This lecture presents work from a paper with Eli Ben-Sasson

[Proc '2005]

[SAM J. Computing '2008]
Today

Probabilistically Checkable Proofs

- Definition, parameters
- Idea behind a PCP construction

PCP: ① New format for writing proofs
      ② Should allow short proofs of true theorems
      ③ Should not allow any proofs of false "theorems"
      ④ Key ingredient: Verifier
          - reads theorem \( \& G \)
          - tosses random coins \( r(n) \) \( \in \{0,1\}^r(n) \)
          - depends on \( G, R \)
          - (nonadaptively) decides query locations \( Q_1, Q_2, \ldots, Q_q \)
          - Receives \( G \), computes (circuit for) \( P: \{0,1\}^2 \rightarrow \{0,1\} \)
          - Outputs \( \hat{P}(T_1(Q_1), T_1(Q_2), \ldots, T_1(Q_q)) \)

  ⑤ Parameters:
  ① Randomness \( r(n) \)
  ② Length \( l(n) \)
  ③ Query Complexity \( l(n) \)

  ⑥ Guarantees:
  ① \( G \) 3-colorable \( \Rightarrow \exists \hat{T} \in \{0,1\}^l \) s.t. \( P(-) = 1 \) always
  ② \( G \) not 3-colorable \( \Rightarrow \forall \hat{T} \)
      \( \Pr[P(\hat{T}) = 1] \leq \frac{1}{2} \).
Can they even exist? Not obvious ... but yes they do.

Today: Insight into one "non-trivial" problem.

PCP Theorem: [AS'92, Almss'92]: \( \exists \) PCP verifier with

\[ l(n) = n^{0(c)}; q(n) = O(1); r(n) = O(\log n) \]

Today: Weak theorem (with details omitted) giving

\[ q(n) = \text{poly} (\log n) \]

Main ingredients: polynomials, randomness ...

(similar to \( \text{IP} = \text{PSPACE} \); not coincidental)

Facts about polynomials:

1. Let \( F \) be (finite) field \( \mathbb{F} \) and \( f: \mathbb{F} \to \mathbb{F} \)
   \( \exists \) poly \( P: \mathbb{F} \to \mathbb{F} \) of degree \( \leq |S| \) s.t.
   \[ P(x) = f(x) \quad \forall x \in S. \quad \text{[Exercise]} \]

2. (Bivariate version) \( f: S \times S \to \mathbb{F} \)
   \( \exists \) poly \( P: \mathbb{F} \times \mathbb{F} \to \mathbb{F} \) of degree \( \leq |S| \) in each variable
   \[ P(x, \beta) = f(x, \beta) \quad \forall (x, \beta) \in S \times S. \quad \text{[Exercise]} \]
Additional facts:

3. \( P : F \to F \) has \( \deg \) in a polynomial \( \deg \) such that
\[
P(\alpha) = 0 \quad \forall \alpha \in S \quad \text{then} \quad \frac{P(x)}{Z_s(x)} \quad \text{is also a polynomial (of } \deg \leq \deg(P) - 1)\]

where \( Z_s(x) = \prod_{\alpha \in S} (x - \alpha) \)

4. \( Q : F \times F \to F \) is of \( \deg \) in \( (x, y) \).
   \( \forall \alpha, \beta \in S \times S \quad Q(\alpha, \beta) = 0 \)

5. \( A, B : F \times F \to F \) and \( \deg \leq (d, d) \) in \( (x, y) \)
   \( [ \text{even better...} ] \)

6. \( \deg \leq (d, d) \) in \( (x, y) \)

7. \( Q(x, y) = Z_s(x) \cdot A(x, y) + Z_s(y) \cdot B(x, y) \).

8. \( \frac{d}{\text{d}} \)

9. \( \text{distinct} \)

5. \( A_1, A_2 : F \to F \) have \( \deg \leq d \) then
   \[
   \Pr_{\alpha \in F} [ A_1(\alpha) = A_2(\alpha) ] \leq \frac{d}{1F}
   \]

6. \( B_1, B_2 : F \times F \to F \) have \( \deg \leq (d, d) \) in \( (x, y) \)

   then \( \Pr_{\alpha, \beta} [ B_1(\alpha, \beta) = B_2(\alpha, \beta) ] \leq \frac{2d}{1F} \)
Overview of Proof:

"Theorem": \( G \) given by \( E : V \times V \rightarrow \{0,1,\} \)
("\( G \) is 3-colorable")

"PC Proof":
\[
\begin{align*}
A_1 &: F \rightarrow F \\
A_2 &: F \rightarrow F \\
B_1 &: F \times F \rightarrow F \\
B_2 &: F \times F \rightarrow F
\end{align*}
\]

Verification:

1. Syntactic Checks [don't depend on \( G \)]
   - Verify degree \( \deg(A_1) \leq d_1 \)
   - Verify degree \( \deg(B_1) \leq c_1 \)
   - Verify degree \( \deg(A_2) \leq d_2 \)
   - Verify degree \( \deg(B_2) \leq c_2 \)

2. Semantic Checks [depend on \( G \)]
   - [somehow imply "\( G \) is 3-colorable"]
Syntactic Checks [Omitted]

Given "table": \( A : F \rightarrow F \), can add proof \( T_T A : (\cdot ) \rightarrow F \)

\( \exists \) verifier \( V_i \) s.t.

1. \( \text{if } \deg (A) \leq d \), \( \exists T_T A \) s.t. \( V_i (d) \) reads \( O (\text{polylog}) \) values of \( A, T_T A \)

2. \( \text{if } \deg (A) \leq d \), \( \exists T_T A \) s.t. \( V_i (d) \) accepts.

3. \( \text{if } A \) far from every degree \( d \) poly, then \( T_T A \)

\( \Pr [ V_i (d) \) accepts] \leq \frac{1}{10} \)

Bivariate version

\( B : F \times F \rightarrow F \)

(fill in details yourself later) 😊
Idea (of Semantics)

1. \( E : V \times V \to \mathbb{Z} \) \( n = 1 \times 1 \)

2. \( \text{Pick } F \text{ s.t. } \|F\| \geq \mathcal{B} \) \& let \( V \leq F \)

\( \text{Extend } E \text{ to } \hat{E} : F \times F \to F \text{ if } \deg \leq (n,n) \)

[\( \hat{E} \text{ known to verif.} \)]

2. Ask for \( X : V \to \mathbb{Z} \) \( \delta < \)

\( \hat{F} (x, y) \in V \times V \) at least one of the following holds

- \( X(\hat{F}) = 0 \)
- \( X(y) - X(y) = -2 \)
- \( \frac{\hat{F}}{} = -1 \)
- \( \frac{\hat{F}}{} = 1 \)
- \( \frac{\hat{F}}{} = 2 \)
1. \( E \)  
   \( E : \mathbb{F} \times \mathbb{F} \rightarrow \mathbb{F} \)  
   s.t. \( E(\alpha, \beta) = E(\alpha, \beta) \)  
   \( \forall (\alpha, \beta) \in \mathbb{V} \times \mathbb{V} \)  
   \( d(E) \leq (n, n) \).  

2. \( X \)  
   \( X : \mathbb{F} \rightarrow \mathbb{F} \)  
   \( \text{of degree } \leq n \).  

   Verifier "syntactic" checks are done;  
   still needs to check  

1. \( X \) is a 3-coloring  
   \( \hat{X}(\alpha), (\hat{X}(\alpha) - 1), (\hat{X}(\alpha) - 2) = 0 \)  
   \( \forall \alpha \in \mathbb{V} \).  

2. \( X \) is valid for \( E \)  
   \( \hat{E}(\alpha, \beta) \cdot \prod_{i \in \{2, -1, 1, 2\}} (\hat{X}(\alpha) - \hat{X}(\beta) - i) = 0 \)  
   \( \forall \alpha, \beta \in \mathbb{V} \).
3-Coloring?

V works for

\[ A_1 = \chi : \mathbb{F} \to \mathbb{F} \]

\[ A_2 = \chi(x) \cdot (\chi(x) - 1) \cdot (\chi(x) - 2) \]

with proof that

it has deg \( \leq 3n \)

\[ A_2(x) = A_1(x) \cdot (A_1(x) - 1) \cdot (A_1(x) - 2) \]

for random \( x \)

\((\text{power of polynomials})\)

But still need to check \( A_2(x) = 0 \) \( \forall x \in \mathbb{V} \).

How can we do this?
Proving $A_2$ is ZERO on $V$

Idea: Use Fact (3) on Page 3

$$A_3(x) = \frac{A_2(x)}{Z_V(x)} = \text{poly (of deg } \leq 2n)$$

Prover writes

- $A_1$
- $A_2$
- $A_3$

Verifies: 1) Syntactic Checks

2) $A_2(\alpha) = A_{\alpha}(\alpha) \cdot (A_{\alpha}(\alpha) - 1) \cdot (A_{\alpha}(\alpha) - 2)$ for random $\alpha$

3) $A_3(\alpha) = \frac{A_2(\alpha)}{Z_V(\alpha)}$ for random $\alpha$. 

[Note: The image contains a text snippet with mathematical expressions and steps in a proof, but the full context and completeness of the proof cannot be accurately represented here due to the limitations of text-based transcription.]
Valid 3-coloring:

1. \[ B_1(x,y) = \hat{E}(x,y) \cdot \Pi_i (A_i(x)-A_i(y)-i) \]
2. \( B_2, B_3 \) (based on Fact 4 on Page 3)

Verifier Checks

1. Syntactic Checks on \( B_1, B_2, B_3 \)
2. \[ B_1(x,\beta) = \hat{E}(x,\beta) \cdot \Pi_i (A_i(x)-A_i(\beta)-i) \]
   for random \((x,\beta)\)
3. \[ B_2(x,\beta) = Z_V(x) \cdot B_2(x,\beta) 
   + Z_V(\beta) \cdot B_3(x,\beta) \]
   for random \((x,\beta)\).

\( \text{QED} \)
Getting $O(1)$ queries

Current Proof:

$\rightarrow \quad n^4 \quad \text{sized} \quad \rightarrow$

Vertex reads $O(\text{polylog})$ pieces

With lots of work:

Then: Some recursion & some new ideas
State of the art

Three parameters: constants ($a, b, q$)

1. $e(n) = n$
2. Error $= 1 - \frac{1}{b}$ [Prob. of accepting incorrect proof]
3. Query $= 2$

Best hope $- a = 1 + o(1)$
- $(b, q) = (2 + o(1), 3)$

Can we achieve these simultaneously?

Many interesting steps
- [Polishchuk-Spielman]: $a = 1 + \varepsilon$
- [Itai-Stein]: $(b, q) = (2 + o(1), 3)$
- [Mohkowitz-Raz]: $(a, b, q) = (\varepsilon o(1), 2 + o(1), 3)$

Real Question: Can they be as good as ECC? linear blowup?