This lecture presents work from

a paper with ELI BEN-SASSON

[STOC '2005]

[SIAM J. Computing '2008]

TODAY

PROBABILISTICALLY CHECKABLE PROOFS

- Definition, parameters
- Idea behind a PCP construction

"G" is 3-colorable

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) coins~~ $R \in \{0,1\}^{r(n)}$
- (nonadaptively) decides query locations $Q_1, Q_2 \ldots Q_q$ $\in \{1 \ldots \ell\}$
- ~~Reviews~~ Precomputes (circuit for) $P: \{0,1\}^q \to \{0,1\}$
- outputs $P(\Pi(Q_1), \Pi(Q_2) \ldots \Pi(Q_q))$

depend on G, R

(5) Parameters: (1) Randomness $r(n)$

(2) length $\ell(n)$

(3) Query Complexity $q(n)$

(6) Guarantees: ⊙ G 3colorable $\Rightarrow$ $\exists \Pi \in \{0,1\}^\ell$ s.t. $P(\_\_) = 1$ always

⊙ G not 3colorable $\Rightarrow$ $\forall \Pi$ $\Pr[P(\ ) = 1] \le 1/2$.

- Can they even exist? Not obvious ... but yes they do.

~~Today: Insight into one "non-trivial" constru~~

<u>PCP Theorem</u>: [AS'92, ALMSS'92]: $\exists$ PCP verifier with

$$\ell(n) = n^{O(1)} \; ; \quad q(n) = O(1) \; ; \quad r(n) = O(\log n)$$

Today: weak theorem (with details omitted) giving

$$q(n) = \text{poly}(\log n)$$

<u>Main Ingredients</u>: polynomials, randomness ...

(similar to IP = PSPACE; <u>not</u> coincidental)

<u>Facts about polynomials</u>:

(1) Let $\mathbb{F}$ be (finite) field & $S \subseteq \mathbb{F}$ & $f: S \to \mathbb{F}$

$\exists$ poly $p: \mathbb{F} \to \mathbb{F}$ of degree $\leq |S|$ s.t.

$p(\alpha) = f(\alpha) \quad \forall \alpha \in S$. [Exercise]

(2) (bivariate version) $f: S \times S \to \mathbb{F}$

$\exists \; p: \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ of degree $\leq |S|$ in each variable

$p(\alpha, \beta) = f(\alpha, \beta) \quad \forall (\alpha, \beta) \in S \times S$.

[Exercise]

Additional facts : [DON'T READ THIS PAGE NOW]

3. if $P : \mathbb{F} \to \mathbb{F}$ ~~has deg~~ is a polynomial s.t.

$P(\alpha) = 0 \quad \forall \alpha \in S$ then

$\frac{P(x)}{Z_S(x)}$ is also a polynomials (of deg $\le \deg(P) - |S|$)

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

4. if $Q : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ is of deg (d, d) in (x, y).

& $Q(\alpha, \beta) = 0 \quad \forall (\alpha, \beta) \in S \times S$ then

$\exists\, A, B : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ of deg $\le (d, d)$ in (x, y) [or even better...]

s.t. $Q(x, y) = Z_S(x) \cdot A(x, y) + Z_S(y)\, B(x, y)$.

5. if distinct $A_1, A_2 : \mathbb{F} \to \mathbb{F}$ have deg $\le d$ then

$$\Pr_{\alpha \in \mathbb{F}} \left[A_1(\alpha) = A_2(\alpha) \right] \le \frac{d}{|\mathbb{F}|}$$

if distinct $B_1, B_2 : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ have deg $\le (d, d)$ in (x, y)

then $$\Pr_{\alpha, \beta} \left[B_1(\alpha, \beta) = B_2(\alpha, \beta) \right] \le \frac{2d}{|\mathbb{F}|}$$

Overview of Proof:

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

"PCProof" : $A_1 : \mathbb{F} \to \mathbb{F}$ $\quad B_1 : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$

$A_2 : \mathbb{F} \to \mathbb{F}$ $\quad B_2 : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$

$\vdots$ $\quad \vdots$

Verifier: (1) Syntactic Checks [don't depend on G]

Verify degree $(A_1) \le d_1$ $\quad \deg(B_1) \le e_1$

degree $(A_2) \le d_2$ $\quad \deg(B_2) \le e_2$

$\vdots$ $\quad \vdots$

(2) Semantic Checks [depend on G]

[somehow imply "G is 3colorable"]

5

Syntactic Checks [Construction Omitted]

I) $\exists$ verifier V_1 s.t.
Given "table": $A : \mathbb{F} \to \mathbb{F}$, can add proof $\Pi_A : \mathbb{F}^2 \to \mathbb{F}$

~~s.t. & & & s.t.~~

① ~~if $\deg(A) \leq d$, $\exists \Pi_A$~~ s.t. $V_1(d)$ reads $O(\text{polylog} n)$ values of A, Π_A

② if $\deg(A) \leq d$, $\exists \Pi_A$ s.t. $V_1(d)$ accepts.

③ if A far from every deg d poly, then $\forall \Pi_A$ $\Pr[V_1(d) \text{ accepts}] \leq \frac{1}{10}$

II Bivariate version
$B : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$

(fill in details yourselves later)

☺

Idea (of Semantics)

① $E : V \times V \to \{0,1\}$; Pick $\mathbb{F}$ s.t. $|\mathbb{F}| \geq c \cdot n$

$n = |V|$ & let $V \subseteq \mathbb{F}$

~~"Extend E to $\hat{E} : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ of deg $\leq (n,n)$~~

~~[$\hat{E}$ known to verifier]~~

② Ask for $\chi : V \longrightarrow \{0,1,2\}$ s.t.

$\forall (\alpha,\beta) \in V \times V$ at least one of the following holds

$$E(\alpha,\beta) = 0$$

or $\chi(\alpha) - \chi(\beta) = -2$

or " $= -1$

or $= 1$

or $= 2$

~~Con~~ Arithemetization

verifier knows

① $E \xrightarrow[\mathbb{F} \text{ with } V \subseteq \mathbb{F}]{\text{Pick large enough}} \hat{E} : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$

$\mathbb{F} = \Theta(n)$ suffices

s.t. $\hat{E}(\alpha, \beta) = E(\alpha, \beta)$

$\forall (\alpha, \beta) \in V \times V$

$d(\hat{E}) \leq (n, n)$.

---

② $x \longrightarrow \hat{x} : \mathbb{F} \to \mathbb{F}$

of degree $\leq n$.

---

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

① x is a 3-coloring

$$\hat{x}(\alpha) \cdot (\hat{x}(\alpha) - 1) \cdot (\hat{x}(\alpha) - 2) = 0 \quad \forall \alpha \in V$$

② x is valid for E

$$\hat{E}(\alpha, \beta) \cdot \prod_{i \in \{-2,-1,1,2\}} (\hat{x}(\alpha) - \hat{x}(\beta) - i) = 0 \quad \forall \alpha, \beta \in V$$

3-Coloring?

V asks for

- $A_1 = \hat{\chi} : \mathbb{F} \to \mathbb{F}$
- $A_2 = \chi(z) \cdot (\chi(z) - 1) \cdot (\chi(z) - 2)$ with proof that it has $\deg \leq 3n$

[Can check consistency easily

just ~~pick~~ check $A_2(\alpha) = A_1(\alpha) \cdot (A_1(\alpha) - 1) \cdot (A_1(\alpha) - 2)$

for random α

(POWER OF POLYNOMIALS)]

But still need to check $A_2(\alpha) = 0 \;\; \forall\, \alpha \in V$.

how can we do this?

Proving A_2 is ZERO on V

Idea: Use Fact 3 on Page 3

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

$$\left[Z_V(x) = \prod_{\alpha \in V} (x-\alpha) \right]$$

Prover writes

A_1

A_2

A_3

& proof ~~for~~ Π_{A_1} ← for syntactic check.

Π_{A_2}

Π_{A_3}

Verifier: ① Syntactic Checks

② $A_2(\alpha) = A_1(\alpha) \cdot (A_1(\alpha) - 1) \cdot (A_1(\alpha) - 2)$

for random α

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

Valid 3-Coloring:

1. $B_1(x,y) \triangleq \hat{E}(x,y) \cdot \prod_i (A_1(x) - A_1(y) - i)$
2. B_2, B_3 (based on Fact 4 on Page 3)

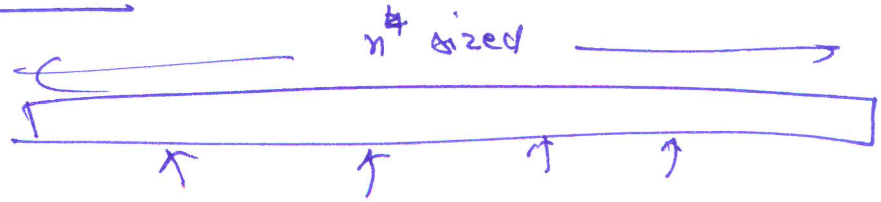
Verifier Checks

1. Syntactic Checks on B_1, B_2, B_3
2. $B_1(\alpha,\beta) = \hat{E}(\alpha,\beta) \cdot \prod_i (A_1(\alpha) - A_1(\beta) - i)$ for random (α,β)
3. $B_1(\alpha,\beta) = Z_V(\alpha) \cdot B_2(\alpha,\beta) + Z_V(\beta) \cdot B_3(\alpha,\beta)$ for random (α,β).

$\boxed{\text{QED}}$

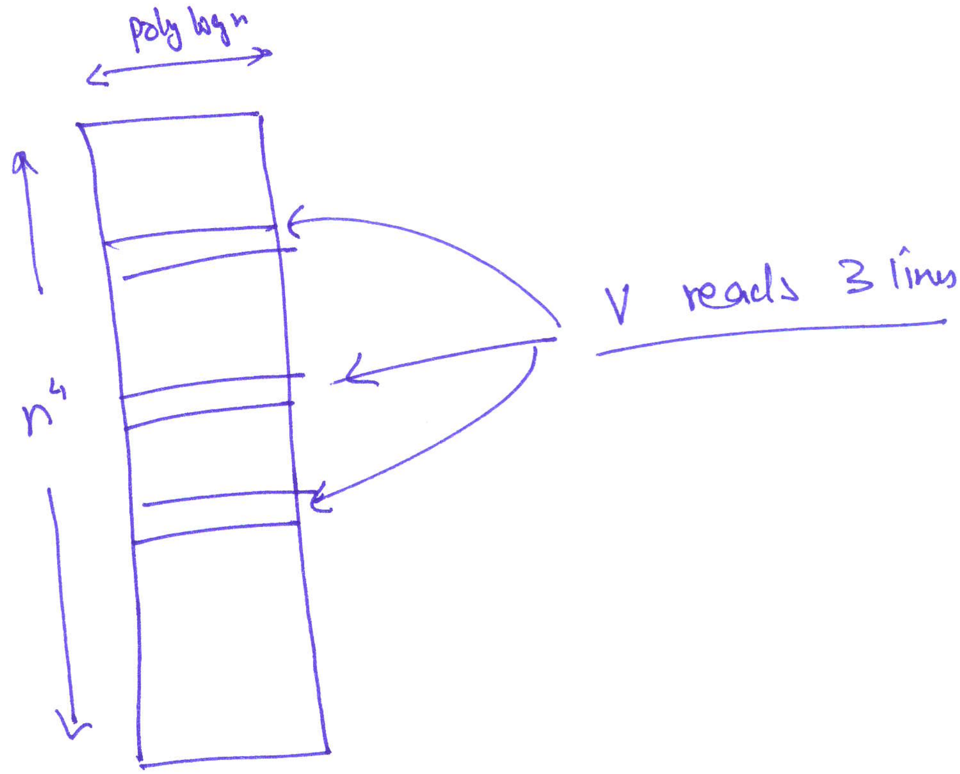
Getting O(1) queries

Current Proof:



Verifier reads $O(\text{polylog}\, n)$ pieces

With lots of work:



Then: Some recursion & some new ideas .....

State-of-the-art

- Three ~~parameters~~ constants (a, b, q)

  ① $\ell(n) = n^{a}$

  ② Error $= 1 - \frac{1}{b}$ [Prob. of accepting incorrect proof]

  ③ Query $= q$

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

- Can we achieve these simultaneously?

  Many interesting steps
  - [Polishchuk Spielman] $a = 1 + \epsilon$
  - [Hastad] : $(b, q) = (2 + o(1), 3)$
  - [Moshkovitz, Raz] : $(a, b, q) = (1 + o(1), 2 + o(1), 3)$

$\boxtimes$

Real Question : Can they be as good as ECC?

linear blowup?