Foundations of Probabilistic Proofs

A course by **Alessandro Chiesa**

Lecture 12

PCP for NTIME

PCP for NTIME

We have constructed PCPs for NP and NEXP:

$$NP \subseteq PCP\left[\varepsilon_c=0,\ \varepsilon_s=\tfrac{1}{2},\ \Sigma=\{0,1\},\ \ell=\exp(n),\ q=O(1),\ r=\mathrm{poly}(n)\right]$$

$$NP \subseteq PCP\left[\varepsilon_c=0,\ \varepsilon_s=\tfrac{1}{2},\ \Sigma=\{0,1\},\ \ell=\mathrm{poly}(n),\ q=\mathrm{poly}(\log n),\ r=O(\log n)\right] \quad ▲$$

$$NEXP \subseteq PCP\left[\varepsilon_c=0,\ \varepsilon_s=\tfrac{1}{2},\ \Sigma=\{0,1\},\ \ell=\exp(n),\ q=\mathrm{poly}(n),\ r=\mathrm{poly}(n)\right] \quad ●$$

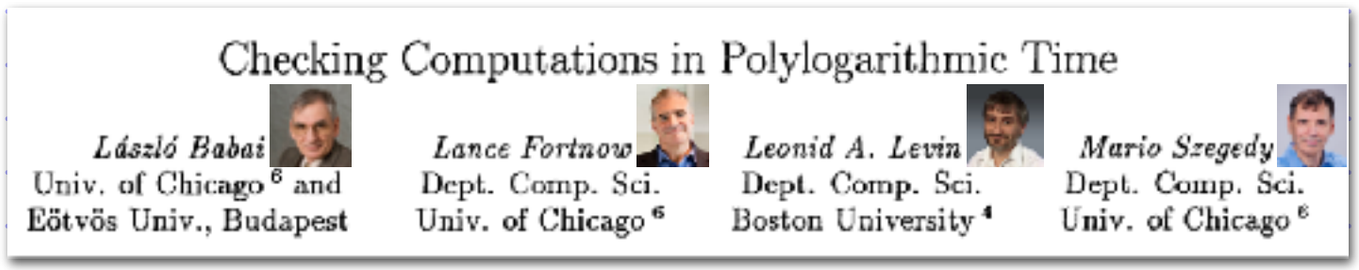
Today we construct a PCP for NTIME:

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

$$NTIME(T) \subseteq PCP\left[\begin{array}{llll}\varepsilon_c=0, & \Sigma=\{0,1\}, & \ell=\mathrm{poly}(T), & pt=\mathrm{poly}(T)\\ \varepsilon_s=\frac{1}{2}, & q=\mathrm{poly}(\log T), & r=O(\log T), & vt=\mathrm{poly}(n,\log T)\end{array}\right]$$

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

If we set $T=\exp(n)$ then we get ●.


Checking Computations in Polylogarithmic Time

László Babai, Univ. of Chicago [6] and Eötvös Univ., Budapest

Lance Fortnow, Dept. Comp. Sci. Univ. of Chicago [6]

Leonid A. Levin, Dept. Comp. Sci. Boston University [4]

Mario Szegedy, Dept. Comp. Sci. Univ. of Chicago [6]

More generally: the time complexities of the PCP prover and PCP verifier "scale gracefully" with the (non-deterministic) time complexity of the language.

This is a seminal result: DELEGATION OF COMPUTATION VIA PCPs.

Recycle the PCP for OSAT?

We can reduce from NTIME(T) to OSAT:

def: $$\text{OSAT} := \left\{ (m,n,\varphi) \;\middle|\; \begin{array}{l} m,n \in \mathbb{N},\ \varphi:\{0,1\}^{m+3n+3} \to \{0,1\} \text{ boolean formula} \\ \exists\, A:\{0,1\}^n \to \{0,1\}\ \ \forall w \in \{0,1\}^m\ \forall v_1,v_2,v_3 \in \{0,1\}^n\ \ \varphi(w,v_1,v_2,v_3,A(v_1),A(v_2),A(v_3)) = 0 \end{array} \right\}.$$

claim: $\forall L \in \text{NTIME}(T)$ $\exists$ poly$(|x|,\log T)$-time reduction R from L to OSAT $(x \in L \leftrightarrow R(x) \in \text{OSAT})$ s.t. $R(x)$ outputs an OSAT instance (m,n,φ) with $n = O(\log T)$, $m = \text{poly}(\log T)$, $|\varphi| = \text{poly}(|x|,\log T)$.

The proof is by keeping track of x and T in the proof of NEXP hardness for OSAT.

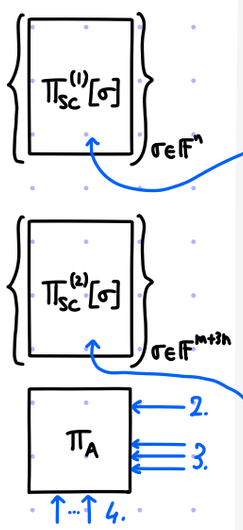
$P((m,n,\varphi),A)$

1. Compute $\hat{\varphi} := T(\mathbb{F},(m,n,\varphi))$.
2. For every $\sigma \in \mathbb{F}^n$:

   output sumcheck proof $\pi_{sc}^{(1)}[\sigma]$ for $\sum_{a\in\{0,1\}^n} \hat{A}(a)\cdot(\hat{A}(a)-1)\cdot\prod_{i\in[n]}\hat{\sigma}_i(a_i) = 0$.
3. For every $\sigma \in \mathbb{F}^{m+3n}$:

   output sumcheck proof $\pi_{sc}^{(2)}[\sigma]$ for $\sum_{a=(w,v_1,v_2,v_3)\in\{0,1\}^{m+3n}} \hat{\varphi}(w,v_1,v_2,v_3,\hat{A}(v_1),\hat{A}(v_2),\hat{A}(v_3))\cdot\prod_{i\in[m+3n]}\hat{\sigma}_i(q_i) = 0$
4. Output $\hat{A}:\mathbb{F}^n \to \mathbb{F}$ as π_A.

(The multilinear extension of $A:\{0,1\}^n \to \{0,1\}$.)



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

1. Compute $\hat{\varphi} := T(\mathbb{F},(m,n,\varphi))$.
2. Sample $\sigma \in \mathbb{F}^n$ and run sumcheck for $\sum_{a\in\{0,1\}^n} \hat{A}(a)\cdot(\hat{A}(a)-1)\cdot\prod_{i\in[n]}\hat{\sigma}_i(a_i) = 0$.

   $V_{sc}(\mathbb{F}, \{0,1\}, n, 0, 3)$ (field, domain, vars, sum, degree)

   $(g_1,\dots,g_n)$ ⇨ • query π_A at $(g_1,\dots,g_n)$
   • for every $i\in[n]$: eval $\hat{\sigma}_i(x)$ at g_i
3. Sample $\sigma \in \mathbb{F}^{m+3n}$ and run sumcheck for $\sum_{a=(w,v_1,v_2,v_3)\in\{0,1\}^{m+3n}} \hat{\varphi}(w,v_1,v_2,v_3,\hat{A}(v_1),\hat{A}(v_2),\hat{A}(v_3))\cdot\prod_{i\in[m+3n]}\hat{\sigma}_i(q_i) = 0$

   $V_{sc}(\mathbb{F}, \{0,1\}, m+3n, 0, |\varphi|+1)$ (field, domain, vars, sum, degree)

   $(g_1,\dots,g_{m+3n})$ ⇨ • query π_A at $(g_{m+1},\dots,g_{m+n})$, $(g_{m+n+1},\dots,g_{m+2n})$, $(g_{m+2n+1},\dots,g_{m+3n})$
   • for every $i\in[m+3n]$: eval $\hat{\sigma}_i$ at g_i
   • eval $\hat{\varphi}$ at $(g_1,\dots,g_{m+3n},\text{ans}_1,\text{ans}_2,\text{ans}_3)$
4. $V_{LDT}^{\pi_A}(\mathbb{F}, n, \text{ind} \le 1)$ (vars, degree)

PCP for OSAT from previous lecture

PROBLEM: PCP is too long

For soundness $O(1)$, we need $|\mathbb{F}| \ge (m+3n)\cdot|\varphi|$ (at minimum).

Hence

$$|\pi| = |\pi_A| + |\pi_{sc}^{(1)}| + |\pi_{sc}^{(2)}|$$
$$= |\mathbb{F}|^n + |\mathbb{F}|^n \cdot O(|\mathbb{F}|^n \cdot 1) + |\mathbb{F}|^{m+3n} \cdot O(|\mathbb{F}|^{m+3n}\cdot|\varphi|)$$
$$\ge |\mathbb{F}|^{m+n} \ge ((m+n)|\varphi|)^{m+n} \ge ((m+n)\cdot|x|)^{m+n}$$
$$\ge (|x|\cdot\log T)^{\text{poly}(\log T)}.$$

SUPER-POLYNOMIAL!

An NTIME-Complete Problem [1/3]

We consider a variant of the OSAT problem:

$$\underline{\text{def:}}\ \text{IOSAT} := \left\{ (m,n,\varphi,z) \;\middle|\; \begin{array}{l} m\in\mathbb{N},\ n\in\mathbb{N},\ \varphi:\{0,1\}^{3n+6+m}\to\{0,1\} \text{ boolean formula} \\ \text{such that } \exists\, A:\{0,1\}^n\to\{0,1\},\ B:\{0,1\}^{3n+3}\to\{0,1\}^m \text{ s.t.} \\ \bullet\ A|_{\{0,1\}^{\log|z|}\times 0^{n-\log|z|}} \equiv z \\ \bullet\ \forall\, v_1,v_2,v_3\in\{0,1\}^n\ \forall\, c\in\{0,1\}^3\ \ \varphi(v_1,v_2,v_3,c,A(v_1),A(v_2),A(v_3),B(v_1,v_2,v_3,c))=0 \end{array} \right\}$$

We can reduce from NTIME(T) to IOSAT:

$$\underline{\text{claim:}}\ \forall\, L\in\text{NTIME}(T)\ \exists\ \text{poly}(|x|,\log T)\text{-time reduction } R \text{ from } L \text{ to IOSAT } (x\in L\leftrightarrow R(x)\in\text{IOSAT})$$

s.t. $R(x)$ outputs an IOSAT instance (m,n,φ,x) with $n=O(\log T)$ and $m,|\varphi|=\text{poly}(\log T)$.

Differences with OSAT:

- The explicit input enables reducing $|\varphi|$ from $\text{poly}(|x|,\log T)$ to $\text{poly}(\log T)$.
- The additional witness B enables reducing the number of constraints from $2^{m+3n}=2^{\text{poly}(\log T)}$ to $2^{3n+3}=2^{O(\log T)}=\text{poly}(T)$ at the cost of increasing witness size from $2^n=2^{O(\log T)}=\text{poly}(T)$ to $2^n+2^{3n+3}\cdot m=2^{O(\log T)}\cdot\text{poly}(\log T)=\text{poly}(T)$.

The reduction from NTIME(T) to IOSAT is similar to the reduction from NTIME(T) to OSAT.

An NTIME-Complete Problem [2/3]

claim: $\forall\, L \in \text{NTIME}(T)$ $\exists$ poly$(|x|, \log T)$-time reduction R from L to IOSAT ($x \in L \leftrightarrow R(x) \in \text{IOSAT}$) s.t. $R(x)$ outputs an IOSAT instance (m, n, φ, x) with $n = O(\log T)$ and $m, |\varphi| = \text{poly}(\log T)$.

proof: Suppose that $L \in \text{NTIME}(T)$ and let M be an NTIME(T) machine deciding L.

Let x be an input to M.

By the Cook-Levin Theorem, can reduce (M, x, T) to a 3CNF Φ s.t.

- Φ has $N_v = \text{poly}(T)$ variables (and $N_c = \text{poly}(T)$ clauses),
- $M(x) = 1 \leftrightarrow \exists\, A : [N_v] \to \{0,1\}$ $A(\{1, 2, \ldots, |x|\}) = x$ and $\Phi(A) = 1$.

Set $n = \log N_v = O(\log T)$, and relabel $[N_v]$ as $\{0,1\}^n$ and $[|x|]$ as $\{0,1\}^{\log|x|} \times 0^{n - \log|x|}$.

Moreover, $\exists$ poly$(\log T)$-size circuit $D : \{0,1\}^{3n+3} \to \{0,1\}$ that specifies Φ's clauses: (no polynomial dependence on $|x|$)

$D(v_1, v_2, v_3, c_1, c_2, c_3) = 1 \leftrightarrow \Phi$ contains clause $\bigvee_{i=1}^{3} (x_{v_i} \oplus c_i)$

Hence $\Phi(A) = 1 \leftrightarrow \forall\, v_1, v_2, v_3 \in \{0,1\}^n$ $\forall\, c_1, c_2, c_3 \in \{0,1\}$ $D(v_1, v_2, v_3, c_1, c_2, c_3) \wedge \overline{\left(\bigvee_{i=1}^{3} A(v_i) \oplus c_i \right)} = 0$.

Therefore, $M(x) = 1 \leftrightarrow \exists\, A : \{0,1\}^n \to \{0,1\}$ s.t.

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

An NTIME-Complete Problem [3/3]

claim: $\forall\, L \in \text{NTIME}(T)$ $\exists$ poly$(|x|, \log T)$-time reduction R from L to IOSAT $(x \in L \leftrightarrow R(x) \in \text{IOSAT})$ s.t. $R(x)$ outputs an IOSAT instance (m, n, φ, x) with $n = O(\log T)$ and $m, |\varphi| = \text{poly}(\log T)$.

proof: [continued]

Therefore, $M(x)=1 \leftrightarrow \exists\, A:\{0,1\}^n \to \{0,1\}$ s.t.

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

Reduce the boolean circuit D to a boolean formula $\psi:\{0,1\}^{3n+3+m} \to \{0,1\}$ with $m = O(|D|) = \text{poly}(\log T)$ and $|\psi| = O(|D|) = \text{poly}(\log T)$ s.t.

$\forall\, v_1, v_2, v_3 \in \{0,1\}^n$ $\forall\, c_1, c_2, c_3 \in \{0,1\}$ $D(v_1, v_2, v_3, c_1, c_2, c_3) = 1 \leftrightarrow \exists\, w \in \{0,1\}^m$ $\psi(v_1, v_2, v_3, c_1, c_2, c_3, w) = 1$.

Define $\varphi(v_1, v_2, v_3, c_1, c_2, c_3, a_1, a_2, a_3, w) := \psi(v_1, v_2, v_3, c_1, c_2, c_3, w) \wedge \overline{\left(\bigvee_{i=1}^{3} a_i \oplus c_i\right)}$.

In sum, $M(x)=1 \leftrightarrow \exists\, A:\{0,1\}^n \to \{0,1\}$ s.t.

- $A|_{\{0,1\}^{\log|x|} \times 0^{n-\log|x|}} \equiv x$
- $\forall\, v_1, v_2, v_3 \in \{0,1\}^n$ $\forall\, c_1, c_2, c_3 \in \{0,1\}$ $\exists\, w \in \{0,1\}^m$ $\varphi(v_1, v_2, v_3, c_1, c_2, c_3, A(v_1), A(v_2), A(v_3), w) = 0$.

Define $B:\{0,1\}^{3n} \times \{0,1\}^3 \to \{0,1\}$ as $B(v_1, v_2, v_3, c_1, c_2, c_3) :=$ "witness w for $D(v_1, v_2, v_3, c_1, c_2, c_3)$". ■

Part 1: Arithmetization of IOSAT [1/3]

$\bar{n} := \frac{n}{\log|H|}$

claim: There is a transformation T s.t.

① $T(\mathbb{F}, H, (m, n, \varphi))$ outputs in $\text{poly}(|\varphi|, |H|, \log|\mathbb{F}|)$-time a circuit $C : \mathbb{F}^{3\bar{n}+6+m} \to \mathbb{F}$ of size and total degree $\text{poly}(|\varphi|, |H|)$

② $(m, n, \varphi, z) \in \text{IOSAT}$ iff $\exists\, \hat{A} : \mathbb{F}^{\bar{n}} \to \mathbb{F}$, $\hat{B} : \mathbb{F}^{3\bar{n}+3} \to \mathbb{F}^m$ of individual degree $< |H|$ s.t.

- $\hat{A}$ is boolean on $H^{\bar{n}}$
- $\hat{B}$ is boolean on $H^{3\bar{n}+3}$
- $\hat{A}$ equals z on $H^{\frac{\log|2|}{\log|H|}} \times O^{\bar{n} - \frac{\log|2|}{\log|H|}}$
- $\forall\, v_1, v_2, v_3 \in H^{\bar{n}}\ \forall\, c \in H^3$ $C(v_1, v_2, v_3, c, \hat{A}(v_1), \hat{A}(v_2), \hat{A}(v_3), \hat{B}(v_1, v_2, v_3, c)) = 0$

We proved a similar statement when arithmetizing OSAT:

- we used $H = \{0,1\}$ (so $\hat{A}$ has $\bar{n} = n$ variables and is multilinear)
- we used $C := \hat{\varphi}$ where $\hat{\varphi} := \text{arithmetize}(\mathbb{F}, \varphi)$ $[x \wedge y \mapsto x \cdot y,\ x \vee y \mapsto 1-(1-x)\cdot(1-y),\ \overline{x} \mapsto 1-x]$
- no input consistency (z was "hardcoded" in φ)

The set H provides crucial flexibility (by allowing us to choose $|H| > 2$):

$|\mathbb{F}|^{\bar{n}} = |\mathbb{F}|^{\frac{n}{\log|H|}} = (2^n)^{\frac{\log|\mathbb{F}|}{\log|H|}} = |A|^{\frac{\log|\mathbb{F}|}{\log|H|}}$ ← if $|\mathbb{F}| = \text{poly}(|H|)$ then $|\hat{A}| = \text{poly}(|A|)$! (Ditto for $\hat{B}$ vs B.)

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

IDEA: convert from H to boolean via additional circuits.

Part 1: Arithmetization of IOSAT [2/3]

$\bar{n} := \frac{n}{\log|H|}$

claim: There is a transformation T s.t.

① $T(\mathbb{F}, H, (m, n, \varphi))$ outputs in $\mathrm{poly}(|\varphi|, |H|, \log|\mathbb{F}|)$-time a circuit $C : \mathbb{F}^{3\bar{n}+6+m} \to \mathbb{F}$ of size and total degree $\mathrm{poly}(|\varphi|, |H|)$

② $(m, n, \varphi, z) \in \mathrm{IOSAT}$ iff $\exists\, \hat{A} : \mathbb{F}^{\bar{n}} \to \mathbb{F}$, $\hat{B} : \mathbb{F}^{3\bar{n}+3} \to \mathbb{F}^m$ of individual degree $< |H|$ s.t.

- $\hat{A}$ is boolean on $H^{\bar{n}}$
- $\hat{B}$ is boolean on $H^{3\bar{n}+3}$
- $\hat{A}$ equals z on $H^{\frac{\log|2|}{\log|H|}} \times O^{\bar{n} - \frac{\log|2|}{\log|H|}}$
- $\forall\, v_1, v_2, v_3 \in H^{\bar{n}}\ \forall\, c \in H^3$ $C(v_1, v_2, v_3, c, \hat{A}(v_1), \hat{A}(v_2), \hat{A}(v_3), \hat{B}(v_1, v_2, v_3, c)) = 0$

proof:

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

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

$$\hat{p}_{H,i}(x) = \sum_{a \in H} p_{H,i}(a) \cdot L_{H,a}(x)$$

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

We can convert from $H^{\bar{n}}$ to $\{0,1\}^n$: $V \mapsto \left(\hat{p}_{H,i}(V[j])\right)_{\substack{i=1,\dots,\log|H| \\ j=1,\dots,\bar{n}}}$.

Part 1: Arithmetization of IOSAT [3/3]

$\bar{n} := \frac{n}{\log|H|}$

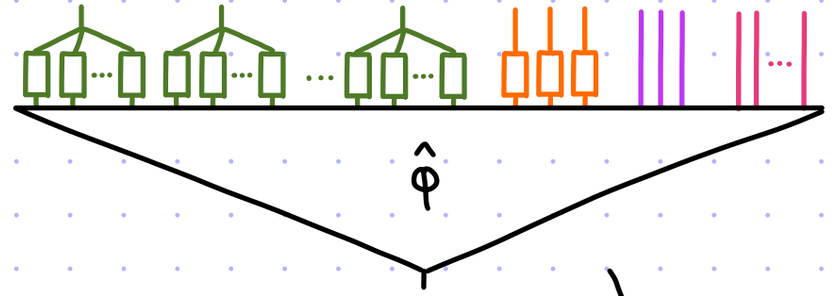
claim: There is a transformation T s.t.

① $T(\mathbb{F}, H, (m, n, \varphi))$ outputs in $\mathrm{poly}(|\varphi|, |H|, \log|\mathbb{F}|)$-time a circuit $C : \mathbb{F}^{3\bar{n}+6+m} \to \mathbb{F}$ of size and total degree $\mathrm{poly}(|\varphi|, |H|)$

② $(m, n, \varphi, z) \in \mathrm{IOSAT}$ iff $\exists\, \hat{A} : \mathbb{F}^{\bar{n}} \to \mathbb{F}$, $\hat{B} : \mathbb{F}^{3\bar{n}+3} \to \mathbb{F}^m$ of individual degree $< |H|$ s.t.

- $\hat{A}$ is boolean on $H^{\bar{n}}$
- $\hat{B}$ is boolean on $H^{3\bar{n}+3}$
- $\hat{A}$ equals z on $H^{\frac{|\log|z||}{\log|H|}} \times O^{\bar{n} - \frac{|\log|z||}{\log|H|}}$
- $\forall\, v_1, v_2, v_3 \in H^{\bar{n}}\ \forall\, c \in H^3$ $C(v_1, v_2, v_3, c, \hat{A}(v_1), \hat{A}(v_2), \hat{A}(v_3), \hat{B}(v_1, v_2, v_3, c)) = 0$

proof: [continued]



The circuit we use is

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

– total degree of C: $\deg_{tot}(\hat{\varphi}) \cdot (|H|-1) \leq |\varphi| \cdot |H| = \mathrm{poly}(|\varphi|, |H|)$.

– size of C: $|\varphi| + (3\bar{n} \cdot \log|H| + 3) \cdot \mathrm{poly}(|H|) = \mathrm{poly}(|\varphi|, |H|)$.

Completeness and soundness are established similarly to the case of the arithmetization of OSAT in the prior lecture. ■

Part 2: Zero-on-Subcube Test

We solved this problem in the previous lecture:

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

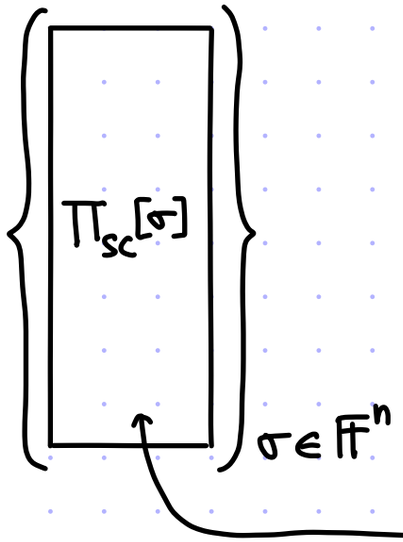
For every $\sigma_1, \ldots, \sigma_n \in \mathbb{F}$:

output eval table $\Pi_{sc}[\sigma_1, \ldots, \sigma_n]$ of

IP prover for sumcheck claim

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

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



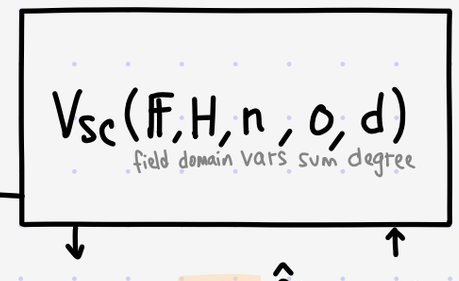
δ-close to $\hat{f} \in \mathbb{F}^{\leq d}[x_1, \ldots, x_n]$

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

Sample $\sigma_1, \ldots, \sigma_n \in \mathbb{F}$.

Run sumcheck for the claim:

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



1. Query f at $(\rho_1, \ldots, \rho_n)$.
2. For every $i \in [n]$: evaluate $\hat{\sigma_i}$ at ρ_i.

proof length: $|\Pi_{sc}| = |\mathbb{F}|^n \cdot O(|\mathbb{F}|^n \cdot (|H|+d)) = |\mathbb{F}|^{O(n)} \cdot (|H|+d)$

query complexity:

- n queries to Π_{sc} (each retrieving $|H|+d$ elts)
- 1 random query to f

verifier time: $\text{poly}(n, |H|, d)$ for $V_{sc} + n \cdot \text{poly}(|H|)$ to evaluate $\{\hat{\sigma_i}\}_{i \in [n]}$

COMPLETENESS: if $f \equiv \hat{f} \wedge \hat{f}|_{H^n} \equiv 0$ then, for $\pi := P(\mathbb{F}, H, n, f)$, $\Pr[V^{f,\pi}(\mathbb{F}, H, n, d) = 1] = 1$.

SOUNDNESS: if $\Delta(f, \hat{f}) < \delta \wedge \hat{f}|_{H^n} \not\equiv 0$ then $\forall \tilde{\pi}$ $\Pr[V^{f,\tilde{\pi}}(\mathbb{F}, H, n, d) = 1] \leq \frac{n \cdot (|H|-1+d)}{|\mathbb{F}|} + \delta$.

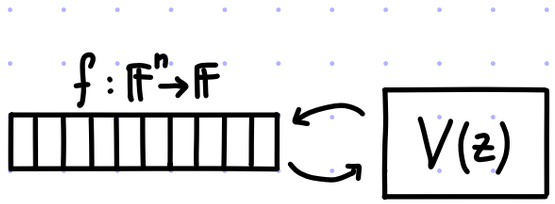
Part 3: Input Consistency Test [1/2]

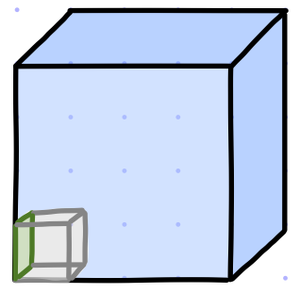
Given: • oracle access to $f: \mathbb{F}^n \to \mathbb{F}$ that is δ-close to $\hat{f}$ of individual degree d

• input $z: H^k \to \mathbb{F}$ with $0 < k \leq n$

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

(0^{n-k}: arbitrary element in H)





Idea #1: query f at every point in $H^k \times 0^{n-k}$ and compare to z

Problem: if even 1 corruption is in $H^k \times 0^{n-k}$ then test may accept even if $\hat{f}|_{H^k \times 0^{n-k}} \neq z$

→ test is not sound

Idea #2: locally correct the value of f at every point in $H^k \times 0^{n-k}$ (and compare to z)

This leads to $H^k \cdot q_{LC}$ queries and error $H^k \cdot \varepsilon_{LC}$ where

q_{LC} := "query complexity of local correction" and ε_{LC} := "error of local correction".

Minor Problem: query complexity grows with $|z|$

RECALL: local correction of f δ-close to $LD(\mathbb{F}, n, \text{ind} \leq d)$ has $q_{LC} = O(d)$ and $\varepsilon_{LC} = O(d \cdot \delta)$,
and by repeating t times and taking plurality we get $q'_{LC} = O(td)$ and $\varepsilon'_{LC} = \exp(-t \cdot (1 - d \cdot \delta))$.

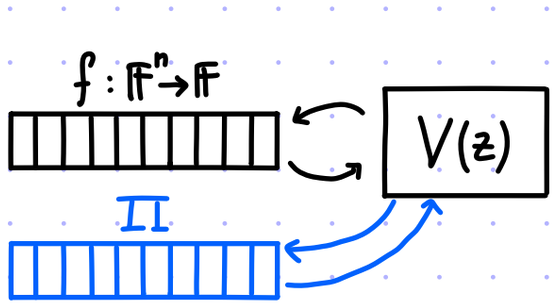
Part 3: Input Consistency Test [2/2]

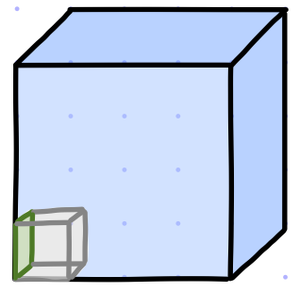
Given: • oracle access to $f: \mathbb{F}^n \to \mathbb{F}$ that is δ-close to $\hat{f}$ of individual degree d

• input $z: H^k \to \mathbb{F}$ with $0 < k \leq n$

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

arbitrary element in H





Idea #3: reduce to zero-on-subcube problem

Let $\hat{z}: \mathbb{F}^k \to \mathbb{F}$ be the low-degree extension of $z: H^k \to \mathbb{F}$.

Add $n-k$ dummy variables $\hat{z}_*(x_1, \ldots, x_n) := \hat{z}(x_1, \ldots, x_k)$.

Note that $\hat{z}_*$ can be evaluated at any point in $\mathbb{F}^n$ in $\text{poly}(|H|^k) = \text{poly}(|z|)$ time.

Rewrite as zero-on-subcube: $\hat{f}|_{H^k \times 0^{n-k}} \equiv z \iff (\hat{f} - \hat{z}_*)|_{H^k \times 0^{n-k}} \equiv 0$.

Crucially, the sumcheck approach to zero-on-subcube directly extends from domains of the form H^n to domains of the form $H_1 \times \cdots \times H_n$.

⟶ • proof length $|\mathbb{F}|^{O(n)}(|H|+d)$ • soundness error $\frac{n \cdot (|H|-1+d)}{|\mathbb{F}|} + \delta$

• query complexity $\text{poly}(n, |H|, d)$ • verifier time $\text{poly}(n, |H|, d) + \text{poly}(|z|)$

PCP for IOSAT: Putting the Parts Together

$P((m,n,\varphi,z),(A,B))$

1. Compute $C := T(\mathbb{F}, H, (m,n,\varphi))$.
2. $\forall \sigma \in \mathbb{F}^{\bar{n}}$ output sumcheck proof $\pi_{sc}^{(1)}[\sigma]$

   for $\sum_{a \in H^{\bar{n}}} \hat{A}(a) \cdot (\hat{A}(a)-1) \cdot \prod_{i \in [\bar{n}]} \hat{\sigma}_i(a_i) = 0$
3. $\forall \sigma \in \mathbb{F}^{3\bar{n}+3}$ output sumcheck proof $\pi_{sc}^{(2)}[\sigma]$

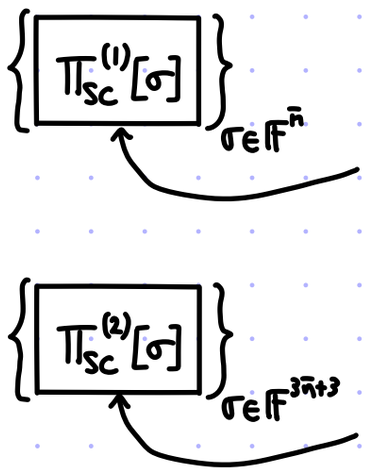
   for $\sum_{a \in H^{3\bar{n}+3}} \hat{B}(a) \cdot (\hat{B}(a)-1) \cdot \prod_{i \in [3\bar{n}+3]} \hat{\sigma}_i(a_i) = 0^m$
4. $\forall \sigma \in \mathbb{F}^{3\bar{n}+3}$ output sumcheck proof $\pi_{sc}^{(3)}[\sigma]$

   for $\sum_{a=(v_1,v_2,v_3,c) \in H^{3\bar{n}+3}} C(a, \hat{A}(v_1), \hat{A}(v_2), \hat{A}(v_3), \hat{B}(a)) \cdot \prod_{i \in [3\bar{n}+3]} \hat{\sigma}_i(q_i) = 0$
5. Output $\hat{A}: \mathbb{F}^{\bar{n}} \to \mathbb{F}$ as π_A.

   (The $(\mathbb{F}, H, \bar{n})$-extension of $A: \{0,1\}^n \to \{0,1\}$.)
6. Output $\hat{B}: \mathbb{F}^{3\bar{n}+3} \to \mathbb{F}^m$ as π_B.

   (The $(\mathbb{F}, H, 3\bar{n}+3)$-extension of $B: \{0,1\}^{3n+3} \to \{0,1\}^m$.)

[Omitted is consistency between π_A and z.
This is another zero-on-subcube test.]



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

1. Compute $C := T(\mathbb{F}, H, (m,n,\varphi))$.
2. Sample $\sigma \in \mathbb{F}^{\bar{n}}$ and run sumcheck

   $V_{sc}(\underset{\text{field}}{\mathbb{F}}, \underset{\text{domain}}{H}, \underset{\text{vars}}{\bar{n}}, \underset{\text{sum}}{0}, \underset{\text{degree}}{3 \cdot (|H|-1)})$ → $(\rho_1, \ldots, \rho_{\bar{n}})$

   ← $\pi_A(\rho) \cdot (\pi_A(\rho)-1) \cdot \prod_{i \in [\bar{n}]} \hat{\sigma}_i(\rho_i)$
3. Sample $\sigma \in \mathbb{F}^{3\bar{n}+3}$ and run sumcheck

   $V_{sc}(\underset{\text{field}}{\mathbb{F}}, \underset{\text{domain}}{H}, \underset{\text{vars}}{3\bar{n}+3}, \underset{\text{sum}}{0^m}, \underset{\text{degree}}{3 \cdot (|H|-1)})$ → $(\rho_1, \ldots, \rho_{3\bar{n}+3})$

   ← $\pi_B(\rho) \cdot (\pi_B(\rho)-1) \cdot \prod_{i \in [3\bar{n}+3]} \hat{\sigma}_i(\rho_i)$
4. Sample $\sigma \in \mathbb{F}^{3\bar{n}+3}$ and run sumcheck for

   $\sum_{a=(v_1,v_2,v_3,c) \in H^{3\bar{n}+3}} C(a, \hat{A}(v_1), \hat{A}(v_2), \hat{A}(v_3), \hat{B}(a)) \cdot \prod_{i \in [3\bar{n}+3]} \hat{\sigma}_i(q_i) = 0$

   $V_{sc}(\underset{\text{field}}{\mathbb{F}}, \underset{\text{domain}}{H}, \underset{\text{vars}}{3\bar{n}+3}, \underset{\text{sum}}{0}, \underset{\text{degree}}{(|\varphi|+1) \cdot (|H|-1)})$

   $(\rho_1, \ldots, \rho_{3\bar{n}+3})$ ⇨
   - query π_A at $(\rho_1, \ldots, \rho_{\bar{n}}), (\rho_{\bar{n}+1}, \ldots, \rho_{2\bar{n}}), (\rho_{2\bar{n}+1}, \ldots, \rho_{3\bar{n}})$
   - query π_B at $(\rho_1, \ldots, \rho_{3\bar{n}+3})$
   - for every $i \in [3\bar{n}+3]$: eval $\hat{\sigma}_i$ at ρ_i
   - eval C at $(\rho_1, \ldots, \rho_{3\bar{n}+3}, ans_1, ans_2, ans_3, ans_4)$
5. $V_{LDT}^{\pi_A}(\underset{\text{vars}}{\mathbb{F}, \bar{n}}, \underset{\text{degree}}{\text{ind} \le |H|-1})$
6. $V_{LDT}^{\pi_B}(\underset{\text{vars}}{\mathbb{F}, 3\bar{n}+3}, \underset{\text{outputs}}{m}, \underset{\text{degree}}{\text{ind} \le |H|-1})$

PCP for IOSAT: Analysis [1/2]

Setting $|\mathbb{F}| \doteq \text{poly}(|H|, |\varphi|)$, $|H| \doteq \text{poly}(|\varphi|)$ makes the protocol sound and efficient.

Recall that, reducing from NTIME(T), $n \doteq O(\log T)$ and $m, |\varphi| \doteq \text{poly}(\log T)$.

$P((m, n, \varphi, z), (A, B))$

1. Compute $C := T(\mathbb{F}, H, (m, n, \varphi))$.
2. $\forall \sigma \in \mathbb{F}^{\bar{n}}$ output sumcheck proof $\pi_{SC}^{(1)}[\sigma]$ for $\sum_{a \in H^{\bar{n}}} \hat{A}(a) \cdot (\hat{A}(a) - 1) \cdot \prod_{i \in [\bar{n}]} \hat{\sigma}_i(a_i) = 0$

$\left\{ \boxed{\pi_{SC}^{(1)}[\sigma]} \right\}_{\sigma \in \mathbb{F}^{\bar{n}}}$

3. $\forall \sigma \in \mathbb{F}^{3\bar{n}+3}$ output sumcheck proof $\pi_{SC}^{(2)}[\sigma]$ for $\sum_{a \in H^{3\bar{n}+3}} \hat{B}(a) \cdot (\hat{B}(a) - 1) \cdot \prod_{i \in [3\bar{n}+3]} \hat{\sigma}_i(a_i) = 0^m$

$\left\{ \boxed{\pi_{SC}^{(2)}[\sigma]} \right\}_{\sigma \in \mathbb{F}^{3\bar{n}+3}}$

4. $\forall \sigma \in \mathbb{F}^{3\bar{n}+3}$ output sumcheck proof $\pi_{SC}^{(3)}[\sigma]$ for $\sum_{a=(v_1, v_2, v_3, c) \in H^{3\bar{n}+3}} C(a, \hat{A}(v_1), \hat{A}(v_2), \hat{A}(v_3), \hat{B}(a)) \cdot \prod_{i \in [3\bar{n}+3]} \hat{\sigma}_i(a_i) = 0$

$\left\{ \boxed{\pi_{SC}^{(3)}[\sigma]} \right\}_{\sigma \in \mathbb{F}^{3\bar{n}+3}}$

5. Output $\hat{A} : \mathbb{F}^{\bar{n}} \to \mathbb{F}$ as π_A.

(The $(\mathbb{F}, H, \bar{n})$-extension of $A : \{0,1\}^n \to \{0,1\}$.)

$\boxed{\pi_A}$

6. Output $\hat{B} : \mathbb{F}^{3\bar{n}+3} \to \mathbb{F}^m$ as π_B.

(The $(\mathbb{F}, H, 3\bar{n}+3)$-extension of $B : \{0,1\}^{3n+3} \to \{0,1\}^m$.)

$\boxed{\pi_B}$

- proof length: (in field elements)

$$
\begin{aligned}
|\pi| &= |\pi_A| + |\pi_B| + |\pi_{SC}^{(1)}| + |\pi_{SC}^{(2)}| + |\pi_{SC}^{(3)}| + |\pi_{IC}| \\
&= |\mathbb{F}|^{\bar{n}} + |\mathbb{F}|^{3\bar{n}+3} \cdot m \\
&\quad + |\mathbb{F}|^{\bar{n}} \cdot O(|\mathbb{F}|^{\bar{n}} \cdot |H|) \\
&\quad + |\mathbb{F}|^{3\bar{n}+3} \cdot O(|\mathbb{F}|^{3\bar{n}+3} \cdot |H|) \cdot m \\
&\quad + |\mathbb{F}|^{3\bar{n}+3} \cdot O(|\mathbb{F}|^{3\bar{n}+3} \cdot |H| \cdot |\varphi|) \\
&\quad + |\mathbb{F}|^{\bar{n}} \cdot O(|\mathbb{F}|^{\bar{n}} \cdot |H|) \\
&= |\mathbb{F}|^{O(\bar{n})} \cdot |H| \cdot |\varphi| = |\mathbb{F}|^{O\left(\frac{n}{\log |H|}\right)} \cdot |H| \cdot |\varphi| \\
&\doteq \text{poly}(|H|, |\varphi|)^{O\left(\frac{n}{\log |H|}\right)} \\
&\doteq 2^{O(n)} \\
&\doteq 2^{O(\log T)} = \text{poly}(T).
\end{aligned}
$$

PCP for IOSAT: Analysis [2/2]

Setting $|\mathbb{F}| \doteq \text{poly}(|H|, |\varphi|)$, $|H| \doteq \text{poly}(|\varphi|)$ makes the protocol sound and efficient.

Recall that, reducing from NTIME(T), $n \doteq O(\log T)$ and $m, |\varphi| \doteq \text{poly}(\log T)$.

- **soundness error:**

$$\max\left\{\varepsilon_{LDT}(\delta),\ 4\delta + \frac{\text{poly}(\bar{m}, \bar{n}, |H|, |\varphi|)}{|\mathbb{F}|}\right\} \doteq O(1)$$

- **query complexity:**

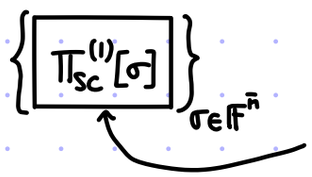
$$5 + (m+1)\cdot q_{LDT} + \bar{n}\cdot O(|H|) + (3\bar{n}+3)\cdot O(|H|)\cdot m + (3\bar{n}+3)\cdot O(|\varphi|\cdot|H|)$$
$$= O(\bar{n}\cdot|H|\cdot|\varphi|) = O\left(\frac{n}{\log|H|}\cdot|H|\cdot|\varphi|\right)$$
$$\doteq \text{poly}(|\varphi|) \doteq \text{poly}(\log T)$$

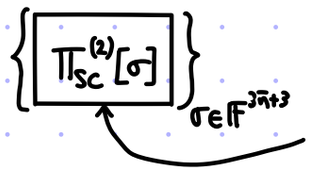
- **verifier time:** (in field operations)

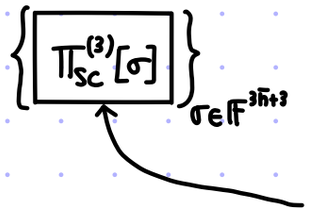
$$\text{poly}(\bar{n}, |H|, |\varphi|) + \text{poly}(|z|) + (m+1)\cdot t_{LDT}$$
$$\doteq \text{poly}(|\varphi|, |z|) \doteq \text{poly}(|x|, \log T)$$

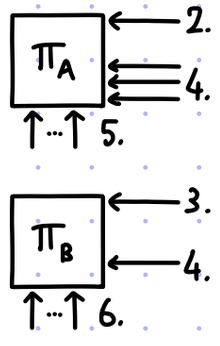
- **randomness complexity:**

$$O(\bar{n}\cdot\log|\mathbb{F}|) + r_{LDT} = O\left(\frac{n}{\log|H|}\cdot\log|\mathbb{F}|\right) = O(\log T)$$









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

1. Compute $C := T(\mathbb{F}, H, (m,n,\varphi))$.
2. Sample $\sigma \in \mathbb{F}^{\bar{n}}$ and run sumcheck

$V_{sc}(\mathbb{F}, H, \bar{n}, 0, 3\cdot(|H|-1))$ (field, domain, vars, sum, degree) $\rightarrow (\rho_1,\dots,\rho_{\bar{n}})$ $\leftarrow \Pi_A(\rho)\cdot(\Pi_A(\rho)-1)\cdot\prod_{i\in[\bar{n}]}\hat{\sigma}_i(\rho_i)$

3. Sample $\sigma \in \mathbb{F}^{3\bar{n}+3}$ and run sumcheck

$V_{sc}(\mathbb{F}, H, 3\bar{n}+3, 0^m, 3\cdot(|H|-1))$ (field, domain, vars, sum, degree) $\rightarrow (\rho_1,\dots,\rho_{3\bar{n}+3})$ $\leftarrow \Pi_B(\rho)\cdot(\Pi_B(\rho)-1)\cdot\prod_{i\in[3\bar{n}+3]}\hat{\sigma}_i(\rho_i)$

4. Sample $\sigma \in \mathbb{F}^{3\bar{n}+3}$ and run sumcheck for

$$\sum_{a=(v_1,v_2,v_3,c)\in H^{3\bar{n}+3}} C(a, \hat{A}(v_1), \hat{A}(v_2), \hat{A}(v_3), \hat{B}(a))\cdot\prod_{i\in[3\bar{n}+3]}\hat{\sigma}_i(q_i) = 0$$

$V_{sc}(\mathbb{F}, H, 3\bar{n}+3, 0, (|\varphi|+1)\cdot(|H|-1))$ (field, domain, vars, sum, degree)

$(\rho_1,\dots,\rho_{3\bar{n}+3})$ ⇨
- query Π_A at $(\rho_1,\dots,\rho_{\bar{n}}), (\rho_{\bar{n}+1},\dots,\rho_{2\bar{n}}), (\rho_{2\bar{n}+1},\dots,\rho_{3\bar{n}})$
- query Π_B at $(\rho_1,\dots,\rho_{3\bar{n}+3})$
- for every $i\in[3\bar{n}+3]$: eval $\hat{\sigma}_i$ at ρ_i
- eval C at $(\rho_1,\dots,\rho_{3\bar{n}+3}, ans_1, ans_2, ans_3, ans_4)$

5. $V_{LDT}^{\Pi_A}(\mathbb{F}, \bar{n}, \text{ind}, \leq |H|-1)$ (vars, degree)
6. $V_{LDT}^{\Pi_B}(\mathbb{F}, 3\bar{n}+3, m, \text{ind}, \leq |H|-1)$ (vars, outputs, degree)

More on Proof Length

The proof length for the PCP for NTIME(T) described today is at least T^6:

$$|\pi| = |\pi_A| + |\pi_B| + |\pi_{sc}^{(1)}| + |\pi_{sc}^{(2)}| + |\pi_{sc}^{(3)}| + |\pi_{Ic}|$$

$$= |\mathbb{F}|^{\bar{n}} + |\mathbb{F}|^{3\bar{n}+3} \cdot m + |\mathbb{F}|^{\bar{n}} \cdot O(|\mathbb{F}|^{\bar{n}} \cdot |H|) + |\mathbb{F}|^{3\bar{n}+3} \cdot O(|\mathbb{F}|^{3\bar{n}+3} \cdot |H|) \cdot m + |\mathbb{F}|^{3\bar{n}+3} \cdot O(|\mathbb{F}|^{3\bar{n}+3} \cdot |H| \cdot |\varphi|) + |\mathbb{F}|^{n} \cdot O(|\mathbb{F}|^{n} \cdot |H|)$$

$$\geq |\mathbb{F}|^{6\bar{n}} \geq |H|^{6 \cdot \frac{\log T}{\log |H|}} = T^6.$$

WHY?

① QUADRATIC BLOWUP in the reduction from zero-on-subcube to sumcheck:

to prove that $\hat{f}|_{H^n} \equiv 0$ the prover includes, $\forall \sigma \in \mathbb{F}^n$, a sumcheck proof $\pi_{sc}[\sigma]$ of size $\geq |\mathbb{F}|^n$.

② CUBIC BLOWUP in the reduction from NTIME(T) to IOSAT:

there are $\Omega(T)$ variables in the computation trace of the machine

and the reduction considers all possible 3CNF clauses formed by these.

Reducing proof length makes a PCP harder to construct.

Fundamental question: HOW SHORT CAN A PCP BE ?

Trading Shorter Proof for More Queries

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

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

$$\mathrm{NTIME}(T) \subseteq \mathrm{PCP}\left[\begin{array}{lll} \varepsilon_c = 0, & \Sigma = \{0,1\}, & \ell = T^{1+O(\varepsilon)}, \quad pt = \mathrm{poly}_\varepsilon(T) \\ \varepsilon_s = 1/2, & q = (\log T)^{\frac{1}{\varepsilon}}, & r = \mathrm{poly}_\varepsilon(\log T), \quad vt = \mathrm{poly}_\varepsilon(n, \log T) \end{array}\right]$$

The blowups in the prior slide can be avoided.

① Alternative reduction from zero-on-subcube.

The VANISHING POLYNOMIAL of H is $Z_H(x) := \prod_{a \in H}(x-a)$.

lemma: Let $\hat{f} \in \mathbb{F}[X_1,\ldots,X_n]$ have individual degree $\leq d$.

Then $\hat{f}|_{H^n} \equiv 0 \leftrightarrow \exists\, \hat{g}_1,\ldots,\hat{g}_n \in \mathbb{F}[X_1,\ldots,X_n]$ of individual degree $\leq d$ s.t. $\hat{f}(X_1,\ldots,X_n) \equiv \sum_{i=1}^{n} Z_H(X_i) \cdot g_i(X_1,\ldots,X_n)$.

② Routing techniques to reduce from NTIME(T) to a smaller zero-on-subcube problem:

$$\forall\, v \in \{0,1\}^n \quad \phi(v, A(\phi_1(v)), A(\phi_2(v)), A(\phi_3(v)), B(v)) = 0 \quad \text{for} \quad n = \log T + O(\log\log T)$$

Best Possible Proof Length for PCPs?

Different techniques lead to PCPs with QUASILINEAR proof length:

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

$$\mathrm{NTIME}(T) \subseteq \mathrm{PCP}\left[\begin{array}{lll} \varepsilon_c=0, & \Sigma=\{0,1\}, & \ell = T\cdot\mathrm{poly}(\log T), \quad pt = T\cdot\mathrm{poly}(\log T) \\ \varepsilon_s=1/2, & q=\mathrm{poly}(\log T), & r=\log T+O(\log\log T),\quad vt=\mathrm{poly}(n,\log T)\end{array}\right]$$

SHORT PCPS WITH POLYLOG QUERY COMPLEXITY*

ELI BEN-SASSON† AND MADHU SUDAN‡

Short PCPs Verifiable in Polylogarithmic Time*

Eli Ben-Sasson † Oded Goldreich ‡ Prahladh Harsha § Madhu Sudan ¶

Salil Vadhan ‖

On the Concrete Efficiency of Probabilistically-Checkable Proofs*

Eli Ben-Sasson†	Alessandro Chiesa†	Daniel Genkin‡	Eran Tromer†
eli@cs.technion.ac.il	alexch@csail.mit.edu	danielg3@cs.technion.ac.il	tromer@cs.tau.ac.il
Technion	MIT	Technion	Tel Aviv University

Achieving LINEAR proof length remains a MAJOR open problem.

For example:

$$\mathrm{CSAT} \overset{?}{\in} \mathrm{PCP}\left[\begin{array}{lll} \varepsilon_c=0, & \Sigma=\{0,1\}, & \ell = O(|C|) \\ \varepsilon_s=1/2 & q=\mathrm{poly}(\log|C|), & r=\log|C|+O(1)\end{array}\right]$$

At the time of writing, the state of the art is: $\exists\, a>0\ \forall\, \tau>0\ \forall\, n>0$

$\exists$ PCP verifier V for CSAT on circuits of size n with $\ell = 2^{a/\tau}\cdot n$ and $q=n^{\tau}$.

Bibliography

PCP for NTIME

PCP for NTIME with ϵ tradeoff

- [BFLS 1991]: Checking computations in polylogarithmic time, by László Babai, Lance Fortnow, Leonid Levin, Mario Szegedy.
- [HS 2000]: Small PCPs with low query complexity, by Prahladh Harsha and Madhu Sudan.
- [BS 2005]: Short PCPs with polylog query complexity, by Eli Ben-Sasson, Madhu Sudan.
- [BGHSV 2006]: Short PCPs verifiable in polylogarithmic time, by Eli Ben-Sasson, Oded Goldreich, Prahladh Harsha, Madhu Sudan, Salil Vadhan.
- [BCGT 2012]: On the concrete efficiency of probabilistically checkable proofs, by Eli Ben-Sasson, Alessandro Chiesa, Daniel Genkin, Eran Tromer.

PCP with quasilinear proof length

& succint verifier

& quasilinear time prover

PCP with linear proof length and sublinear query complexity

- [BKKMS 2013]: Constant rate PCPs for Circuit-SAT with sublinear query complexity, by Eli Ben-Sasson, Yohay Kaplan, Swastik Kopparty, Or Meir, Henning Stichtenoth.

PCP with linear proof length & sublinear query complexity, based on special AG codes