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

Jin-Yi Cai

University of Wisconsin, Madison

Research supported in part by NSF CCR-0196197 and a Guggenheim Fellowship.
The Polynomial Hierarchy

The most well known complexity classes are $\text{P}$ and $\text{NP}$.

Building on top of $\text{NP}$, are the classes called the Polynomial Hierarchy $\text{PH}$.

(Stockmeyer)

Inductively, $\Sigma_1^p = \text{NP}$, and $\Pi_1^p = \text{coNP}$.

$$\Sigma_{k+1}^p = \text{NP}^\Sigma_k^p,$$

$$\Pi_{k+1}^p = \text{coNP}^\Sigma_k^p.$$

More succinctly, $L \in \Sigma_2^p$ iff there is a $\text{P}$-time predicate $P$ such that:

$$x \in L \iff \exists^p y \ \forall^p z \ P(x, y, z).$$
The Class $S^p_2$

There is a symmetric version of the second level PH class introduced by Russell and Sundaram and by Canetti independently.

A language $L$ is in $S^p_2$ iff there is a P-time predicate $P$ such that:

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 the length of $x$. 
An Ideal Court

Imagine two contestants $Y$ and $Z$ making the opposite claims.

An ideal court that can render a perfect justice:

- If whenever $Y$ is right, he has an argument $y$, no matter what $Z$ puts forward as his argument $z$, $y$ defeats $z$;

- On the other hand, if $Z$ is right, he has an argument $z$, no matter what $Y$ puts forward as his argument $y$, $z$ defeats $y$. 
Formal Definition

Formally, $L \in S_2^p$ iff there is a P-time computable 0-1 function $P$ on three arguments, such that

$$x \in L \Rightarrow (\exists y)(\forall z)[P(x, y, z) = 1] \quad (1)$$

$$x \notin L \Rightarrow (\exists z)(\forall y)[P(x, y, z) = 0] \quad (2)$$

where as usual "$\exists^p y$" stands for "$\exists y \in \{0, 1\}^{p(|x|)}$" for some polynomial $p(\cdot)$. Similarly for "$\forall^p z$".

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 $x$. 
Easy Containment

Both implications “⇒” can be replaced by the if and only if relation “⇔” without changing the class $S^p_2$.

**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

$$x \in L \iff (\exists^p y)(\forall^p z)[P(x, y, z) = 1]$$

$$x \notin L \iff (\exists^p z)(\forall^p y)[P(x, y, z) = 0]$$

Hence,

$$S^p_2 \subseteq \Sigma^p_2 \cap \Pi^p_2.$$
Probabilistic polynomial time Turing machines: Just like non-deterministic TM, except all moves are counted as probabilistic.

Then we say \( M \) accepts \( L \) with error probability \(< 1/3\), if for all \( x \),
\[
\text{Prob}[ M \text{ accepts } x \text{ iff } x \in L ] < 1/3.
\]

Such sets \( L \) are called in BPP.

(Note this is true for all \( x \). Not merely for “average \( x \”).)

BPP is a.k.a. Monte Carlo.
For ZPP (zero error), we consider probabilistic TM, where each path can end with 3 possible answers: “Y”, or “N”, or “?”.

Then we say $M$ accepts $L$ with zero error probability:

If $\forall x \in L$, $M$ can only say “Y” or “?” and $\text{Prob}[M(x) \text{ says “Y” }] > 1/2$;

And $\forall x \notin L$, $M$ can only say “N” or “?” and $\text{Prob}[M(x) \text{ says “N” }] > 1/2$.

Clearly $\text{ZPP} \subseteq \text{BPP}$.

$\text{ZPP}$ is a.k.a. Las Vegas.
Now consider oracle probabilistic TM.

Just like $\Sigma_2^p = \text{NP}^\text{NP}$ denotes oracle non-deterministic TM with access to NP, we can equip a probabilistic TM with access to an oracle set, say SAT of NP. Thus queries to a satisfiability query $f \in \text{SAT}$ is answered in one step, we ask what can be done probabilistically in P-time with zero error?

This is the class $\text{ZPP}^\text{NP}$.
Easy Containment for $ZPP^{NP}$

It is easy to show that

$$ZPP^{NP} \subseteq \Sigma_2^p \cap \Pi_2^p.$$ 

Our main theorem is:

**Theorem**

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

The proof uses universal hashing, approximate counting and witness sampling. We also discuss the problem of finding irrefutable proofs in $ZPP^{NP}$.
Universal Hashing

Recall a family of hash functions

\[ \{h_s : \{0,1\}^n \rightarrow \{0,1\}^k \}_{s \in S} \]

is 2-universal if for every pair of distinct \( x \neq y \) in \( \{0,1\}^n \), and for every \( \alpha, \beta \in \{0,1\}^k \),

\[ \Pr_{s \in S}[h_s(x) = \alpha \land h_s(y) = \beta] = \frac{1}{2^{2k}}. \]

\( h_s(x) \) and \( h_s(y) \) are pair-wise independent and uniformly distributed when \( s \in_R S \).

It is well known such universal hash functions can be easily constructed:

\( \text{e.g., } h_{a,b}(x) = ax + b \) and then truncate to \( k \) bits, where \( a, b \) and \( x \) range over a finite field \( \text{GF}[2^n] \).
A Lemma

Lemma

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

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

The algorithm runs in time $(n/\varepsilon)^{O(1)}$. 
Proof of Theorem

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, \( Y_1 = \{0^n\} \). 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 \( y \in Y_k \).
Proof, Cont.

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 $y \in Y_k$. 
Proof, Cont.

Suppose the answer is Yes,

Let

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

Next we grow \( Y_k \).

Our goal is, either to find conclusively that \( x \not\in L \), or to find a new \( y^* \) to be appended to the list \( Y_k \) so that the corresponding \( Z(Y_{k+1}) \) is shrunk significantly.

We will use the sampling lemma with universal hashing.
Proof, Cont.

For any $y' \in \{0, 1\}^n$, define

$$T_{y'} := Z(Y_k \cup \{y'\}) = \{z \in Z(Y_k) \mid P(x, y', z) = 0\}.$$ 

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

$$|T_{y'}| > \frac{|Z(Y_k)|}{2}.$$ 

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

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

Since there are at most $2^n$ bad witnesses,

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

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 $z \in Z'$.
Proof, Cont.

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 $z \in Z'$.

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

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

So in polynomial time we converge.
Outline of Proof of Lemma

First we will use hash functions and the \( SAT \) oracle to get an approximate count of the subset \( S^{\equiv n} \).

If this set is polynomially small, then we can handle it trivially. Suppose it is large.

Then we use a sampling strategy based on an estimate of points with unique inverse images from \( S^{\equiv n} \) under a random hash function.
Sampling Procedure

For a set $E \subseteq \{0,1\}^n$, first we can get $U$,

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

**Let** $R = O(U/\varepsilon)$.

1. Get estimate $U$
2. For $i = 1, \ldots, 3n$
3. Randomly pick $h_{s_i} : \{0,1\}^n \rightarrow R$
4. Repeat $2^{10r^2n^2}$ times
5. Randomly pick $\alpha \in R$
6. Try to find an $x \in E$
   s.t. $h_{s_i}(x) = \alpha$ using **SAT**
7. if found $4rn$ points, Goto 3
   with $i := i + 1$. 
Irrefutable Proofs

Let $L \in S^p_2$ be defined as before.

If $x \in L$, there exists $y$ that beats all $z$:

$$P(x, y, z) = 1.$$ 

We call such a $y$ an irrefutable proof w.r.t. $P$.

Similarly when $x \notin L$.

Can we find irrefutable proofs in $\text{ZPP}^{\text{NP}}$?

Theorem

For every $L \in S^p_2$, there is a P-time predicate $Q$ defining $L$, such that irrefutable proof w.r.t. $Q$ can be found in $\text{ZPP}^{\text{NP}}$. 

21
Definition of $Q$

Given $L$ defined via $P$, define $Q$ as follows:

$$Q(x; y_1, \ldots, y_m; z_1, \ldots, z_m) = 1$$

$$\iff$$

$$|\{(i, j) | 1 \leq i, j \leq m, P(x, y_i, z_j) = 1\}| > \frac{m^2}{2},$$

where $x$ is the input to $L$, $y_i, z_j \in \{0, 1\}^n$, the length $n = |x|^{O(1)}$ is determined by $P$, and $m = 7n$ or $7n + 1$, whichever is odd.
What We Look For

It is clear that $Q$ is defined symmetrically. Also $Q$ defines $L$: if $x \in L$, one can take all $y_i$ to be an irrefutable proof $y$ w.r.t. $P$. The case $x \notin L$ is symmetric.

We can find in $ZPP^{NP}$ irrefutable proof w.r.t. $Q$ in the following strong sense: Suppose $x \in L$, Find $y_1, \ldots, y_m$ such that $\forall z \in \{0,1\}^n$, $|\{i \mid P(x, y_i, z) = 1, 1 \leq i \leq m\}| > \frac{m}{2}$, (3) and symmetrically if $x \notin L$. 
By symmetry, we assume \( x \in L \), and have found out this is so in \( ZPP^{NP} \).

The sequence \( y_1, \ldots, y_m \) is defined inductively.

\( y_1, \ldots, y_k \) defines \( \{Z_k\}_{k \geq 0} \), a sequence of partitions of \( Z = \{0, 1\}^n \).

\( Z_k = \{Z_{k0}, Z_{k1}, \ldots, Z_{kk}\} \) consists of \( k + 1 \) disjoint subsets of \( Z \), where \( Z_{ki} \) consists of those \( z \) for which exactly \( i \) of \( y_1, \ldots, y_k \) beat it.
The Partitions \( \{Z_k\} \)

\( \forall z \in Z, \text{ let} \)

\[ c_k(z) = |\{ j \mid P(x, y_j, z) = 1, 1 \leq j \leq k\}|; \]

\( \text{then for } 0 \leq i \leq k, \)

\[ Z_{k,i} = \{ z \in Z \mid c_k(z) = i \}. \]

Suppose \( Z_k \) is defined. For any \( y \), it divides \( Z_{k,i} \) into two parts,

\[ Z_{k,i}^\epsilon = \{ z \in Z_{k,i} \mid P(x, y, z) = \epsilon \}, \]

for \( \epsilon = 0, 1 \). We want to choose \( y = y_{k+1} \), so that \( |Z_{k,i}^1| \geq \frac{3}{4}|Z_{k,i}| \), for all \( 0 \leq i \leq k \).

Our \( y_{k+1} \) will be chosen probabilistically.
The Vanishing Lemma

Let \( p_{k,i} = \frac{|Z_{k,i}^1|}{|Z_{k,i}|} \), we require that

\[ p_{k,i} \geq 3/4 \quad (4) \]

**Lemma**

Let \( \{Z_k\}_{k \geq 0} \) be any sequence of partitions of \( Z \), where each \( Z_{k,i} \) is divided into a disjoint union \( Z_{k,i} = Z_{k,i}^0 \cup Z_{k,i}^1 \) and

\[ Z_{k+1,i+1} = Z_{k,i}^1 \cup Z_{k,i+1}^0. \]

Suppose \( p_{k,i} \) as defined above satisfy (4), then

\[ Z_{m,0} = Z_{m,1} = \ldots = Z_{m,\left\lfloor \frac{m}{2} \right\rfloor} = \emptyset, \]

where \( m = 7n \) or \( 7n + 1 \), whichever is odd.
A Probabilistic Construction

Assume the Lemma.

With \( Z_k \) defined and \( y_1, \ldots, y_k \in \{0, 1\}^n \) in hand, we apply sampling lemma to each \( Z_{k,i}, 0 \leq i \leq k \), and probabilistically produce samples \( Z'_{k,i} \subseteq Z_{k,i} \), where each \( |Z'_{k,i}| \) is polynomially bounded. Let \( E \) denote the event:

\[
\exists y \in \{0, 1\}^n \text{ } y \text{ beats all } Z'_{k,i}, 0 \leq i \leq k, \text{ yet } \exists i, y \text{ beats at most } \frac{3}{4} \text{ of } Z_{k,i}.
\]

Then

\[
\Pr[E] \leq 2^n \cdot (k + 1) \cdot \frac{1}{22n}.
\]
Apply the Vanishing Lemma

Assume such bad $y$ does not exist, then we can ask our SAT oracle to find a $y_{k+1}$, via self-reducibility, that beats all $Z'_{k,i}$, $0 \leq i \leq k$.

Such $y_{k+1}$ certainly exists since $x \in L$ and $p_{k,i} \geq 3/4$ are all satisfied.

The Vanishing Lemma then shows that $y_1, \ldots, y_m$ is an irrefutable proof w.r.t. $Q$. 

28
Proof of Vanishing Lemma

Our proof of the Vanishing Lemma will be probabilistic in nature.

**Note:** This use of probability has nothing to do with the probabilistic construction of $Z_k$ in the proof of Theorem. The statement of Lemma is completely deterministic.

We define an ensemble of r.v. $\{\tilde{c}_k(z) : z \in Z\}_{k \geq 0}$ where for each $k \geq 0$, the family $\{\tilde{c}_k(z) : z \in Z\}$ is i.i.d. and defined as follows: $\forall z \in Z$, $\tilde{c}_0(z) = 0$, and if $\tilde{c}_k(z) = i$ then $\tilde{c}_{k+1}(z) = i + 1$ or $i$ with probability $p_{k, i}$ and $1 - p_{k, i}$ respectively.
A Random Cousin of $\mathcal{Z}_k$.

Let $\mathcal{Z}_k = \{\mathcal{Z}_{k0}, \mathcal{Z}_{k1}, \ldots, \mathcal{Z}_{kk}\}$ be defined as follows: For $0 \leq i \leq k$,

$$\mathcal{Z}_{ki} = \{z \in \mathbb{Z} \mid \tilde{c}_k(z) = i\}.$$  

We can show that

Claim: $\mathbb{E}|\mathcal{Z}_{ki}| = |\mathcal{Z}_{ki}|$, for all $k \geq 0$ and $0 \leq i \leq k$.  

A Second Random Cousin of $Z_k$

Define a second ensemble of r.v. $\{c_k(z) : z \in Z\}_{k \geq 0}$, for fixed $k \geq 0$, the family $\{c_k(z) : z \in Z\}$ is i.i.d. and defined simply as the sum of $k$ Bernoulli independent 0-1 variables with $p = 3/4$.

Formally, $c_k(z) = \sum_{j=1}^{k} I_j(z)$, where $I_j(z)$ are i.i.d. 0-1 variables with $\Pr[I_j(z) = 1] = 3/4$. Then $Z_k = \{Z_{k,0}, \ldots, Z_{k,k}\}$ is defined:

$$Z_{k,i} = \{z \in Z \mid c_k(z) = i\}.$$

We can “realize” $\tilde{Z}_k$ via $Z_k$ by a “nibbling” process.
The Nibble

Define a third ensemble \( \{c_k^*(z) : z \in Z\}_{k \geq 0} \) via \( c_k(z) \) as follows: \( c_0^*(z) = 0 \), and

\[
c_k^*(z) = c_k^*(z) + I_k(z) + \Delta,
\]

where the “nibble” \( \Delta \) is a 0-1 r.v. dependent on \( c_k^*(z) \) and \( I_k(z) \): If \( I_k(z) = 1 \) then \( \Delta = 0 \), if \( I_k(z) = 0 \), and \( i = c_k^*(z) \), then \( \Delta = 1 \) with probability \( 4p_{k,i} - 3 \), and \( \Delta = 0 \) with probability \( 4(1 - p_{k,i}) \).

The combined effect of \( I_k(z) + \Delta \) is a Bernoulli 0-1 variable taking value 1 with probability exactly \( p_{k,i} \), independent for every \( z \).
Thus $c_k^*(z)$ has exactly the same distribution as $\tilde{c}_k(z)$, and $c_k^*(z)$ is highly correlated with $c_k(z)$: $\forall z, \forall k$,

$$c_k(z) \leq c_k^*(z).$$

Thus, $\forall z, k, \ell$,

$$\Pr[\tilde{c}_k(z) \leq \ell] = \Pr[c_k^*(z) \leq \ell] \leq \Pr[c_k(z) \leq \ell].$$

Hence by Chernoff bound,

$$(\forall z) \Pr[c_m(z) \leq \left\lfloor \frac{m}{2} \right\rfloor] \leq 2e^{-\frac{7}{6}n}.$$
A Reverse Erdős Type Proof

Thus,

\[ \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} |Z_{m,i}| = \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} E|\tilde{Z}_{m,i}| \]

\[ = \sum_{z \in Z} \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \Pr[z \in \tilde{Z}_{m,i}] \]

\[ = \sum_{z \in Z} \Pr[\tilde{c}_m(z) \leq \lfloor \frac{m}{2} \rfloor] \]

\[ \leq 2^{n+1}e^{-\frac{7}{6}n} < 1. \]

But the cardinalities of the sets \( Z_{m,i} \) are all non-negative integers, we must conclude that

\[ Z_{m,0} = Z_{m,1} = \ldots = Z_{m,\lfloor \frac{m}{2} \rfloor} = \emptyset. \]

A wholly non-probabilistic statement!