Today

- Proof: UNSAT $\subseteq$ IP
- Proof: $\#3$SAT $\subseteq$ IP
- PH $\subseteq$ IP
- Start discussing PSPACE $\subseteq$ IP
Representing boolean formulas with polynomials

- Formula $\phi$ with $m$ clauses on variables $x_1, \ldots, x_n$.
- $N \geq 2^n \cdot 3^m$ prime number.
- Translate $\phi$ to a polynomial $p$ over the field (mod $N$) as follows:
  - $x_i \rightarrow x_i$, $\overline{x_i} \rightarrow (1 - x_i)$
  - Clause is translated to the sum of the (at most 3) expressions corresponding to the literals in the clause.
  - $p$ is the product of all the $m$ expressions corresponding to the $m$ clauses.
Representing boolean formulas with polynomials

- Each literal has degree 1, so \( p \) has degree at most \( m \).
- For a zero-one assignment, \( p \) evaluates to zero if this assignment does not satisfy \( \phi \), and to a non-zero number otherwise.
- This number can be at most \( 3^m \).
- \( \phi \) is unsatisfiable if and only if

\[
\sum_{x_1 \in \{0,1\}} \ldots \sum_{x_n \in \{0,1\}} p(x_1, \ldots, x_n) \equiv 0 \pmod{N}
\]
\( \phi \downarrow \)

\[ P \]

\[ N, \text{ a proof that } N \text{ is prime} \]

\[ q_1(x) = \sum_{x_2, \ldots, x_n \in \{0,1\}} p(x, x_2, \ldots, x_n) \]

\[ r_1 \]

\[ q_2(x) = \sum_{x_3, \ldots, x_n \in \{0,1\}} p(r_1, x, x_3, \ldots, x_n) \]

\[ r_2 \]

\[ \vdots \]

\[ q_i(x) = \sum_{x_{i+1}, \ldots, x_n \in \{0,1\}} p(r_1, \ldots, r_{i-1}, x, x_{i+1}, \ldots, x_n) \]

\[ r_i \]

\[ \vdots \]

\[ q_n(x) = p(r_1, \ldots, r_{n-1}, x) \]

\[ \phi \downarrow \]

\[ V \]

check primality proof

check \( q_1(0) + q_1(1) = 0 \)

pick random \( r_1 \in \{0, \ldots, N - 1\} \)

check \( q_2(0) + q_2(1) = q_1(r_1) \)

pick random \( r_2 \in \{0, \ldots, N - 1\} \)

\[ \vdots \]

check \( q_i(0) + q_i(1) = q_{i-1}(r_{i-1}) \)

pick random \( r_i \in \{0, \ldots, N - 1\} \)

check \( q_n(0) + q_n(1) = q_{n-1}(r_{n-1}) \)

pick random \( r_n \in \{0, \ldots, N - 1\} \)

check \( q_n(r_n) = p(r_1, \ldots, r_n) \)
A proof system for \#SAT

- Formula $\phi$ with $m$ clauses on variables $x_1, \ldots, x_n$, suppose it has $k$ satisfying assignments.
- We want an IP s.t. if $P$ gives $k$ as an answer then $V$ will accept w.p. 1, otherwise $V$ will reject w.h.p.
- Change the way to translate $\phi$ to a polynomial $p$ over the field (mod $N$) as follows:
  - $z_1 \lor z_2 \lor z_3 \rightarrow 1 - (1 - z_1)(1 - z_2)(1 - z_3)$
  - $p$ is the product of all the $m$ expressions corresponding to the $m$ clauses.
A proof system for \#SAT

- For a zero-one assignment the clause evaluates to 1 if the assignment satisfies that clause and 0 if not.
- So zero-one assignments that satisfy formula will make $p=1$ and the rest $p=0$.
- Degree of $p$ is now $3m$, instead of $m$, but now
  \[
  \sum_{x_1 \in \{0,1\}} \ldots \sum_{x_n \in \{0,1\}} p(x_1, \ldots, x_n) = \# \text{ sat. assignments}.
  \]
- Enough to take $N > 2^n$. 
A proof system for #SAT

- First round prover sends $k$.
- Then follows the previous protocol.
- After first message, verifier checks if $q_1(0) + q_1(1) = k$.
- Rest is the same as before.