Lecture 24

- Probabilistic TMs
- Primality Testing
- Polynomial identity testing
- Interactive proofs

A probabilistic TM is a TM that, in addition to its regular tape, also has a "random" tape filled with random bits.

Def \( L \in \text{RP}_c \) if \( \exists \text{ prob. TM } M \) s.t.

- \( \forall x \in L \Rightarrow \Pr [M \text{ accepts } x] \geq 1 - c \)
- \( \forall x \notin L \Rightarrow \Pr [M \text{ accepts } x] = 0 \)

Then [Amplification of RP]:

If \( L \in \text{RP}_c \) for some constant \( c \), then it is in \( \text{RP} \) \( 1 - c \cdot \text{poly}(n) \) for any poly.

pf: just run M \( \text{poly}(n) \) times, accept if it accepts just once.

\[ \text{NP} \]
\[ \text{RP} \]
\[ \text{P} \]
Def \( L \in \text{coRP}_s \) if \( \exists \) a p.p.t. TM \( M \) s.t.,
completeness: \( x \in L \Rightarrow \Pr[ M \text{ accepts } x ] = 1 \)
\( x \notin L \Rightarrow \Pr[ M \text{ accepts } x ] \leq \frac{1}{s} \)

Then [amplification of coRP] A const.,
A polynomials \( \text{coRP}_s = \text{coRP}_{s \cdot \text{poly}(n)} \)

Most widely used prob alg.
Rabin-Miller primality test
On input candidate prime \( p \), written in binary
if \( p \text{ prime } \), always accept
if \( p \text{ composite } \), reject w/ prob \( \frac{1}{2} \)

Polynomial identity testing
Given polynomials \( p, s \), determine if they are identical (\( \deg(p), \deg(s) \leq m \))
\( p = \text{product and sum of other polynomials} \)
compact form e.g. \( (x+1)^{10000} \)
poly identity testing

on input $P, S$, both polynomials of degree $\leq m$ and univariate

- pick $q$, prime, $\geq 2m$
- pick random $0 \leq x < q$
- if $P(x) \mod q = S(x) \mod q$, accept
  else, reject

Graph non-isomorphism $m = \exists \langle G_0, G_1 \rangle$
no matter how you permute vertices of $G_0$ can't get $G_1$

Verifier

Power

(corp. unbounded)

Determine if $H = G_0$, if $H \neq G_0$, if random (call it $G_0$)

$\rightarrow$ accept if $b' = b$, reject otherwise
Def: An interactive proof system for a language $L$ is a pair of TMs, $P$, $V$, interactive

$V$ is a pptm

S.t.

(perfect) completeness: $x \in L \Rightarrow \Pr[V \text{ accepts } x] = 1$

soundness: $x \notin L \Rightarrow \Pr[V \text{ accepts } x] \leq \frac{1}{2}$

$L \in IP$ if it has an interactive proof system

Thm: $IP = PSPACE$

Thm: $co-NP \subseteq PSPACE$

Goal: interactive proof for Tautology

$\#SAT = \exists \langle \phi, k \rangle \mid \phi \text{ has exactly } k \text{ sat. assignments}$

To prove $\phi \in \text{Taut}$, prove $\langle \phi, 2^n \rangle \in \#SAT$

for $\phi$ with $n$ variables
"Arithmetize" \( \phi(x_1, \ldots, x_n) \) to represent it as a polynomial \( f(x_1, \ldots, x_n) \) s.t.
\[
f(a_1, \ldots, a_n) = \phi(a_1, \ldots, a_n) \text{ for } a_1, \ldots, a_n \text{ broken}
\]

\[x_1 \lor x_2 \lor \overline{x_3} \rightarrow 1 - (1 - x_1)(1 - x_2)x_3\]

to show \( \phi \) is taut, sufficient to show
\[
\frac{1}{2} \cdots \frac{1}{2} f(a_1, \ldots, a_n) = 2^n
\]

Sufficient to show that \( g_1(x_1) = \frac{1}{2} \cdots \frac{1}{2} f(a_1, \ldots, a_n) \)

is s.t.
\[
g_1(0) + g_1(1) = 2^n
\]

Proof:

1. Verify \( \phi \)

   \[
s_1'(x_1) \quad \text{if } s_1'(0) + s_1'(1) \neq 2^n
   \]

   reject

   or

   pick random \( x_1 \)

   \[
g_2'(x_1, x_2) \quad \text{check}
   \]

   \[
g_1'(x_1) = g_2'(0, 0) + g_2'(1, \phi)
   \]

   \[
   g_{n-1}(x_1, x_2, \ldots, x_{n-1}, x_n)
   \]