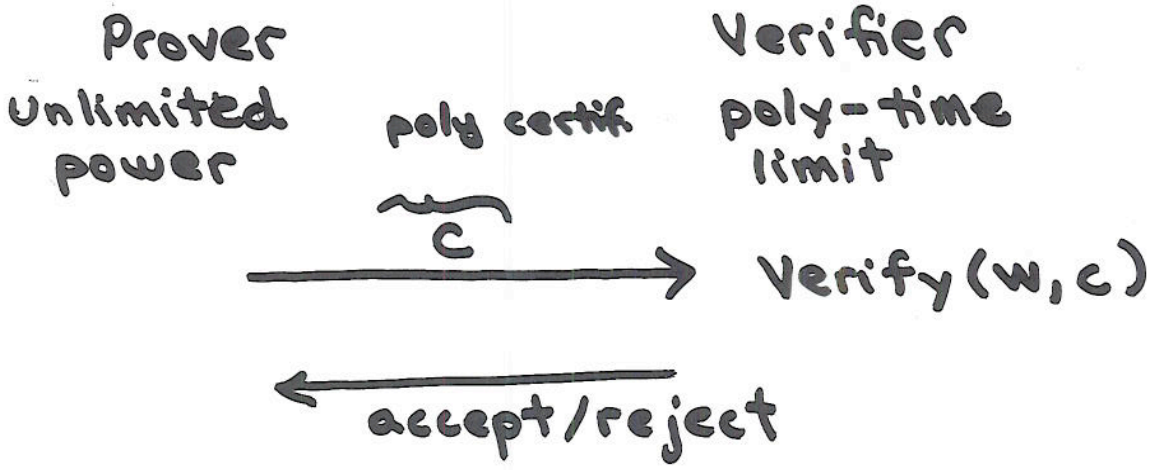
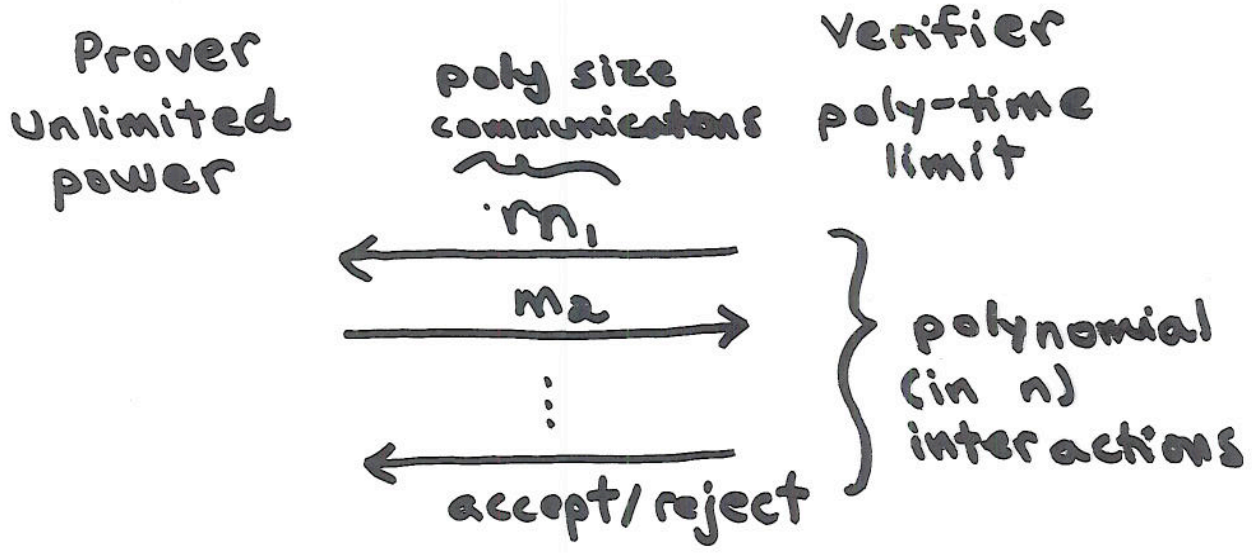
Interactive Proofs (IP)

$w \in L$

NP



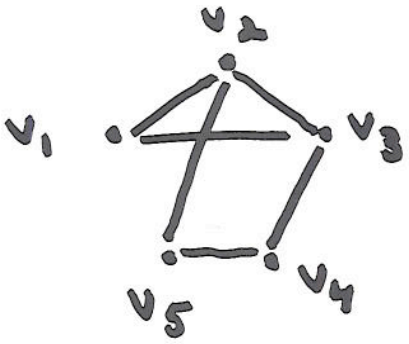
IP



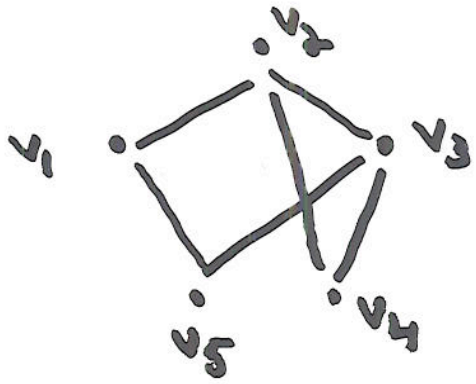
+  random bits available to verifier

1. If $w \in L$, Verifier accepts with "high probability" $(1-\epsilon)$
2. If $w \notin L$, verifier...

A "Hard" Problem in IP



G_1



G_2

(GI) Graph Isomorphism: G_1, G_2

(GNI) Graph NON Isomorphism: G_1, G_2

Claim 1: GNI $\in$ IP

Claim 2: #3SAT $\in$ IP

#SAT ∈ IP

(Attempt #1)

- Let the variables be $x_1, \ldots, x_m$
- Let $f_i(x_1, \ldots, x_i)$ be a function where $f_i(b_1, \ldots, b_i) \triangleq$ number of sat. valuations when $x_1 = b_1, \ldots, x_i = b_i$
- Consider, for example, ...

$$f_m(\underbrace{0, 1, 1, 0, \ldots, 1}_{m})$$

$f_1(0)$

$f_0()$

- Claim: $f_i(b_1, \ldots, b_i) =$

$$f_{i+1}(b_1, \ldots, b_i, 0) + f_{i+1}(b_1, \ldots, b_i, 1)$$

Protocol : Attempt #1

Input: 3SAT instance

Can check $f_m(x_1, \ldots, x_n$

Prover

Verifier

Look, here's $\tilde{f}_0()$

Nice, but I'd like to be sure that your $\tilde{f}_0() = f_0()$

Look, here's $\tilde{f}_1(0), \tilde{f}_1(1)$

If $\tilde{f}_0() = f_0()$ then $\tilde{f}_1(0) + \tilde{f}_1(1) = f_0()$

But if $\tilde{f}_0() \neq f_0()$ then it's not possible that both $\tilde{f}_1(0) = f_1(0)$ and $\tilde{f}_1(1) = f_1(1)$.

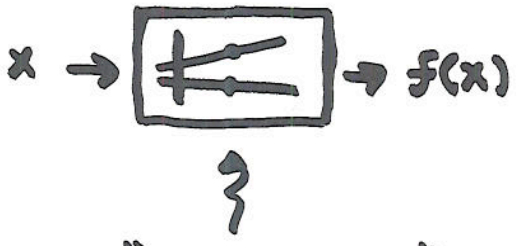
So, I'll check both $\tilde{f}_1(0)$ and $\tilde{f}_1(1)$

A Proof of Identity Protocol

Prover

Verifier

"I'll send you the line $f(x)=ax+b$ to demonstrate that I'm honest"



"Expensive" line evaluator

$0 \leq x \leq 10^9$

Arithmetization!

$(x_1 \vee x_2) \wedge (x_1 \vee \overline{x}_3)$

$\downarrow$

$p(x_1, x_2, x_3) = (1-(1-x_1)(1-x_2)) \cdot (1-(1-x_1)x_3)$

Assume variables $x_1, \ldots, x_m$

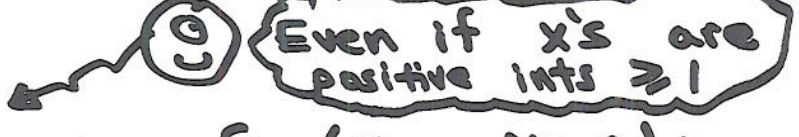
$f_i(x_1, \ldots, x_i) \triangleq$ # satisfying valuations assuming given values of $x_1, \ldots, x_i$

Ex $f_m(\underbrace{1,1,1,\ldots,1}_{m})$ $f_1(1)$ $f_2(1,0)$

Building f_i ...

$f_m(x_1, \ldots, x_m) = p(x_1, \ldots, x_m)$

$f_i(x_1, \ldots, x_i) = \sum_{b_{i+1}, \ldots, b_m \in \{0,1\}} p(x_1, \ldots, x_i, b_{i+1}, \ldots, b_m)$

Properties ... 

$f_i(x_1, \ldots, x_i) = f_{i+1}(x_1, \ldots, x_i, 0) + f_{i+1}(x_1, \ldots, x_i, 1)$

f_i "low degree"

This space for you!