongest Karp-Lipton Theorem becomes

Theorem 2 (Sengupta) *If* **SAT** *has polynomial size circuits, then the Polynomial-time Hierarchy collapses to* S_2^p.

We observe that while this becomes the strongest collapse for the Karp-Lipton Theorem, its proof reverts back to the simple "book" proof.

Theorem 1 also subsumes the result MA $\subseteq$ ZPP$^{\mathrm{NP}}$ by Goldreich-Zuckerman [GZ97] and Arvind-Köbler [AK97], as we know from Russell and Sundaram [RS95] that MA $\subseteq \mathrm{S}_2^p$.

2 Preliminaries

The class S_2^p was defined by Russell and Sundaram [RS95] as follows: $L \in \mathrm{S}_2^p$ iff there is a P-time computable 0-1 function P on three arguments, such that

$$\begin{aligned} x \in L &\implies (\exists^p y)(\forall^p z)[P(x,y,z) = 1] \\ x \notin L &\implies (\exists^p z)(\forall^p y)[P(x,y,z) = 0] \end{aligned}$$

where as usual "$\exists^p y$" stands for "$\exists y \in \{0,1\}^{p(|x|)}$" for some polynomial $p(\cdot)$. Similarly "$\forall^p z$" stands for "$\forall z \in \{0,1\}^{q(|x|)}$" for some polynomial $q(\cdot)$. By padding we can suitably extend the length of both y and z, and henceforth we can assume they both vary over the same length n which is a power of 2, and n is polynomially bounded in the length of x.

Given x, for convenience, for a pair (y,z) we say y beats z if $P(x,y,z) = 1$, and z beats y if $P(x,y,z) = 0$.

It is immediately clear that both implications "$\implies$" can be replaced by the if and only if relation "$\iff$" without changing the class S_2^p. For instance, suppose $(\exists^p y)(\forall^p z)[P(x,y,z) = 1]$, let y_0 be such a y. Then certainly $x \in L$, else we would have a z_0 such that $(\forall^p y)[P(x,y,z_0) = 0]$, which is clearly a contradiction to $P(x,y_0,z_0) = 1$. Similarly $(\exists^p z)(\forall^p y)[P(x,y,z) = 0]$ implies $x \notin L$. Thus

$$\begin{aligned} x \in L &\iff (\exists^p y)(\forall^p z)[P(x,y,z) = 1] \\ x \notin L &\iff (\exists^p z)(\forall^p y)[P(x,y,z) = 0] \end{aligned}$$

It follows from this if and only if condition that $\mathrm{S}_2^p \subseteq \Sigma_2^p \cap \Pi_2^p$. In fact S_2^p consists of precisely those languages in $\Sigma_2^p \cap \Pi_2^p$ where membership in both Σ_2^p and Π_2^p are demonstrated by a single predicate P.

Canetti [C96] defined the class S_2^p as follows: $L \in \mathrm{S}_2^p$ iff there is a P-time computable 0-1 function P on three arguments, such that for all x,

$$(\exists^p y)(\forall^p z)[P(x,y,z) = \chi_L(x)]$$

and

$$(\exists^p z)(\forall^p y)[P(x,y,z) = \chi_L(x)],$$

where χ_L is the characteristic function of L.

Clearly the Canetti definition implies the Russell-Sundaram definition. The reverse implication also holds. For completeness we sketch a simple proof (see [RS95, C96] for more details.) Suppose a predicate P is given in the Russell-Sundaram definition. We define an

extended predicate $\hat{P}$ to satisfy the Canetti definition. For x, suppose y and z vary over $\{0,1\}^n$. Then $\hat{P}$ is defined over $\{0,1\}^{|x|} \times \{0,1\}^{n+1} \times \{0,1\}^{n+1}$:

$$\begin{aligned}
\hat{P}(x, 1y, 1z) &= 1 \\
\hat{P}(x, 1y, 0z) &= P(x, y, z) \\
\hat{P}(x, 0y, 1z) &= P(x, z, y) \\
\hat{P}(x, 0y, 0z) &= 0
\end{aligned}$$

Intuitively in the Canetti set up both provers are expected to prove the right assertion whether or not $x \in L$.

ZPP denotes zero-error probabilistic polynomial time. $\mathrm{ZPP}^{\mathrm{NP}}$ is the class accepted by zero-error probabilistic polynomial time oracle Turing machines using an NP oracle. By Cook's Theorem, we can assume without loss of generality that this oracle is the set of satisfiable boolean formulae **SAT**.

3 $\mathrm{S}_2^p \subseteq \mathrm{ZPP}^{\mathrm{NP}}$

To prove the main Theorem 1, we proceed as follows. Let x be given. Let $\{0,1\}^n$ be the witness sets for both provers Y and Z. Here n is polynomially bounded by $|x|$, and is a power of 2.

We will grow a list $Y_k \subset \{0,1\}^n$ of y's, where $|Y_k| = k$, and $k = 1, 2, \ldots, n^{O(1)}$; initially the list Y_1 can be arbitrary given, for example $Y_1 = \{0^n\}$. In the k-th stage, with Y_k in hand, we ask the **SAT** oracle whether there exists a $z \in \{0,1\}^n$ such that $P(x, y, z) = 0$ for every $y \in Y_k$, i.e., a z that beats every $y \in Y_k$. Since $|Y_k| = k$ is polynomially bounded, this is clearly a **SAT** query by Cook's Theorem. If the answer is No, we can already conclude that $x \in L$ and halt. Even though we may not have found a witness y_0 which beats every z as promised in the definition when $x \in L$, we *can* conclude that $x \in L$, since otherwise $x \notin L$ would have guaranteed a z_0 which beats *all* y, which certainly include all $y \in Y_k$.

Hence let's assume the answer to the **SAT** query is Yes, then we can use self-reducibility to obtain from the **SAT** oracle one such z. Then we can ask if there is another such z which beats all $y \in Y_k$.

Let

$$Z(Y_k) = \{z \in \{0,1\}^n \mid (\forall y \in Y_k)[P(x, y, z) = 0]\}.$$

There are two cases. Either $|Z(Y_k)| \leq n^2$ or $|Z(Y_k)| > n^2$. In the first case we can find out this is so in no more than $n^2 + 1$ steps querying the **SAT** oracle, and obtain the complete list $z_1, z_2, \ldots, z_\ell$, where $\ell \leq n^2$. Then we will ask the **SAT** oracle sequentially for each $i = 1, \ldots, \ell$, whether $(\forall y \in \{0,1\}^n)[P(x, y, z_i) = 0]$, i.e. if this z_i is a promised witness that beats all y when $x \notin L$. If for some $1 \leq i \leq \ell$, we get an answer that this z_i beats all y then we reject x and halt. If for all $1 \leq i \leq \ell$, we get an answer that this z_i does not beat all y, we claim that $x \in L$, and we should accept x and halt. This is because, had it been $x \notin L$, then some z_0 which beats all $y \in \{0,1\}^n$ certainly belong to $Z(Y_k)$, and would have been among the complete list $z_1, z_2, \ldots, z_\ell$. Thus we accept x in this case correctly, even though we may not have found the promised witness y which beats all z.

Now we assume the "general case" where we found that $|Z(Y_k)| > n^2$. So far we have not used any probabilistic moves. It is here we will use random coins. Our goal is to find a new y^* to be appended to the list Y_k so that the corresponding $Z(Y_{k+1})$ is shrunk significantly. Let $Y_{k+1} = Y_k \cup \{y^*\}$, then we wish to guarantee that $|Z(Y_{k+1})| \leq |Z(Y_k)|/2$ with high probability. If so, we would guarantee that the size $|Z(Y_k)|$ shrinks geometrically every step by a constant fraction with high probability, and thus in polynomial time we end up in the case with $|Z(Y_k)| \leq n^2$.

Lemma 1 *For every set S in* P*, there is a probabilistic polynomial time sampling procedure A using a* **SAT** *oracle, such that for every n, $A(1^n)$ samples at most $n^{O(1)}$ elements $S' \subseteq S^{=n} = S \cap \{0,1\}^n$ in such a way that, for every subset $T \subseteq S^{=n}$, with $|T| > |S^{=n}|/2$,*

$$\Pr[S' \cap T = \emptyset] \leq \frac{1}{2^{2n}}.$$

We will give a proof of Lemma 1 in the next section.

For any witness $y' \in \{0,1\}^n$, consider the set

$$T_{y'} := Z(Y_k \cup \{y'\}) = \{z \in \{0,1\}^n \mid (\forall y \in Y_k)[P(x,y,z) = 0] \wedge [P(x,y',z) = 0]\}.$$

We say a $y' \in \{0,1\}^n$ is a "bad witness" with respect to $Z(Y_k)$ if

$$|\{z \in Z(Y_k) \mid P(x,y',z) = 1\}| < \frac{|Z(Y_k)|}{2}.$$

That is, y' is a"bad witness" if it beats less than $1/2$ of $Z(Y_k)$. Then for a fixed bad witness y', the subset $T_{y'}$ has cardinality greater than $|Z(Y_k)|/2$. In this case, by Lemma 1, we can sample a polynomial number of $z \in Z(Y_k)$, call the set Z', such that the probability

$$\Pr[Z' \cap T_{y'} = \emptyset] \leq \frac{1}{2^{2n}}.$$

Since there are at most 2^n bad witnesses,

$$\Pr[(\exists \text{ a bad witness } y' \in \{0,1\}^n)[Z' \cap T_{y'} = \emptyset]] \leq \frac{1}{2^n}.$$

Suppose now for every bad witness $y' \in \{0,1\}^n$, the sample set Z' has a non-empty intersection with $T_{y'} = Z(Y_k \cup \{y'\})$. That means that for every bad witness y', y' cannot beat all of Z'. With the polynomial sized set Z' in hand, we ask the **SAT** oracle once again whether there is a y which beats all these $z \in Z'$. Again this is a **SAT** query by Cook's Theorem. If the answer is No, then we know $x \notin L$ since otherwise there is a y which beats all $z \in \{0,1\}^n$, and certainly y beats all these $z \in Z'$. So we reject x and halt.

If the answer is Yes, we use self-reducibility of the **SAT** oracle to obtain one such y^*. Notice that by now there is no bad witness y' which can beat all of Z'. Thus this y^* is not a bad witness. This is true with probability $\geq 1 - 1/2^n$. We then define $Y_{k+1} = Y_k \cup \{y^*\}$. Then with high probability we have

$$|Z(Y_{k+1})| \leq \frac{|Z(Y_k)|}{2}.$$

As remarked earlier this gives our $\mathrm{ZPP}^{\mathrm{NP}}$ algorithm.

4 A sampling lemma

To prove Lemma 1, we will make use of universal hashing. Consider a family of hash functions:

$$\{h_s : \{0,1\}^n \to \{0,1\}^k\}_{s \in \mathcal{S}}$$

Recall that a family of hash functions is 2-universal if for every pair of distinct $x \neq y$ in $\{0,1\}^n$, and for every $\alpha, \beta \in \{0,1\}^k$, $\Pr_{s \in \mathcal{S}}[h_s(x) = \alpha \wedge h_s(y) = \beta] = 1/2^{2k}$, i.e., $h_s(x)$ and $h_s(y)$ are pair-wise independent and uniformly distributed when $s \in_R \mathcal{S}$. It is well known such family of 2-universal hash functions exist and can be easily constructed with small sample space, e.g., $h_{a,b}(x) = ax + b$ and then truncate to k bits, where a, b and x range over a finite field $\mathbf{GF}[2^n]$.

Here is an outline of the proof of Lemma 1. First we will use hash functions and the **SAT** oracle to get an approximate count of the subset $S^{=n}$. If this set is polynomially small, then we can handle it trivially. Suppose it is large. Then we will devise a simple sampling strategy satisfying the Lemma. The estimation can be done in a number of ways; we give a self-contained account using the notion of *isolation* of Sipser. (See [Si83, St83, JVV86].) The second stage is done by a simple procedure based on an estimate of points with unique inverse images from $S^{=n}$ under a random hash function. The details follow.

First we handle the trivial case where $|S^{=n}| \leq n^2$, say. We can ask our **SAT** oracle if $S^{=n} = \emptyset$. If so then Lemma 1 is vacuously true (no subset T exists with $|T| > |S^{=n}|/2$). If $S^{=n} \neq \emptyset$ yet $|S^{=n}| \leq n^2$, then we can find all the elements with the help of the **SAT** oracle. With all of $S^{=n}$ in hand, we can simply let the sample set S' be $S^{=n}$ itself.

Now assume $|S^{=n}| > n^2$.

Given $x \neq y$, we say x **collides** with y under h_s if $h_s(x) = h_s(y)$. For a subset $E \subseteq \{0,1\}^n$, we say that h_s **isolates** $x \in E$ iff x does not collide under h_s with any other element of E. The following lemma of Sipser is well known and follows from a simple probability estimate [Si83] (see also [St83]).

Lemma 2 *Let $E \subseteq \{0,1\}^n$, and let $\{h_s : \{0,1\}^n \to \{0,1\}^k\}_{s \in \mathcal{S}}$ be a family of 2-universal hash functions of cardinality 2^{2n} with $1 \leq k \leq n$. Then for all $m \geq k$,*

1. *if $|E| \leq 2^{k-1}$ then*

$$P_{s_1,\ldots,s_m \in_R \mathcal{S}}[\forall x \in E \text{ some } h_{s_i} \text{ isolates } x\,] \geq 1 - \frac{1}{2^{m-k+1}}$$

2. *if $|E| > m2^k$ then*

$$P_{s_1,\ldots,s_m \in_R \mathcal{S}}[\forall x \in E \text{ some } h_{s_i} \text{ isolates } x\,] = 0.$$

For our set $E = S^{=n}$, there is a unique k_e, where $2\log_2 n < k_e \leq n$, such that $2^{k_e - 1} < |E| \leq 2^{k_e}$. If we take every k in the range $2\log_2 n < k \leq n+1$, and randomly pick $m = 4n$ hash functions $h_{s_1}, \ldots, h_{s_m} : \{0,1\}^n \to \{0,1\}^k$, with probability $\geq 1 - \frac{1}{2^{3n}}$, at least for $k = k_e + 1$, we would get *isolation*. For each k we ask the **SAT** oracle, whether the chosen set of $h_{s_1}, \ldots, h_{s_m}$ has the property that "$\forall x \in E$, one of h_i isolates x". Since there are

only $m = 4n$ hash functions this is a **SAT** query. We pick the least k_0 such that the oracle confirms *isolation*. We abort if for no k the chosen hash functions achieve *isolation*. With probability $\geq 1 - \frac{1}{2^{3n}}$ we do not abort, and we get $k_0 \leq k_e + 1$. Also by the second part of the Lemma 2, we know definitely $|E| \leq 4n2^{k_0}$. Hence

$$k_0 - 1 \leq k_e \leq k_0 + \log_2 n + 2.$$

Denote by $U = 4n2^{k_0}$; this is an upper bound of $|E|$, and also not too far from a lower bound of $|E|$,

$$\frac{U}{16n} < |E| \leq U.$$

With this estimate, we take n hash functions $h_{s_1}, h_{s_2}, \ldots, h_{s_n}$ uniformly and independently from a family of 2-universal hash functions from $\{0,1\}^n$ to $\{0,1\}^{k_0+2\log_2 n+1}$. Note that the size of the range is $nU/2$.

For any such h_s, define the random variable C to be the number of colliding pairs,

$$C = \sum_{x \neq y \in E} \chi_{[h_s(x)=h_s(y)]}.$$

The expectation of C is

$$E[C] = \sum_{x \neq y \in E} \Pr_{s \in_R \mathcal{S}}[h_s(x) = h_s(y)] = \binom{|E|}{2} \frac{1}{nU/2} < \frac{|E|}{n}.$$

Hence by Markov's inequality

$$\Pr[C \geq |E|/8] \leq \frac{8}{n}.$$

Say a point $\alpha \in \{0,1\}^{k_0+2\log_2 n+1}$ is a *unique image* if there is a unique $x \in E$ such that $h_s(x) = \alpha$. Suppose $C \leq |E|/8$, then there can be at most $|E|/4$ many $x \in E$ involved in a collision, i.e., such that there exists some $y \neq x$, $y \in E$, $h_s(x) = h_s(y)$. At least $3|E|/4$ elements of E are mapped to a unique image. Since Lemma 1 assumes the subset T has cardinality $|T| > |S^{=n}|/2 = |E|/2$, at least $|E|/4$ many elements from T are mapped to a unique image.

We now sample as follows. After the hash functions h_{s_i} are chosen, for each $1 \leq i \leq n$, uniformly pick a target $\alpha \in \{0,1\}^{k_0+2\log_2 n+1}$, and ask the **SAT** oracle whether it has an inverse image from the set $E = S^{=n}$. Since S is in P, this is a **SAT** query. If $\alpha \in h_{s_i}(E)$, we use self-reducibility to get one inverse image. This inverse image is a sample point. If $\alpha \notin h_{s_i}(E)$, we uniformly independently pick another target α', and repeat this at most $20n^3$ times, until one sample point is found. If we do not get any sample in $20n^3$ tries for this h_{s_i}, we give up on this h_{s_i}. If we fail to get any sample point, for all h_{s_i}, $1 \leq i \leq n$, we abort.

The probability that at least one of n hash functions has its $C \leq |E|/8$ is $\geq 1 - (\frac{8}{n})^n$. Given $C \leq |E|/8$ for a h_{s_i}, the image of E has cardinality at least $3|E|/4$ (counting only those with unique images), and the range for the hashing function has cardinality $nU/2 < 8n^2|E|$, the probability that no element from $h_{s_i}(E)$ was chosen as a target α in $20n^3$ tries is $< \left(1 - \frac{3}{32n^2}\right)^{20n^3} < e^{-\frac{15}{8}n} \ll 2^{-2n}$. Given that an element from $h_{s_i}(E)$ is picked in $20n^3$

tries, the first element picked is not from $|E|/4$ many unique images from T is at most $3/4$, (a unique image has at least as high a probability to be picked as those with multiple inverse images: $|h_{s_i}(E)| \leq |E|$.)

Now we iterate this procedure a polynomial number of times ($5n$ times suffice). Given that we get at least one sample in each iteration, the sampling procedure $A(1^n)$ produces $n^{O(1)}$ elements S', the probability that all of which are not from T is exponentially small $\leq (3/4)^{5n} \ll \frac{1}{2^{2n}}$. The total error probability is at most

$$\frac{1}{2^{3n}} + 5n\left[\left(\frac{8}{n}\right)^n + e^{-\frac{15}{8}n}\right] + \left(\frac{3}{4}\right)^{5n} < \frac{1}{2^{2n}}.$$

Comment: It is possible to state a more general lemma than Lemma 1. But we shall only need the statement of this Lemma to complete our proof of Theorem 1. It is also possible to use some earlier work by Jerrum, Valiant and V. Vazirani [JVV86], Bshouty et. al. [BCGKT94], and Köbler and Watanabe [KW95] for this purpose. Please also see a recent paper by Bellare, Goldreich and Petrank [BGP00]. But this simple lemma has a sufficiently simple and self-contained proof which is sufficient for our purposes. Another useful aspect is to avoid circularity when we claim later in Section 5 that the "book" proof of Karp-Lipton gives the strongest form of this theorem to date. Of course from a logical point of view there is no difference which approach to take, any proof of this lemma is acceptable.

5 An implication for Karp-Lipton

There has been a lot of work on the general theme inspired by the Karp-Lipton Theorem. For example, Mahaney [M80] showed that if the sparse oracle is itself in NP (i.e., NP has $\leq^p_T$-complete, not just $\leq^p_T$-hard sparse set) then PH collapses to Δ^p_2. Long [Lo82] extended this to co-sparse oracles. Arvind et. al. [AKSS95] showed that under the same assumption as in Karp-Lipton that **SAT** has small circuits then MA = AM. (See [HMO92] for a survey.)

Suppose NP has polynomial size circuits. The Karp-Lipton Theorem says that the Polynomial-time Hierarchy collapses to $\Sigma^p_2 \cap \Pi^p_2$. Sengupta [Se00] pointed out that the same proof collapses the Polynomial-time Hierarchy to S^p_2. To see this we recount the "book" proof, but this time phrase it in terms of provers Y and Z. We only need to show that $\Pi^p_2 \subseteq \mathrm{S}^p_2$, then it follows that $\Pi^p_2 \subseteq \mathrm{S}^p_2 \subseteq \Sigma^p_2$ and hence they are all equal.

Let L be any language in Π^p_2. There is a normal form $L = \{x \mid (\forall^p y)(\exists^p z)[P(x, y, z)]\}$, where P is a P-time predicate. By Cook's Theorem, without loss of generality we can assume that it takes the form

$$L = \{x \mid (\forall^p s)[\phi_{x,s} \in \mathbf{SAT}]\},$$

where $\phi_{x,s}$ is a boolean formula computable in P-time from x and s. Let the size of $\phi_{x,s}$ be bounded by $p(|x|)$ for some polynomial $p(\cdot)$.

Now to show membership in S^p_2 we receive two strings y and z, from provers Y and Z respectively. We expect the string y to be a poly-size circuit for formulae of size up to $p(|x|)$. For a pair (y, z) we accept if and only if the circuit y says the boolean formula $\phi_{x,z}$ is satisfiable and by self-reducibility produced a satisfying assignment which satisfied it.

We note that there exists a relativized world where the Karp-Lipton Theorem cannot be improved to P^{NP} [H86, W85].

Acknowledgement

I thank Venkat Chakaravarthy, Oded Goldreich, Lane Hemaspaandra, Alex Russell, Uwe Schöning, Alan Selman and Samik Sengupta for interesting discussions and comments.

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.

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

[AKSS95] V. Arvind, J. Köbler, U. Schöning and R. Schuler. If NP has polynomial size circuits then MA=AM, *Theoretical Computer science* 137 (1995) 279-282.

[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.

[BCGKT94] N. Bshouty, R. Cleve, S. Kannan, R. Gavaldà 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). JCSS 52(3): 421–433 (1996).

[BGP00] M. Bellare, O. Goldreich and E. Petrank. "Uniform Generation of NP-witnesses using an NP-oracle", *Inform. and Comp.*, Vol. 163, pages 510–526, 2000.

[C96] R. Canetti. On BPP and the Polynomial-time Hierarchy. *Information Processing Letters*, 57, pages 237–241, 1996.

[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.

[H86] H. Heller, On relativized exponential and probabilistic complexity classes, *Information and Control* 71 (3), (1986), pp 231-243.

[HMO92] L. A. Hemachandra, M. Ogiwara and O. Watanabe: How Hard Are Sparse Sets? Structure in Complexity Theory Conference 1992: 222-238.

[H81] J. Hopcroft, Recent Directions in Algorithmic Research. In the Proceedings 5th GI Conference on Theoretical Computer Science, 1981, pp 123–134. Springer-Verlag *Lecture Notes in Computer Science #104*.

[JVV86] M. Jerrum, L. G. Valiant, V. V. Vazirani: Random Generation of Combinatorial Structures from a Uniform Distribution. *Theoretical Computer Science*, 43: 169-188 (1986).

[KL80] R. Karp and R. Lipton. Some connections between nonuniform and uniform complexity classes. In *Proceedings of the 12th ACM Symposium on Theory of Computing*, pages 302–309. ACM Press, April 1980. An extended version has also appeared as: Turing machines that take advice, *L'Enseignement Mathématique*, 2nd series, 28, 1982, pages 191–209.

[KW95] J. Köbler and O. Watanabe, *New collapse consequences of NP having small circuits* ICALP, LNCS 944:196–207(1995). Journal version *New Collapse Consequences of NP Having Small Circuits*. SIAM J. Comput. 28(1): 311-324 (1998).

[L83] C. Lautemann: BPP and the Polynomial Hierarchy. IPL 17(4): 215-217 (1983)

[Lo82] T. Long. A note on sparse oracles for NP. *JCSS* vol 24, No. 2, pp 224–232. 1982.

[M80] S. Mahaney. Sparse complete sets for NP: Solution of a conjecture of Berman and Hartmanis. In proceedings of 21st IEEE Symposium of Foundations of Computer Science, (1980), pp 54–60. *J. Comput. System Sci.*, 25(2):130–143, 1982.

[OL93] M. Ogiwara and A. Lozano, Sparse hard sets for counting classes. *Theoretical Computer Science* 112, 255–276 (1993).

[OW91] M. Ogiwara and O. Watanabe, On polynomial time bounded truth-table reducibility of NP sets to sparse sets. SIAM Journal on Computing 20, 471–483 (1991).

[RS95] A. Russell and R. Sundaram. Symmetric Alternation Captures BPP. *Computational Complexity* 7(2): 152-162 (1998). A Preliminary version appeared in Technical Report MIT-LCS-TM-541, 1995.

[Se00] S. Sengupta, Personal communications.

[Si83] M. Sipser, A Complexity Theoretic Approach to Randomness. STOC 1983: 330-335.

[St77] L. Stockmeyer. The polynomial-time hierarchy. *Theoretical Computer Science*, 3:1–22, 1977.

[St83] L. J. Stockmeyer: The Complexity of Approximate Counting (Preliminary Version). STOC 1983: 118-126.

[St85] L. J. Stockmeyer: On Approximation Algorithms for #P. SIAM J. Comput. 14(4): 849-861 (1985).

[W85] C. B. Wilson, Relativized circuit complexity, JCSS, 31, (1985), pp 169–181.

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

[Z96] D. Zuckerman: Simulating BPP Using a General Weak Random Source. *Algorithmica*, 16(4/5): 367-391 (1996)

ECCC ISSN 1433-8092
http://www.eccc.uni-trier.de/eccc
ftp://ftp.eccc.uni-trier.de/pub/eccc
ftpmail@ftp.eccc.uni-trier.de, subject 'help eccc'