Amplification of RP/BPP.

BPP in P/poly.

BPP in PH.

Recall: Completeness & Soundness

\[ M \text{ accepts } L \text{ with completeness } c \text{ and soundness } s \text{ if} \]

\[ x \in L_{\text{Yes}} \Pr_r[M(x, r) = 1] \geq c \]

\[ x \in L_{\text{No}} \Pr_r[M(x, r) = 1] \leq s \]

Weak & Strong Definition of RP/BPP

Weak Definition: \( L \) in BPP if there exists \( M \), poly \( p \), functions \( c \) and \( s \) s.t. \( c(n) \geq s(n) + 1/p(n) \) s.t. \( M \) accepts \( L \) with completeness \( c(n) \) and soundness \( s(n) \). (RP is special case with \( s(n) = 0 \).)

Strong Definition: \( L \) in BPP if for every poly \( q \) there exists \( M \), functions \( c \) and \( s \) s.t. \( c(n) \geq 1 - 2^{-q(n)} \) and \( s(n) \leq 2^{-q(n)} \) s.t. \( M \) accepts \( L \) with completeness \( c(n) \) and soundness \( s(n) \). (RP is special case with \( s(n) = 0 \).)

Proposition: Strong Defn. = Weak Defn.

Proof aka “Amplification”

Given \( M \) satisfying weak defn., here’s code for \( M' \):

Run \( M \) on its input \( x t = p(n)^2 \cdot q(n) \) times with independent random coins, and compare number of accepts to \( (c(n) + s(n))/2 \cdot t \). If larger, accept \( x \) and reject otherwise.
“Chernoff Bounds”: If $X_1, \ldots, X_t$ are independent random variables taking values in $[0, 1]$ with $\mathbb{E}[X_i] = \mu$, then 
$$\Pr[|\sum_i X_i - \mu t| \geq \lambda \sqrt{t}] \leq \exp(-\lambda^2).$$

Applying to our case: $X_i$ is indicator of event that $M$ accepts in $i$th iteration.
$$\mu = c(n) \text{ if } x \in L_{Yes}.$$ Do the wrong thing if argument of $|.|$ is greater than $t/2p(n)$, gives 
$$\lambda = O(\sqrt{t/p(n)}) = O(\sqrt{q(n)}).$$

Conclude: Do the wrong thing w.p.
$$\exp(-\lambda^2) = \exp(-q(n)).$$

**Formal proof**

Let $M$ be a strong BPP machine for

$L$

with $q(n) = n + 1$.

Say $M$ errs on $x$ with random string $r$ (denoted $(M, x, r)$ wrong if $M(x, r) = 1$ but $x \in L_{No}$ or $M(x, r) = 0$ but $x \in L_{Yes}$.

$$\Pr_r[(M, x, r) \text{ wrong }] \leq 2^{-(n+1)}.$$

Say $(M, r, n)$ wrong $\exists x$ of length $n$ such that $(M, x, r)$ wrong.

$$\Pr_r[(M, r) \text{ wrong }] \leq 2^n \cdot 2^{-(n+1)}.$$

In particular for every $n \exists r_n$ s.t. $(M, r_n, n)$ not wrong.

---

**Simple application: promise-BPP in P/poly**

Due to [Adleman].

Note: Class $C_1 "\subseteq" C_2$ if for every $L \in C_1$, there exists $K \in C_2$ such that $L_{Yes} \subseteq K_{Yes}$ and $L_{No} \subseteq K_{No}$.

“Reasonable notion of containment.”

Idea (for promise-BPP in P/poly): Use strong defn.; then some random string is good for all strings. Let this be the advice.

Using $r_n$’s as advice, have that language accepted by $M$ with advice $r_1, \ldots, r_n, \ldots$ decides $L$. 
Note: Not quite trivial. How to have a bounded round interaction to convince \( x \in L \)?

Consider following game: Y & Z are all powerful players. Y wants to convince you (the audience) that \( x \in L \) and Z claims otherwise. If \( L \in \Sigma_2 \), then Y should be able to say something, call it \( y \), such that if \( x \notin L \), Z can respond with a \( z \) such the audience can see that \( Z \) was right. On the other hand if \( x \in L \), then no matter what \( Z \) says, audience is not convinced.

What should Y and Z try to do? What should the audience do?

Let \( M \) be the BPP machine recognizing \( L \).

Most strings \( w \) are good (\( M(x,w) = \text{accept} \)); or very few are good. How to convince you?

Idea 1: Y divides space into two equal parts with all bad strings in one part and a bijection \( \pi \) between the two parts. Y claims every string or its map under bijection is good! If Z wants, it can challenge!

If Z finds a string \( w \) where neither \( M(x,w) \) nor \( M(x,\pi(w)) \) accept - he wins.

Else Y wins.

Seems convincing. Y can win if bad set is smaller than \( 1/2 \). Y can’t win if bad set more than \( 1/2 \).

Problem: How do Y give the bijection?

Bijections have to simple: So we’ll stick \( \pi_r : w \mapsto w \oplus r \).

In this space of bijections the proof doesn’t go through. But the idea is starting to emanate.

Debate for membership in BPP

Theorem: If \( x \) in \( L \) there exist \( r_1, \ldots, r_{2m} \in \{0,1\}^m \) such that the \( w \)'s are covered; i.e., for every \( w \) there exists an \( i \in [2m] \) such that \( M(x, \pi_{r_i}(w)) \) accepts.

If \( x \) not in \( L \), then for any \( r_1, \ldots, r_{2m} \in \{0,1\}^m \) there is an uncovered \( w \).

Assuming theorem: Debate: Y announces \( r_1, \ldots, r_{2m} \). Deniss challenges with a \( w \). You compute \( M(x, w \oplus r_1) \lor \cdots \lor M(x, w \oplus r_{2m}) \). If true, Y wins (\( x \in L \)) else Z wins (\( x \notin L \)) - you decide!
Proof of theorem

If $x$ in $L$

\[ \Pr_r[M(x, w \oplus r)] \geq 1 - 2^{-n} \geq 1/2. \]
\[ \Pr_r[\exists i \in [2m] \text{ s.t. } M(x, w \oplus r_i)] \geq 1 - 2^{-2m}. \]
\[ \Pr_r[\forall w \in \{0, 1\}^m, \exists i \in [2m] \text{ s.t. } M(x, w \oplus r_i)] \]

Yields first part.

Proof of theorem (second part)

$x$ not in $L$. Say I pick best possible $r_1, \ldots, r_{2m}$ below.

\[ \Pr_w[M(x, w \oplus r_i)] \leq 1/100m. \]
\[ \Pr_w[\exists i \in [2m] \text{ s.t. } M(x, w \oplus r_i)] \leq 1/50. \]

QED!

Power of the prover

If $Y$ is right - it just needs to pick $r_1, \ldots, r_{2m}$ at random!

If $Z$ is right, he just needs to pick $w$ at random.

So we just need randomness to simulate randomness!

Hmm.... that didn’t sound so impressive - I should have said ...

So we just need one-sided randomness to simulate two-sided randomness!

Current issues in randomness

- Reducing randomness
  - Algorithm specific: Limited independence, Epsilon-bias.
  - Generically, during amplification: “Recycling”.
- Using imperfect randomness: Extractors.
- Derandomization: Pseudorandomness, hardness versus randomness.