Lecture 14

Foundations of Probabilistic Proofs
Fall 2020
Alessandro Chiesa

PCP for NTIME

We have constructed PCPs for NP and NEXP:

$$NP \subseteq PCP[\varepsilon_c = 0, \varepsilon_s = 0.5, \Sigma = \{0,1\}, \ell = \exp(n), q = O(1), r = \mathrm{poly}(n)]$$

$$NP \subseteq PCP[\varepsilon_c = 0, \varepsilon_s = 0.5, \Sigma = \{0,1\}, \ell = \mathrm{poly}(n), q = \mathrm{poly}(\log n), r = O(\log n)] \quad \blacktriangle$$

$$NEXP \subseteq PCP[\varepsilon_c = 0, \varepsilon_s = 0.5, \Sigma = \{0,1\}, \ell = \exp(n), q = \mathrm{poly}(n), r = \mathrm{poly}(n)] \quad \bullet$$

Today we construct a PCP for NTIME:

<u>theorem</u>: For every time function $T: \mathbb{N} \to \mathbb{N}$ with $T(n) = \Omega(n)$,

$$NTIME(T) \subseteq PCP\begin{bmatrix} \varepsilon_c = 0, \varepsilon_s = 0.5, \Sigma = \{0,1\}, pt = \mathrm{poly}(T), vt = \mathrm{poly}(n, \log T) \\ \ell = \mathrm{poly}(T), q = \mathrm{poly}(\log T), r = \mathrm{poly}(\log T) \end{bmatrix}$$

If we set $T = \mathrm{poly}(n)$ then we get $\blacktriangle$.

If we set $T = \exp(n)$ then we get $\bullet$.

More generally, the theorem shows that the time complexity of the PCP prover and PCP verifier can "scale gracefully" with the (non-deterministic) complexity of the language.

Let's revisit ideas from last time to see what we can recycle.

An NTIME-Complete Problem

def: $\text{OSAT} := \left\{ (m,n,\phi,z) \;\middle|\; \begin{array}{l} m,n \in \mathbb{N} \text{ and } \phi: \{0,1\}^{m+3n+3} \to \{0,1\} \text{ is a boolean formula s.t.} \\ \exists A: \{0,1\}^n \to \{0,1\} \text{ for which } A|_{\{0,1\}^{\log|z|} \times 0^{n-\log|z|}} \equiv z \text{ and} \\ \forall w \in \{0,1\}^m \; \forall v_1,v_2,v_3 \in \{0,1\}^n \;\; \phi(w,v_1,v_2,v_3,A(v_1),A(v_2),A(v_3)) = 0 \end{array} \right\}.$

We argue that OSAT is NTIME(T)-complete under poly(|x|, log T)-time reductions.

claim: For every language $L \in \text{NTIME}(T)$ there is a poly(|x|, log T)-time algorithm R s.t. $\forall x$:

① $R(x)$ outputs an OSAT instance (m,n,ϕ,z) with $m,n = O(\log T)$ and $|\phi| = \text{poly}(\log T)$

② $x \in L$ iff $R(x) \in \text{OSAT}$

proof: Analogous to proof that OSAT is NEXP-complete under poly(n)-time reductions, but we need to explicitly keep track of computation size & separate out the input.

Apply Cook-Levin Theorem to a T-time non-deterministic machine M that decides L on input x, to obtain a poly(log T)-size circuit D s.t., for $n := O(\log T)$, $x \in L$ iff $\exists A: \{0,1\}^n \to \{0,1\}$ s.t.

(i) $A|_{\{0,1\}^{\log|x|} \times 0^{n-\log|x|}} \equiv x$ (ii) $\forall v_1,v_2,v_3 \in \{0,1\}^n \; \forall c_1,c_2,c_3 \in \{0,1\} \; D(v_1,v_2,v_3,c_1,c_2,c_3) \wedge \left(\overline{\bigvee_{i=1}^{3} A(v_i) \oplus c_i} \right) = 0$

Then apply Cook-Levin Theorem to D to get poly(|D|)-size formula ψ and then set
$\phi(w,v_1,v_2,v_3,a_1,a_2,a_3) := \psi(w',v_1,v_2,v_3,c_1,c_2,c_3) \wedge \left(\overline{\bigvee_{i=1}^{3} a_i \oplus c_i} \right)$ where $w = (w',c_1,c_2,c_3) \in \{0,1\}^m$ and $m := m'+3$.

Problem with PCP for NEXP

Here is the PCP for NEXP from last time →

$P((m,n,\phi),A)$

1. Output $\Pi_A : \mathbb{F}^n \to \mathbb{F}$ that equals the multilinear extension of $A : \{0,1\}^n \to \{0,1\}$
2. For every $r_1,\dots,r_n \in \mathbb{F}$: output sumcheck proof $\Pi_{SC}^{(1)}[r_1,\dots,r_n]$ for $\sum_{a_1,\dots,a_n \in \{0,1\}} \Pi_A(a)(1-\Pi_A(a)) \prod_{i\in[n]} \hat{r}_i(a_i) = 0$
3. For every $r_1,\dots,r_{m+3n} \in \mathbb{F}$: output sumcheck proof $\Pi_{SC}^{(2)}[r_1,\dots,r_{m+3n}]$ for $\sum_{\substack{a=(w,v_1,v_2,v_3)\\ \in \{0,1\}^{m+3n}}} \hat{\phi}(w,v_1,v_2,v_3,\Pi_A(v_1)\Pi_A(v_2),\Pi_A(v_3)) \prod_{i\in[m+3n]} \hat{r}_i(a_i) = 0$

Π_A ← 2., 3.; ↑…↑ 4.

$\Pi_{SC}^{(1)}[r_1,\dots,r_n]$, $r_1,\dots,r_n \in \mathbb{F}$ ⇄ $V_{SC}(\mathbb{F},\{0,1\},n,0)$

$\Pi_{SC}^{(2)}[r_1,\dots,r_{m+3n}]$, $r_1,\dots,r_{m+3n} \in \mathbb{F}$ ⇄ $V_{SC}(\mathbb{F},\{0,1\},m+3n,0)$

$V((m,n,\phi))$

1. Compute $\hat{\phi} := T(\mathbb{F},(m,n,\phi))$ for $\mathbb{F}$ of size $\mathrm{poly}(|\phi|)$
2. Sample $r_1,\dots,r_n \in \mathbb{F}$ & run sumcheck for claim
$$\sum_{a_1,\dots,a_n \in \{0,1\}^n} \Pi_A(a)(1-\Pi_A(a)) \prod_{i\in[n]} \hat{r}_i(a_i) = 0$$
$V_{SC}(\mathbb{F},\{0,1\},n,0)$ → $(s_1,\dots,s_n)$
   - query Π_A at $(s_1,\dots,s_n)$
   - for $i=1,\dots,n$: eval $\hat{r}_i(x)$ at s_i
3. Sample $r_1,\dots,r_{m+3n} \in \mathbb{F}$ & run sumcheck for claim:
$$\sum_{\substack{a=(w,v_1,v_2,v_3)\\ \in \{0,1\}^{m+3n}}} \hat{\phi}(w,v_1,v_2,v_3,\Pi_A(v_1)\Pi_A(v_2),\Pi_A(v_3)) \prod_{i\in[m+3n]} \hat{r}_i(a_i) = 0$$
$V_{SC}(\mathbb{F},\{0,1\},m+3n,0)$ → $(s_1,\dots,s_{m+3n})$
   - query Π_A at $(s_{m+1},\dots,s_{m+n}),(s_{m+n+1},\dots,s_{m+2n}),(s_{m+2n+1},\dots,s_{m+3n})$
   - for $i=1,\dots,m+3n$: eval $\hat{r}_i(x)$ at s_i
   - evaluate $\hat{\phi}$ at (s,ans_1,ans_2,ans_3)
4. low-degree test Π_A for total degree n [poly(n) queries]

1. explicit input

Instances of OSAT now contain an explicit input: (m,n,ϕ,z).

So: ⓐ arithmetization of OSAT has to be adapted

ⓑ the PCP verifier will need an extra check for input consistency

2. PCP string is too long

$$|\Pi| \geq |\mathbb{F}|^n \geq n^n = (2^n)^{\log n} = \left(2^{O(\log T)}\right)^{\log\log T + O(1)} = \mathrm{poly}(T)^{\log\log T + O(1)}$$ ← super-polynomial

Part 1: Arithmetization of OSAT

claim: there is a transformation T s.t.

① $T(\mathbb{F}, H, (m,n,\phi))$ runs in $\text{poly}(|\phi|, |H|, \log|\mathbb{F}|)$-time and outputs an circuit $C : \mathbb{F}^{\bar{m}+3\bar{n}+3} \to \mathbb{F}$ of size & total degree $\text{poly}(|\phi|, |H|)$, with $\bar{m} := \frac{m}{\log|H|}$ and $\bar{n} := \frac{n}{\log|H|}$

② $(m,n,\phi,z) \in \text{OSAT}$ iff $\exists\, \hat{A} : \mathbb{F}^{\bar{n}} \to \mathbb{F}$ of individual degree $< |H|$ s.t.

i) $\hat{A}$ is boolean on $H^{\bar{n}}$ & equals z on $H^{\frac{\log|z|}{\log|H|}} \times 0^{\bar{n} - \frac{\log|z|}{\log|H|}}$

ii) $\forall w \in H^{\bar{m}}\ \forall v_1, v_2, v_3 \in H^{\bar{n}}\quad C(w, v_1, v_2, v_3, \hat{A}(v_1), \hat{A}(v_2), \hat{A}(v_3)) = 0$

proof:

We proved the case $H = \{0,1\}$ (where $\bar{m} = m$, $\bar{n} = n$, and $\hat{A}$ is multilinear) and no input consistency, by setting $C := \hat{\phi}$ where $\hat{\phi} := \text{arithmetize}(\mathbb{F}, \phi)$. $[x \wedge y \mapsto x \cdot y,\ x \vee y \mapsto 1-(1-x)(1-y),\ \bar{x} \mapsto 1-x]$

This is not enough when $H \neq \{0,1\}$:

$\hat{\phi}$ works on boolean inputs but C receives tuples of elements from H.

Idea: convert from H to boolean via additional circuits

Let $\text{bin} : H \to \{0,1\}^{\log|H|}$ be an efficiently computable bijection.

Define:
- $p_{H,i} : H \to \{0,1\}$ is the i-th bit function $p_{H,i}(a) := \text{bin}(a)_i$
- $\hat{p}_{H,i} : \mathbb{F} \to \mathbb{F}$ is the low-degree extension of $p_{H,i}$

Note that $\deg(\hat{p}_{H,i}) < |H|$ and $\hat{p}_{H,i}$ can be evaluated in $\text{poly}(|H|)$ field operations.

Part 1: Arithmetization of OSAT [2/2]

claim: there is a transformation T s.t.

① $T(\mathbb{F}, H, (m,n,\phi))$ runs in $\mathrm{poly}(|\phi|, |H|, \log|\mathbb{F}|)$-time and outputs an circuit $C : \mathbb{F}^{\bar{m}+3\bar{n}+3} \to \mathbb{F}$ of size & total degree $\mathrm{poly}(|\phi|, |H|)$, with $\bar{m} := \frac{m}{\log|H|}$ and $\bar{n} := \frac{n}{\log|H|}$

② $(m,n,\phi,z) \in \mathrm{OSAT}$ iff $\exists \hat{A} : \mathbb{F}^{\bar{n}} \to \mathbb{F}$ of individual degree $<|H|$ s.t.

i) $\hat{A}$ is boolean on $H^{\bar{n}}$ & equals z on $H^{\frac{\log|z|}{\log|H|}} \times 0^{\bar{n} - \frac{\log|z|}{\log|H|}}$

ii) $\forall w \in H^{\bar{m}}\ \forall v_1, v_2, v_3 \in H^{\bar{n}}\quad C(w, v_1, v_2, v_3, \hat{A}(v_1), \hat{A}(v_2), \hat{A}(v_3)) = 0$

proof: [continued]

Define: • $p_{H,i} : H \to \{0,1\}$ is the i-th bit function $p_{H,i}(a) := \mathrm{bin}(a)_i$

• $\hat{p}_{H,i} : \mathbb{F} \to \mathbb{F}$ is the low-degree extension of $p_{H,i}$

The circuit we use is

$$C(w, v_1, v_2, v_3, a_1, a_2, a_3) := \hat{\phi}\left(\underbrace{\left(p_{H,i}(w[j])\right)_{\substack{i=1,\dots,\log|H| \\ j=1,\dots,\bar{m}}}}_{\text{bits of } w},\ \left(\underbrace{\left(p_{H,i}(v_k[j])\right)_{\substack{i=1,\dots,\log|H| \\ j=1,\dots,\bar{n}}}}_{\text{bits of } v_k}\right)_{k=1,2,3},\ a_1, a_2, a_3 \right)$$

The total degree of C is $\leq \deg_{tot}(\hat{\phi}) \cdot |H| \leq |\phi| \cdot |H| = \mathrm{poly}(|\phi|, |H|)$.

The size of C is also $\mathrm{poly}(|\phi|, |H|)$.

Completeness and soundness are similar to the case $H = \{0,1\}$, because by extracting bits we can "convert" from $H^{\bar{m}}$ & $H^{\bar{n}}$ to $\{0,1\}^m$ & $\{0,1\}^n$.

Part 2: Zero-on-Subcube Test

We have already solved this problem for any hypercube:

$f|_{H^n} \stackrel{?}{\equiv} 0$

$P(\mathbb{F}, H, n, f)$

For every $r_1, \ldots, r_n \in \mathbb{F}$:

output eval table $\Pi_{SC}[r_1, \ldots, r_n]$

of IP prover for sumcheck claim

$$\sum_{a_1,\ldots,a_n \in H} f(a_1,\ldots,a_n) \prod_{i \in [n]} \hat{r}_i(a_i) = 0$$

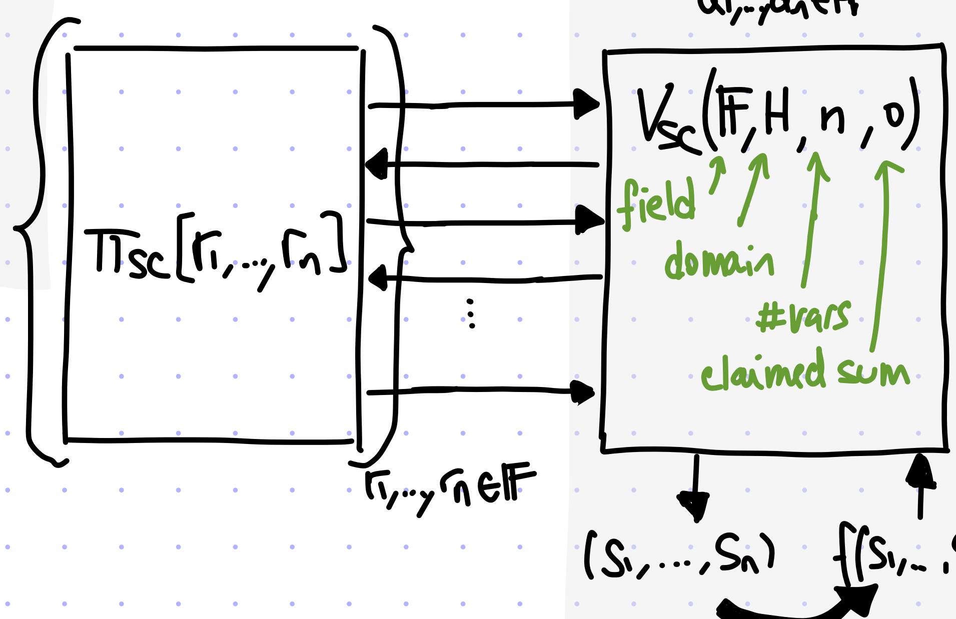
individual degree $\leq d$

$V^{f: \mathbb{F}^n \to \mathbb{F}}(\mathbb{F}, H, n)$

Sample $r_1, \ldots, r_n \in \mathbb{F}$.

Run sumcheck for the claim

$$\sum_{a_1,\ldots,a_n \in H} f(a_1,\ldots,a_n) \prod_{i \in [n]} \hat{r}_i(a_i) = 0$$



query complexity:
- $O(n \cdot (|H|+d))$ elts from Π_{SC}
- 1 elt from f

running time:
- $\mathrm{poly}(n, |H|, d)$ from V_{SC}
- $\mathrm{poly}(n, |H|)$ from

1. query f at $(s_1, \ldots, s_n)$
2. for $i = 1, \ldots, n$: evaluate $\hat{r}_i(x)$ at s_i

proof length:

$|\Pi_{SC}| = |\mathbb{F}|^n \cdot O(|\mathbb{F}|^n \cdot (|H|+d))$

$= |\mathbb{F}|^{O(n)} \cdot (|H|+d)$

Completeness error is 0. Soundness error is $O\left(\frac{n \cdot (|H|+d)}{|\mathbb{F}|}\right)$.

Part 3: Input Consistency Test

Given oracle access to $f: \mathbb{F}^n \to \mathbb{F}$ of individual degree d and input $z: H^k \to \mathbb{F}$ for $0 < k < n$, check that

$$f|_{H^k \times 0^{n-k}} \equiv z.$$

(Assume WLOG $0 \in H$.)

Let $\hat{z}: \mathbb{F}^k \to \mathbb{F}$ be the low-degree extension of z. (It has individual degree $< |H|$.)
Then add more variables trivially: $\hat{z}(x_1, \ldots, x_n) := \hat{z}(x_1, \ldots, x_k)$.
Note that $\hat{z}$ can be evaluated at any $(r_1, \ldots, r_n) \in \mathbb{F}^n$ in time $\mathrm{poly}(|H|^k)$ operations.

Now solve the following zero-on-subcube problem:

$$(f - \hat{z})|_{H^k \times 0^{n-k}} \equiv 0.$$

Putting the Parts Together

$P((m,n,\phi,z),A)$

0. Compute $C := T(\mathbb{F},H,(m,n,\phi))$

1. Output $\Pi_A : \mathbb{F}^{\bar{n}} \to \mathbb{F}$ that equals the $(\mathbb{F},H,\bar{n})$-extension of $A : \{0,1\}^n \to \{0,1\}$

2. For every $r_1,\dots,r_{\bar{n}} \in \mathbb{F}$:
   output sumcheck proof $\Pi_{SC}^{(1)}[r_1,\dots,r_{\bar{n}}]$
   for $\sum_{a \in H^{\bar{n}}} \Pi_A(a)(1-\Pi_A(a)) \prod_{i\in[\bar{n}]} \hat{r}_i(a_i) = 0$

3. For every $r_1,\dots,r_{\bar{m}+3\bar{n}} \in \mathbb{F}$:
   output sumcheck proof $\Pi_{SC}^{(2)}[r_1,\dots,r_{\bar{m}+3\bar{n}}]$
   for $\sum_{\substack{a=(w,v_1,v_2,v_3)\\ \in H^{\bar{m}+3\bar{n}}}} C(w,v_1,v_2,v_3,\Pi_A(v_1)\Pi_A(v_2),\Pi_A(v_3)) \prod_{i\in[\bar{m}+3\bar{n}]} \hat{r}_i(a_i) = 0$

[ignoring the consistency between Π_A and z. this is another zero on subcube test]

$\boxed{\Pi_A}$ ← 2., 3. ; ↑…↑ 4.

$\left\{ \boxed{\Pi_{SC}^{(1)}[r_1,\dots,r_{\bar{n}}]} \right\}_{r_1,\dots,r_{\bar{n}} \in \mathbb{F}}$ ⇄ ⋮ ⇄ $\boxed{V_{SC}(\mathbb{F},H,\bar{n},0)}$

$\left\{ \boxed{\Pi_{SC}^{(2)}[r_1,\dots,r_{\bar{m}+3\bar{n}}]} \right\}_{r_1,\dots,r_{\bar{m}+3\bar{n}} \in \mathbb{F}}$ ⇄ ⋮ ⇄ $\boxed{V_{SC}(\mathbb{F},H,\bar{m}+3\bar{n},0)}$

$V((m,n,\phi,z))$

1. Compute $C := T(\mathbb{F},H,(m,n,\phi))$

2. Sample $r_1,\dots,r_{\bar{n}} \in \mathbb{F}$ & run sumcheck for claim
   $$\sum_{a \in H^{\bar{n}}} \Pi_A(a)(1-\Pi_A(a)) \prod_{i\in[\bar{n}]} \hat{r}_i(a_i) = 0$$
   $\boxed{V_{SC}(\mathbb{F},H,\bar{n},0)}$ → $(s_1,\dots,s_{\bar{n}})$
   - query Π_A at $(s_1,\dots,s_{\bar{n}})$
   - for $i=1,\dots,\bar{n}$: eval $\hat{r}_i(x)$ at s_i

3. Sample $r_1,\dots,r_{\bar{m}+3\bar{n}} \in \mathbb{F}$ & run sumcheck for claim:
   $$\sum_{\substack{a=(w,v_1,v_2,v_3)\\ \in H^{\bar{m}+3\bar{n}}}} C(w,v_1,v_2,v_3,\Pi_A(v_1)\Pi_A(v_2),\Pi_A(v_3)) \prod_{i\in[\bar{m}+3\bar{n}]} \hat{r}_i(a_i) = 0$$
   $\boxed{V_{SC}(\mathbb{F},H,\bar{m}+3\bar{n},0)}$ → $(s_1,\dots,s_{\bar{m}+3\bar{n}})$
   - query Π_A at $(s_{\bar{m}+1},\dots,s_{\bar{m}+\bar{n}}),(s_{\bar{m}+\bar{n}+1},\dots,s_{\bar{m}+2\bar{n}}),(s_{\bar{m}+2\bar{n}+1},\dots,s_{\bar{m}+3\bar{n}})$
   - for $i=1,\dots,\bar{m}+3\bar{n}$: eval $\hat{r}_i(x)$ at s_i
   - evaluate C at (s,ans_1,ans_2,ans_3)

4. low-degree test Π_A for total degree $\bar{n}\cdot|H|$

Analysis

We wish to check that:

- $|\mathbb{F}| \overset{?}{=} \mathrm{poly}(|H|, |\phi|)$
- $|H| \overset{?}{=} \mathrm{poly}(|\phi|)$

make the protocol sound and efficient.

Recall that, reducing from NTIME:

$m, n \overset{?}{=} O(\log T)$, $|\phi| \overset{?}{=} \mathrm{poly}(\log T)$.

$P((m,n,\phi,z), A)$

0. Compute $C := T(\mathbb{F}, H, (m,n,\phi))$
1. Output $\Pi_A : \mathbb{F}^{\bar{n}} \to \mathbb{F}$ that equals the $(\mathbb{F}, H, \bar{n})$-extension of $A : \{0,1\}^n \to \{0,1\}$
2. For every $r_1, \dots, r_{\bar{n}} \in \mathbb{F}$: output sumcheck proof $\Pi_{SC}^{(1)}[r_1, \dots, r_{\bar{n}}]$ for $\sum_{a \in H^{\bar{n}}} \Pi_A(a)(1-\Pi_A(a)) \prod_{i \in [\bar{n}]} \hat{r}_i(a_i) = 0$
3. For every $r_1, \dots, r_{\bar{m}+3\bar{n}} \in \mathbb{F}$: output sumcheck proof $\Pi_{SC}^{(2)}[r_1, \dots, r_{\bar{m}+3\bar{n}}]$ for $\sum_{\substack{a=(w,v_1,v_2,v_3) \\ \in H^{\bar{m}+3\bar{n}}}} C(w,v_1,v_2,v_3,\Pi_A(v_1)\Pi_A(v_2),\Pi_A(v_3)) \prod_{i \in [\bar{m}+3\bar{n}]} \hat{r}_i(a_i) = 0$

$\boxed{\Pi_A}$ ← 2., 3., 4.

$\boxed{\Pi_{SC}^{(1)}[r_1, \dots, r_{\bar{n}}]}$ $\quad r_1, \dots, r_{\bar{n}} \in \mathbb{F}$

$\boxed{\Pi_{SC}^{(2)}[r_1, \dots, r_{\bar{m}+3\bar{n}}]}$ $\quad r_1, \dots, r_{\bar{m}+3\bar{n}} \in \mathbb{F}$

$V((m,n,\phi,z))$

1. Compute $C := T(\mathbb{F}, H, (m,n,\phi))$
2. Sample $r_1, \dots, r_{\bar{n}} \in \mathbb{F}$ & run sumcheck for claim
   $$\sum_{a \in H^{\bar{n}}} \Pi_A(a)(1-\Pi_A(a)) \prod_{i \in [\bar{n}]} \hat{r}_i(a_i) = 0$$
   $\boxed{V_{SC}(\mathbb{F}, H, \bar{n}, 0)}$ → $(s_1, \dots, s_{\bar{n}})$
   - query Π_A at $(s_1, \dots, s_{\bar{n}})$
   - for $i = 1, \dots, \bar{n}$: eval $\hat{r}_i(x)$ at s_i
3. Sample $r_1, \dots, r_{\bar{m}+3\bar{n}} \in \mathbb{F}$ & run sumcheck for claim:
   $$\sum_{\substack{a=(w,v_1,v_2,v_3) \\ \in H^{\bar{m}+3\bar{n}}}} C(w,v_1,v_2,v_3,\Pi_A(v_1)\Pi_A(v_2),\Pi_A(v_3)) \prod_{i \in [\bar{m}+3\bar{n}]} \hat{r}_i(a_i) = 0$$
   $\boxed{V_{SC}(\mathbb{F}, H, \bar{m}+3\bar{n}, 0)}$ → $(s_1, \dots, s_{\bar{m}+3\bar{n}})$
   - query Π_A at $(s_{\bar{m}+1}, \dots, s_{\bar{m}+\bar{n}}), (s_{\bar{m}+\bar{n}+1}, \dots, s_{\bar{m}+2\bar{n}}), (s_{\bar{m}+2\bar{n}+1}, \dots, s_{\bar{m}+3\bar{n}})$
   - for $i = 1, \dots, \bar{m}+3\bar{n}$: eval $\hat{r}_i(x)$ at s_i
   - evaluate C at (s, ans_1, ans_2, ans_3)
4. low-degree test Π_A for total degree $\bar{n} \cdot |H|$

- **soundness error:** $\varepsilon_{LDT}(\delta) + \delta + \dfrac{\mathrm{poly}(\bar{m}, \bar{n}, |H|, |\phi|)}{|\mathbb{F}|} \overset{?}{=} O(1)$

- **proof length:**
  $$|\Pi_A| + |\Pi_{SC}^{(1)}| + |\Pi_{SC}^{(2)}|$$
  $$= |\mathbb{F}|^{\bar{n}} + |\mathbb{F}|^{\bar{n}} \cdot O(|\mathbb{F}|^{\bar{n}} \cdot |H|) + |\mathbb{F}|^{\bar{m}+3\bar{n}} \cdot O(|\mathbb{F}|^{\bar{m}+3\bar{n}} \cdot |H| \cdot |\phi|)$$
  $$= |\mathbb{F}|^{O(\bar{m}+\bar{n})} |H| \cdot |\phi| = |\mathbb{F}|^{O\left(\frac{m+n}{\log|H|}\right)} \cdot |H| \cdot |\phi|$$
  $$\overset{?}{=} \mathrm{poly}(|H|, |\phi|)^{O\left(\frac{m+n}{\log|H|}\right)} \overset{?}{=} 2^{O(m+n)}$$
  $$\overset{?}{=} 2^{O(\log T)} = \mathrm{poly}(T)$$

- **query complexity**
  $$O(1) + \bar{n} \cdot |H| + (\bar{m} + 3\bar{n}) \cdot |\phi| \cdot |H| + q_{LDT}$$
  $$= O((m+n) \cdot |\phi| \cdot |H|)$$
  $$\overset{?}{=} \mathrm{poly}(|\phi|)$$
  $$\overset{?}{=} \mathrm{poly}(\log T)$$

- **verifier time**
  $$\mathrm{poly}(|\phi|, |H|) + t_{LDT} + \mathrm{poly}(|z|, |H|)$$
  $$\overset{?}{=} \mathrm{poly}(|\phi|, |z|)$$
  $$\overset{?}{=} \mathrm{poly}(|x|, \log T)$$

More on Proof Length

The proof length in the PCP for NTIME(T) described so far is at least T^6.
Let's see why:

$$|\pi_A| + |\pi_{SC}^{(1)}| + |\pi_{SC}^{(2)}| = |\mathbb{F}|^{\bar{n}} + |\mathbb{F}|^{\bar{n}} \cdot O(|\mathbb{F}|^{\bar{n}} \cdot |H|) + |\mathbb{F}|^{\bar{m}+3\bar{n}} \cdot O(|\mathbb{F}|^{\bar{m}+3\bar{n}} \cdot |H| \cdot |\phi|) \geq |\mathbb{F}|^{6\bar{n}} \geq |H|^{6 \frac{\log T}{\log |H|}} = T^6$$

Here are the culprits:

1. The reduction from zero-on-subcube to sumcheck causes a quadratic blowup:
   to prove $f|_{H^n} \equiv 0$ the prover includes, for every choice of randomness $r \in \mathbb{F}^n$, a sumcheck proof $\pi_{SC}[r]$ of size at least $|\mathbb{F}|^n$
2. The reduction from NTIME(T) to OSAT causes a cubic blowup:
   there are $\Omega(T)$ variables in the computation trace of the machine and we consider all possible 3CNF clauses formed by these

Intuitively, reducing proof length makes a PCP harder and harder to construct.

Fundamental question:

How short can a PCP be?

Trading Shorter Proof for More Queries

With several additional ideas, today's blueprint leads to this theorem:

<u>theorem</u>: For every time function $T:\mathbb{N}\to\mathbb{N}$ with $T(n)=\Omega(n)$ and $\forall\varepsilon>0$

$$\mathrm{NTIME}(T)\subseteq \mathrm{PCP}\begin{bmatrix}\varepsilon_c=0,\ \varepsilon_s=0.5,\ \Sigma=\{0,1\},\ pt=\mathrm{poly}_\varepsilon(T),\ vt=\mathrm{poly}_\varepsilon(n,\log T)\\ \ell=T^{1+O(\varepsilon)},\ q=(\log T)^{\frac{1}{\varepsilon}},\ r=\mathrm{poly}_{1/\varepsilon}(\log T)\end{bmatrix}$$

Each of the two culprits can be eliminated:

1. Use an alternate reduction from zero-on-subcube to sumcheck:

<u>lemma</u>: Let $Z_H(X):=\prod_{a\in H}(X-a)$ be the vanishing polynomial of H, and let $f:\mathbb{F}^n\to\mathbb{F}$ be a polynomial of individual degree $\leq d$. Then $f|_{H^n}\equiv 0$ iff $\exists\, g_1,\dots,g_n:\mathbb{F}^n\to\mathbb{F}$ of individual degree $\leq d$ s.t.

$$f(X_1,\dots,X_n)\equiv\sum_{i\in[n]} Z_H(X_i)\,g_i(X_1,\dots,X_n)$$

2. Use routing techniques to reduce $\mathrm{NTIME}(T)$ to a smaller zero-on-subcube problem:

$$\text{“}\ \forall w\in\{0,1\}^m\quad \phi(w,\phi_1(w),\phi_2(w),\phi_3(w),A(\phi_1(w)),A(\phi_2(w)),A(\phi_3(w)))=0\ \text{”}$$