Foundations of Probabilistic Proofs

A course by **Alessandro Chiesa**

Lecture 14

Linear-Length IOP for Circuits

Linear-Size IOPs for Arithmetic Computations

We adapted PCPs into IOPs with much better (but not linear) proof length.

TODAY: IOP with linear proof length for arithmetic computations (over large fields)

We use this NP-complete language:

$$\underline{\text{def:}}\quad \mathrm{R1CS}(\mathbb{F}) = \left\{ (\underbrace{A,B,C}_{m\times n \text{ matrices}}, u) \;\middle|\; \exists\, w \in \mathbb{F}^{n-|u|} \text{ s.t. } Az \circ Bz = Cz \text{ for } z := (u,w) \right\}.$$

$$Az \circ Bz = Cz \quad \text{for } z := (u,w) \qquad \{\langle a_i, z\rangle \cdot \langle b_i, z\rangle = \langle c_i, z\rangle\}_{i\in[m]}$$

Rank 1 Constraint Systems

$$\begin{bmatrix} -a_1- \\ -a_2- \\ \vdots \\ -a_m- \end{bmatrix} \cdot \begin{bmatrix} 1 \\ z \\ | \end{bmatrix} \circ \begin{bmatrix} -b_1- \\ -b_2- \\ \vdots \\ -b_m- \end{bmatrix} \cdot \begin{bmatrix} 1 \\ z \\ | \end{bmatrix} = \begin{bmatrix} -c_1- \\ -c_2- \\ \vdots \\ -c_m- \end{bmatrix} \cdot \begin{bmatrix} 1 \\ z \\ | \end{bmatrix}$$

theorem: For "smooth" $\mathbb{F}$ with $|\mathbb{F}| = \Omega(n)$,

$$\mathrm{R1CS}(\mathbb{F}) \in \mathrm{IOP}\left[\varepsilon_c = 0,\ \varepsilon_s = \tfrac{1}{2},\ k = O(\log m),\ \Sigma = \mathbb{F},\ \ell = O(m),\ q = O(\log m),\ r = O(\log m \cdot \log|\mathbb{F}|)\right]$$

We CANNOT conclude that NP has linear-length IOPs (NP reductions introduce overheads).

We assume for simplicity that $m = n$ (# constraints = # variables).

Prior Choices of Encoding

Our recipe to construct PCPs so far has been to set $\pi = (\pi_a, \pi_{sat})$ where

① π_a is (allegedly) the encoding of a candidate assignment, i.e. belongs to $\{Enc(a)\}_a$

② if π_a is close to $Enc(a)$ for some a, π_{sat} facilitates checking that a is satisfying

① What encodings did we use for an assignment $a:[n] \to \mathbb{F}$?

ⓐ For exp-length PCPs we used linear extensions (aka the Hadamard code)

$Enc(a): \mathbb{F}^n \to \mathbb{F}$ where $Enc(a) := (\langle a, c \rangle)_{c \in \mathbb{F}^n}$

exponential
$|Enc| = |\mathbb{F}|^n$

ⓑ For poly-length PCPs we used low-degree multivariate extensions (aka the Reed-Muller code)

$Enc(a): \mathbb{F}^{\log n} \to \mathbb{F}$ where $Enc(a) := "(\mathbb{F}, \{0,1\}, \log n)\text{-extension of } a"$ (multilinear)

almost polynomial
$|Enc| = n^{\log|\mathbb{F}|} = n^{O(\log\log n)}$

$Enc(a): \mathbb{F}^{\frac{\log n}{\log|H|}} \to \mathbb{F}$ where $Enc(a) := "(\mathbb{F}, H, \frac{\log n}{\log|H|})\text{-extension of } a"$

polynomial
$|Enc| = n^{\frac{\log|\mathbb{F}|}{\log|H|}} = n^{1+O(\varepsilon)}$

For ⓐ we have a linearity test and for ⓑ we have a (multivariate) low-degree test.

② How to test satisfiability? For ⓐ, random combination & tensor test. For ⓑ, use sumcheck for everything.

Which Encodings Can We Use?

We seek an encoding Enc with several properties.

- Constant rate: $|Enc(a)| = O(|a|)$
- Constant relative distance: $a \neq a' \rightarrow \Delta(Enc(a), Enc(a')) \geq \Omega(1)$
- Lets us execute our recipe of $\pi = (\pi_a, \pi_{sat})$, which in turn means that we need:
  - a proximity test (check that π_a is close to $\{Enc(z)\}_z$ in few queries)
  - an approach for testing satisfiability (a replacement for the sumcheck protocol)

EASY: satisfying the rate and distance alone (pick any good code over $\mathbb{F}$)

HARD: additionally satisfy the other requirement

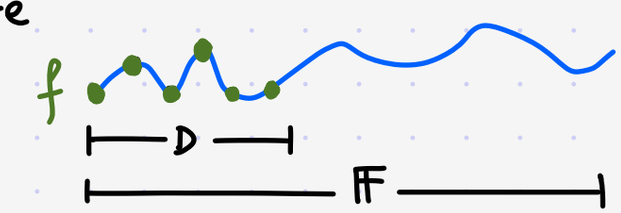
Univariate Low-Degree Extensions

We again place our hopes in polynomials: we use **UNIVARIATE low-degree extensions**.

REVIEW: Fix a finite field $\mathbb{F}$ and domain $D \subseteq \mathbb{F}$.

The interpolation of a function $f: D \to \mathbb{F}$ is $\hat{f} \in \mathbb{F}[X]$ where

$$\hat{f}(X) := \sum_{\alpha \in D} f(\alpha) \cdot L_{D,\alpha}(X) = \sum_{\alpha \in D} f(\alpha) \cdot \left(\prod_{\beta \in D \setminus \{\alpha\}} \frac{X-\beta}{\alpha-\beta} \right).$$



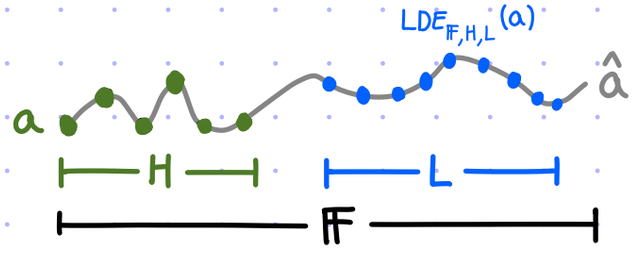
Let $a: [n] \to \mathbb{F}$ be a function.

We can identify $[n]$ with some $H \subseteq \mathbb{F}$ with $|H| = n$. (And sometimes we choose H to have special structure, e.g. a smooth subgroup of $\mathbb{F}^*$ or a subspace in $\mathbb{F}$.)

Fix an evaluation domain $L \subseteq \mathbb{F}$.

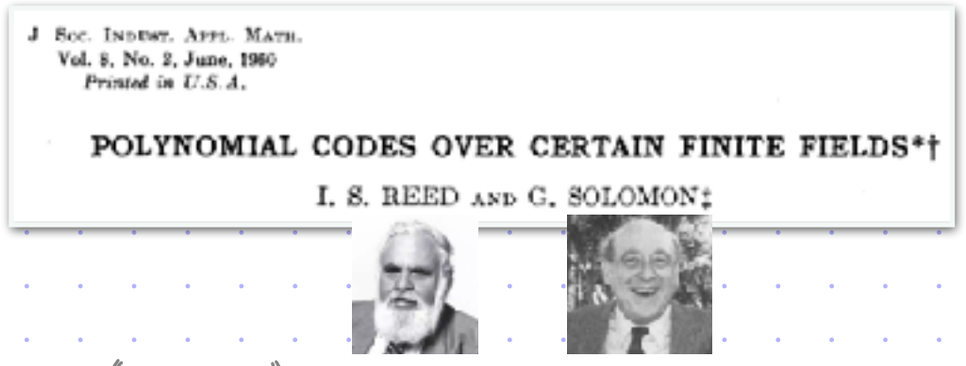
The **univariate low-degree extension** of $a: [n] \to \mathbb{F}$ from H to L is the function $LDE_{\mathbb{F},H,L}(a): L \to \mathbb{F}$ defined as follows:

1. view $a: [n] \to \mathbb{F}$ as $a: H \to \mathbb{F}$
2. let $\hat{a} \in \mathbb{F}[X]$ be the interpolation of a (it has degree $< |H|$)
3. let $LDE_{\mathbb{F},H,L}(a)$ be the evaluation of $\hat{a}$ on L



NOTE: we evaluate the interpolation on a domain $L \subseteq \mathbb{F}$ rather than $\mathbb{F}$ for flexibility.

The Reed–Solomon Code


J. Soc. Indust. Appl. Math.
Vol. 8, No. 2, June, 1960
Printed in U.S.A.

POLYNOMIAL CODES OVER CERTAIN FINITE FIELDS*†

I. S. REED AND G. SOLOMON‡

Fix a finite field $\mathbb{F}$, domain $L \subseteq \mathbb{F}$, and degree bound d.

The Reed–Solomon code with parameters $(\mathbb{F}, L, d)$ is

$$RS[\mathbb{F},L,d] := \{ f : L \to \mathbb{F} \mid \exists \text{ polynomial } p \in \mathbb{F}[X] \text{ s.t. } p(L) = f \text{ and } \deg(p) < d \}.$$

"strictly less" helps us with notation

That is, evaluations on L of polynomials in $\mathbb{F}[X]$ of degree $<d$.

The RS code is a linear (error-correcting) code:

$RS[\mathbb{F},L,d]$ is an $\mathbb{F}$-linear subspace of $\mathbb{F}^L$ $(\forall f,g \in RS[\mathbb{F},L,d]\ \forall \alpha,\beta \in \mathbb{F},\ \alpha f + \beta g \in RS[\mathbb{F},L,d])$.

The RS code's parameters are:

- message length = d. Number of coefficients in a polynomial of degree $<d$.
- block length = $|L|$. Size of a function $f : L \to \mathbb{F}$.
- relative distance $\geq 1 - \frac{d-1}{|L|}$. By the Polynomial Identity Lemma $(\forall p \in \mathbb{F}[X] \text{ with } p \neq 0, \Pr_{\alpha \leftarrow L}[p(\alpha)=0] \leq \frac{\deg(p)}{|L|})$.

The rate $\left(\frac{\text{message length}}{\text{block length}}\right)$ is $\frac{d}{|L|}$. Hence if $|L| = \Theta(d)$ then rate $\geq \Omega(1)$ and relative distance $\geq \Omega(1)$.

OBSERVE: $\forall H \subseteq \mathbb{F}\ \forall a : H \to \mathbb{F}$, $LDE_{\mathbb{F},H,L}(a) \in RS[\mathbb{F},L,|H|]$.

TODAY: we construct a linear-length IOP for RICS, temporarily assuming a proximity test for $RS[\mathbb{F},L,d]$ (which is the focus of the next lecture)

Univariate Arithmetization of R1CS [1/2]

We rewrite the R1CS satisfiability condition in terms of low-degree univariate polynomials.

Let (A,B,C,u) be an $\mathrm{R1CS}(\mathbb{F})$ instance.

We rewrite the satisfiability condition as 4 simpler conditions:

$$\exists\, w\in\mathbb{F}^{n-|u|} \text{ s.t. } A\begin{bmatrix}u\\w\end{bmatrix}\circ B\begin{bmatrix}u\\w\end{bmatrix}=C\begin{bmatrix}u\\w\end{bmatrix} \leftrightarrow \exists\ \substack{w\in\mathbb{F}^{n-|u|}\\ z_A,z_B,z_C\in\mathbb{F}^n} \text{ s.t. } z_A\circ z_B=z_C \wedge \begin{matrix} z_A=Az \\ z_B=Bz \\ z_C=Cz\end{matrix} \text{ where } z:=(u,w)$$

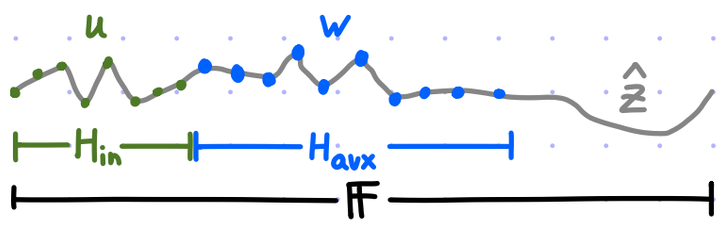
Next we translate the conditions to be about univariate polynomials.

The vanishing polynomial of $S\subseteq\mathbb{F}$ is $V_S(x):=\prod_{\alpha\in S}(x-\alpha)$.

① Entrywise Product

$$z_A\circ z_B=z_C \leftrightarrow \hat{z}_A(X)\cdot\hat{z}_B(X)-\hat{z}_C(X) \text{ vanishes on } H \leftrightarrow \exists\,\hat{h}(X) \text{ s.t. } \hat{z}_A(X)\cdot\hat{z}_B(X)-\hat{z}_C(X)\equiv\hat{h}(X)V_H(X)$$

② Input Consistency



Split H into disjoint H_{in}, H_{aux} for u,w respectively.

The interpolation $\hat{z}(X)$ of $z:=(u,w)$ on H can be constructed as $\hat{u}(X)+V_{H_{in}}(X)\,\hat{w}_*(X)$

where $w_*: H_{aux}\to\mathbb{F}$ is the function defined as $w_*(a):=\dfrac{w(a)-\hat{u}(a)}{V_{H_{in}}(a)}$.

Indeed:
$$\begin{cases}\forall\, a\in H_{in} & \hat{u}(a)+V_{H_{in}}(a)\,\hat{w}_*(a)=u(a)+0\cdot\hat{w}_*(a)=\hat{z}(a)\\ \forall\, a\in H_{aux} & \hat{u}(a)+V_{H_{in}}(a)\,\hat{w}_*(a)=\hat{u}(a)+V_{H_{in}}(a)\cdot\dfrac{w(a)-\hat{u}(a)}{V_{H_{in}}(a)}=w(a)=\hat{z}(a)\end{cases}$$

Univariate Arithmetization of R1CS [2/2]

Let (A,B,C,u) be an $\mathrm{RICS}(\mathbb{F})$ instance.

We rewrite the satisfiability condition as 4 simpler conditions:

$$\exists\, w\in\mathbb{F}^{n-|u|} \text{ s.t. } A\begin{bmatrix}u\\w\end{bmatrix}\circ B\begin{bmatrix}u\\w\end{bmatrix}=C\begin{bmatrix}u\\w\end{bmatrix} \leftrightarrow \exists\ \substack{w\in\mathbb{F}^{n-|u|}\\ z_A,z_B,z_c\in\mathbb{F}^n} \text{ s.t. } z_A\circ z_B=z_c \wedge \begin{matrix}z_A=Az\\ z_B=Bz\\ z_c=Cz\end{matrix} \text{ where } z:=(u,w)$$

Therefore, the RICS satisfiability condition is equivalent to:

$$\exists\ \begin{matrix}\hat{w}_*(x) \text{ of degree } <|H|-|u|\\ \hat{z}_A,\hat{z}_B,\hat{z}_c \text{ of degrees } <|H|\\ \hat{h}(X) \text{ of degree } <|H|-1\end{matrix} \text{ s.t. } \hat{z}_A(x)\cdot\hat{z}_B(x)-\hat{z}_c(x)\equiv\hat{h}(x)v_H(x) \wedge \begin{matrix}\hat{z}_A(H)=A\hat{z}(H)\\ \hat{z}_B(H)=B\hat{z}(H)\\ \hat{z}_c(H)=C\hat{z}(H)\end{matrix} \text{ where } \hat{z}(x):=\hat{u}(x)+v_{H_{in}}(x)\cdot\hat{w}_*(x)$$

This directly leads to a few steps of a protocol:

$P((A,B,C,u),w)$

- $z:=(u,w)$, $\forall M\in\{A,B,C\}$ $z_M:=Mz$.
- $\forall M\in\{A,B,C\}$ $f_M:=\hat{z}_M(L)$.
- $h:=\hat{h}(L)$ where $\hat{h}(X):=\frac{\hat{z}_A(X)\cdot\hat{z}_B(X)-\hat{z}_c(X)}{v_H(X)}$.
- $f_w:=\hat{w}_*(L)$ where $w_*:H_{aux}\to\mathbb{F}$ is defined as $w_*(a):=\frac{w(a)-\hat{u}(a)}{v_{H_{in}}(a)}$.

$\xrightarrow{f_w,f_A,f_B,f_C,h:L\to\mathbb{F}}$

$f:L\to\mathbb{F}$ is defined as $f(a):=\hat{u}(a)+v_{H_{in}}(a)\cdot f_w(a)$

$V((A,B,C,u))$

- Sample $s\leftarrow L$.
- Check $f_A(s)\cdot f_B(s)-f_C(s)\stackrel{?}{=}h(s)\cdot v_H(s)$.
- Low-degree tests:

$V_{LDT}^{f_w}(\mathbb{F},L,|H|-|u|)\stackrel{?}{=}1$ $V_{LDT}^{h}(\mathbb{F},L,|H|-1)\stackrel{?}{=}1$

$\forall M\in\{A,B,C\}$: $V_{LDT}^{f_M}(\mathbb{F},L,|H|)\stackrel{?}{=}1$

MISSING: check that $\forall M\in\{A,B,C\}$ $\hat{f}_M(H)=M\hat{f}(H)$. We discuss this next.

Univariate Sumcheck [1/4]

The verifier has oracle access to $f: L \to \mathbb{F}$ that is δ-close to $\hat{f}$ with $\deg(\hat{f}) < d$ and has input $(\underset{\text{field}}{\mathbb{F}}, \underset{\text{eval domain}}{L}, \underset{\text{degree}}{d}, \underset{\text{summation domain}}{H}, \underset{\text{sum}}{\gamma})$, and wants to check that $\sum_{a \in H} \hat{f}(a) = \gamma$.

Attempt 1: obtain $\hat{f}(a)$ for every $a \in H$ and add up

Obtaining even 1 value of $\hat{f}$ via local correction of f takes $d = \Omega(n)$ queries.

Even if $\hat{f} = f$ the attempt fails:

- if $H \not\subseteq L$ then we need $d = \Omega(n)$ queries to interpolate f
- if $H \subseteq L$ then we need $|H| = \Omega(n)$ queries (to learn $f|_H = \hat{f}|_H$)

Attempt 2: sumcheck IP for the claim "$\sum_{a \in H} \hat{f}(a) = \gamma$" (with $n=1$ variables)

The first (and only) prover message is the $d = \Omega(n)$ coefficients of $\hat{f}$:

$P_{sc} \xrightarrow{(c_0, c_1, \ldots, c_{d-1})} V_{sc}^{f}$: set $\tilde{f}(X) := \sum_{i=0}^{d-1} c_i X^i$ and check $\sum_{a \in H} \tilde{f}(a) = \gamma$ and $\tilde{f}(s) = f(s)$ for random $s \in L$

This is tantamount to reading 1 (huge) symbol from $\Sigma = \mathbb{F}^d$.

WE NEED NEW IDEAS!

Univariate Sumcheck [2/4]

The verifier has oracle access to $f: L \to \mathbb{F}$ that is δ-close to $\hat{f}$ with $\deg(\hat{f}) < d$ and has input $(\mathbb{F}, L, d, H, \gamma)$, and wants to check that $\sum_{a \in H} \hat{f}(a) = \gamma$.

($\mathbb{F}$: field, L: eval domain, d: degree, H: summation domain, γ: sum)

Step 1: reduce the problem to the case $d < |H|$

The vanishing polynomial of H is $V_H(X) := \prod_{a \in H} (X - a)$.

claim: $\sum_{a \in H} \hat{f}(a) = \sum_{a \in H} (\hat{f} \bmod V_H)(a)$

proof: Divide $\hat{f}(x)$ by $V_H(x)$: $\hat{f}(x) \equiv \hat{h}(x) V_H(x) + \hat{g}(x)$ with $\begin{cases} \deg(\hat{g}) < |H| \\ \deg(\hat{h}) = \deg(\hat{f}) - |H| \end{cases}$

Observe that $\sum_{a \in H} \hat{f}(a) = \sum_{a \in H} \hat{h}(a) V_H(a) + \hat{g}(a) = \sum_{a \in H} \hat{g}(a)$. ■

Univariate Sumcheck [3/4]

The verifier has oracle access to $f: L \to \mathbb{F}$ that is δ-close to $\hat{f}$ with $\deg(\hat{f}) < d$ and has input $(\mathbb{F}, L, d, H, \gamma)$, and wants to check that $\sum_{a \in H} \hat{f}(a) = \gamma$.

($\mathbb{F}$: field, L: eval domain, d: degree, H: summation domain, γ: sum)

Step 1: reduce the problem to the case $d < |H|$

claim: $\sum_{a \in H} \hat{f}(a) = \sum_{a \in H} (\hat{f} \bmod V_H)(a)$

Step 2: assume that H has nice algebraic structure

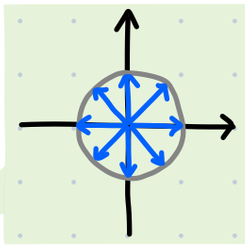
analogous to how the (multivariate) sumcheck protocol works for product sets in $\mathbb{F}^n$ (rather than for all sets)

claim: if $\deg(\hat{g}) < |H|$ and H is a subgroup of $\mathbb{F}^*$ then $\sum_{a \in H} \hat{g}(a) = |H| \hat{g}(0)$

proof: Let ω be a generator for H (which is cyclic). Note that $\omega^{|H|} = 1$.

First consider a monomial:

$$\sum_{a \in H} a^i = \sum_{j=0}^{|H|-1} (\omega^j)^i = \sum_{j=0}^{|H|-1} (\omega^i)^j = \begin{cases} \text{if } i \equiv 0 \bmod |H|: \sum_{j=0}^{|H|-1} (1)^j = |H| \\ \text{if } i \not\equiv 0 \bmod |H|: \frac{(\omega^i)^{|H|} - 1}{\omega^i - 1} = \frac{1-1}{\omega^i - 1} = 0 \end{cases}$$



the sum of all roots of unity is 0

Hence all monomials $\{X^i\}_{0 < i < |H|}$ in $\hat{g}(X)$ sum to 0.

That leaves $|H|$ times $\hat{g}$'s constant coefficient (i.e., $\hat{g}(0)$). ■

REMARK: A similar statement holds when H is an additive subgroup of $\mathbb{F}$.
If $\deg(\hat{g}) < |H|$ then $\sum_{a \in H} \hat{g}(a) = (\sum_{a \in H} a^{|H|-1}) \cdot \text{coeff}(X^{|H|-1}, \hat{g})$. The constant $\sum_{a \in H} a^{|H|-1}$ is $\neq 0$ and computable in $\text{poly}(\log |H|)$ field operations.

Univariate Sumcheck [4/4]

The verifier has oracle access to $f: L \to \mathbb{F}$ that is δ-close to $\hat{f}$ with $\deg(\hat{f}) < d$ and has input $(\mathbb{F}, L, d, H, \gamma)$ (field, eval domain, degree, summation domain, sum), and wants to check that $\sum_{a \in H} \hat{f}(a) = \gamma$.

We know that $\sum_{a \in H} \hat{f}(a) = \gamma \leftrightarrow \exists\ \hat{h}$ with $\deg(\hat{h}) < d - |H|$, $\hat{g}$ with $\deg(\hat{g}) < |H|$ s.t. $\hat{f}(x) \equiv \hat{h}(x) V_H(x) + \hat{g}(x)$ and $\hat{g}(0) = \gamma/|H|$

$\leftrightarrow \exists\ \hat{h}$ with $\deg(\hat{h}) < d - |H|$, $\hat{p}$ with $\deg(\hat{p}) < |H| - 1$ s.t. $\hat{f}(x) \equiv \hat{h}(x) V_H(x) + \left(x\hat{p}(x) + \gamma/|H|\right)$.

$P((\mathbb{F}, L, d, H, \gamma), f)$

Compute $\hat{h}(x)$ and $\hat{p}(x)$ s.t.

$\deg(\hat{h}) = \deg(\hat{f}) - |H|$, $\deg(\hat{p}) < |H| - 1$,

and $\hat{f}(x) \equiv \hat{h}(x) V_H(x) + \left(x\hat{p}(x) + \gamma/|H|\right)$.

Output $h := \hat{h}|_L$ and $p := \hat{p}|_L$.

$h: L \to \mathbb{F}$, $p: L \to \mathbb{F}$ →

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

$V^h_{LDT}(\mathbb{F}, L, d - |H|) \stackrel{?}{=} 1$.

$V^p_{LDT}(\mathbb{F}, L, |H| - 1) \stackrel{?}{=} 1$.

Sample $s \leftarrow L$.

Check that $f(s) = h(s) \cdot V_H(s) + \left(s \cdot p(s) + \gamma/|H|\right)$.

COMPLETENESS: If $\sum_{a \in H} \hat{f}(a) = \gamma$ then the verifier accepts w.p. 1.

SOUNDNESS: If $\sum_{a \in H} \hat{f}(a) \neq \gamma$ then there are two cases.

① h or p is δ-far (from suitable degree) → low-degree test accepts w.p. $\leq \varepsilon_{LDT}(\delta)$

② h and p are δ-close to (unique) $\hat{h} \in \mathbb{F}^{<d-|H|}[X]$ and $\hat{p} \in \mathbb{F}^{<|H|-1}[X]$

↳ consistency check passes w.p. $\leq \frac{d-1}{|L|} + 3\delta$. (If f, h, p have "correlated agreement" then $1 \cdot \delta$.)

Checking Linear Equations

The verifier has oracle access to $f, g : L \to \mathbb{F}$ that are δ-close to $\hat{f}, \hat{g}$ of degree $< d$ and has input $(\mathbb{F}, L, d, H, M)$ (field, eval domain, degree, summation domain, $H \times H$ matrix), and wants to check that $\hat{g}|_H \equiv M \cdot \hat{f}|_H$.

$\Leftrightarrow \{\hat{g}(a) = \sum_{b \in H} M[a,b] \cdot \hat{f}(b)\}_{a \in H}$

Idea: reduce to a univariate sumcheck claim

Let $\text{pow}(X) := (1, X, X^2, \ldots, X^{|H|-1})$. Observe that $\hat{g}|_H = M \cdot \hat{f}|_H \leftrightarrow \langle \text{pow}(X), \hat{g}|_H \rangle \equiv \langle \text{pow}(X), M \cdot \hat{f}|_H \rangle$.

Hence, $\hat{g}|_H \neq M \cdot \hat{f}|_H \to \Pr_{\sigma \leftarrow \mathbb{F}} [\langle \text{pow}(\sigma), \hat{g}|_H \rangle = \langle \text{pow}(\sigma), M \cdot \hat{f}|_H \rangle] \leq \frac{|H|-1}{|\mathbb{F}|}$.

For every $u \in \mathbb{F}^H$, $\langle u, \hat{g}|_H \rangle = \langle u, M \cdot \hat{f}|_H \rangle \leftrightarrow \langle u, \hat{g}|_H \rangle = \langle M^T \cdot u, \hat{f}|_H \rangle$

Recall: $\langle u, v \rangle := u^T v$
So $\langle u, Mv \rangle = u^T M v = (M^T u)^T v = \langle M^T u, v \rangle$

$$\leftrightarrow \sum_{a \in H} \left(u(a) \cdot \hat{g}(a) - (M^T u)(a) \hat{f}(a) \right) = 0$$

$$\leftrightarrow \sum_{a \in H} \left(\hat{u}(a) \cdot \hat{g}(a) - \widehat{(M^T u)}(a) \hat{f}(a) \right) = 0.$$

— univariate sumcheck instance with degree $< d + |H| - 1$

$P((\mathbb{F}, L, d, H, M), (f, g))$

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

$\sigma \in \mathbb{F}$ →

Sample $\sigma \leftarrow \mathbb{F}$.

Univariate sumcheck for

$$\sum_{a \in H} \widehat{\text{pow}(\sigma)}(a) \cdot \hat{g}(a) - \widehat{(M^T \text{pow}(\sigma))}(a) \hat{f}(a) = 0$$

← ans

→ $s \in L$

- query f, g at s
- eval $\widehat{\text{pow}(\sigma)}$ at s
- eval $\widehat{M^T \text{pow}(\sigma)}$ at s

} $O(|H| + |M|_0)$ field ops (# nonzero entries)

soundness error:

$$\underbrace{\frac{|H|-1}{|\mathbb{F}|}}_{\text{reduction error}} + \underbrace{\frac{(d-1)+(|H|-1)}{|\mathbb{F}|}}_{\text{sumcheck error}} + O(1)$$

IOP for R1CS: Construction

View H in 2 parts: H_{in} | H_{aux} — u | w

P((A,B,C,u),w)

1. $z := (u,w)$, $\forall M \in \{A,B,C\}$ $z_M := Mz$.
2. $\forall M \in \{A,B,C\}$ $f_M := \hat{z}_M(L)$.
3. $h := \hat{h}(L)$ where $\hat{h}(X) := \frac{\hat{z}_A(X)\cdot\hat{z}_B(X) - \hat{z}_C(X)}{V_H(X)}$.
4. $f_w := \hat{w_*}(L)$ where $w_* : H_{aux} \to \mathbb{F}$ is defined as $w_*(a) := \frac{w(a) - \hat{u}(a)}{V_{H_{in}}(a)}$.
5. $\forall M \in \{A,B,C\}$ compute $\hat{p}_M, \hat{h}_M$ s.t.
$\widehat{pow(\sigma)}(X)\,\hat{z}_M(X) - \widehat{(M^T pow(\sigma))}(X)\,\hat{z}(X) \equiv \hat{h}_M(X)V_H(X) + X\hat{p}_M(X)$

$\xrightarrow{f_w, f_A, f_B, f_C, h : L \to \mathbb{F}}$

$f : L \to \mathbb{F}$ is defined as $f(a) := \hat{u}(a) + V_{H_{in}}(a)\cdot f_w(a)$

$\xleftarrow{\sigma \in \mathbb{F}}$

For each $M \in \{A,B,C\}$:
univariate sumcheck for
$\sum_{a \in H} \widehat{pow(\sigma)}(a)\cdot\hat{f}_M(a) - \widehat{(M^T\cdot pow(\sigma))}(a)\cdot\hat{f}(a) = 0$

$\xrightarrow{h_M, p_M : L \to \mathbb{F}}$

V((A,B,C,u))

1. Sample $\sigma \leftarrow \mathbb{F}$.
2. Sample $s \leftarrow L$ and check that:
$f_A(s)\cdot f_B(s) - f_C(s) \stackrel{?}{=} h(s)\cdot V_H(s)$
$\forall M \in \{A,B,C\}$:
$\widehat{pow(\sigma)}(s)\cdot f_M(s) - \widehat{(M^T pow(\sigma))}(s)\,f(s) \stackrel{?}{=} h_M(s)\cdot V_H(s) + s\cdot p_M(s)$
3. Low-degree tests:
$V_{LDT}^{f_w}(\mathbb{F}, L, |H|-|u|) \stackrel{?}{=} 1$ $V_{LDT}^{h}(\mathbb{F}, L, |H|-1) \stackrel{?}{=} 1$
$\forall M \in \{A,B,C\}$: $V_{LDT}^{f_M}(\mathbb{F}, L, |H|) \stackrel{?}{=} 1$
$V_{LDT}^{h_M}(\mathbb{F}, L, |H|-1) \stackrel{?}{=} 1$
$V_{LDT}^{p_M}(\mathbb{F}, L, |H|-1) \stackrel{?}{=} 1$

Numerous optimizations possible.
Ex 1: batch 3 sumchecks into 1
Ex 2: batch 11 LDTs into 1
⋮

IOP for R1CS: Soundness

⊛ improves to $1-(1-\delta)^4$ if V makes independent queries
⊛ or improves to δ for $\delta \leq O(1)$ using "correlated agreement"

claim: $\forall \delta, \varepsilon_S \leq \max\left\{\varepsilon_{LDT}(\delta), \frac{|H|-1}{|\mathbb{F}|} + \frac{2|H|-2}{|L|} + 4\delta\right\}$ ⊛ ⊛

If any sent function is δ-far

then the verifier accepts w.p. $\leq \varepsilon_{LDT}(\delta)$.

So suppose that all sent functions are

δ-close to (some) low-degree polynomials

$\hat{f}_w, \hat{f}_A, \hat{f}_B, \hat{f}_C, \hat{h}, \hat{h}_A, \hat{h}_B, \hat{h}_C, \hat{p}_A, \hat{p}_B, \hat{p}_C$.

$P((A,B,C,u),w)$

1. $z := (u,w)$, $\forall M \in \{A,B,C\}$ $z_M := Mz$.
2. $\forall M \in \{A,B,C\}$ $f_M := \hat{z}_M(L)$.
3. $h := \hat{h}(L)$ where $\hat{h}(x) := \frac{\hat{z}_A(x)\cdot\hat{z}_B(x) - \hat{z}_C(x)}{V_H(x)}$.
4. $f_w := \hat{w}_*(L)$ where $w_* : H_{aux} \to \mathbb{F}$ is defined as $w_*(a) := \frac{w(a) - \hat{u}(a)}{V_{H_{in}}(a)}$.
5. $\forall M \in \{A,B,C\}$ compute $\hat{p}_M, \hat{h}_M$ s.t. $\widehat{pow(\sigma)}(x)\,\hat{z}_M(x) - \widehat{(M^T pow(\sigma))}(x)\,\hat{z}(x) \equiv \hat{h}_M(x)V_H(x) + x\hat{p}_M(x)$

$\xrightarrow{f_w, f_A, f_B, f_C, h : L \to \mathbb{F}}$

$f : L \to \mathbb{F}$ is defined as $f(a) := \hat{u}(a) + V_{H_{in}}(a)\cdot f_w(a)$

$\xleftarrow{\sigma \in \mathbb{F}}$

For each $M \in \{A,B,C\}$:
univariate sumcheck for
$\sum_{a\in H} \widehat{pow(\sigma)}(a)\cdot\hat{f}_M(a) - \widehat{(M^T\cdot pow(\sigma))}(a)\cdot\hat{f}(a) = 0$

$\xrightarrow{h_M, p_M : L \to \mathbb{F}}$

$V((A,B,C,u))$

1. Sample $\sigma \leftarrow \mathbb{F}$.
2. Sample $s \leftarrow L$ and check that:
   $f_A(s)\cdot f_B(s) - f_C(s) \stackrel{?}{=} h(s)\cdot V_H(s)$
   $\forall M \in \{A,B,C\}$:
   $\widehat{pow(\sigma)}(s)\cdot f_M(s) - \widehat{(M^T pow(\sigma))}(s)\, f(s) \stackrel{?}{=} h_M(s)\cdot V_H(s) + s\cdot p_M(s)$
3. Low-degree tests:
   $V_{LDT}^{f_w}(\mathbb{F}, L, |H|-|u|) \stackrel{?}{=} 1$ $V_{LDT}^{h}(\mathbb{F}, L, |H|-1) \stackrel{?}{=} 1$
   $\forall M \in \{A,B,C\}$: $V_{LDT}^{f_M}(\mathbb{F}, L, |H|) \stackrel{?}{=} 1$
   $V_{LDT}^{h_M}(\mathbb{F}, L, |H|-1) \stackrel{?}{=} 1$
   $V_{LDT}^{p_M}(\mathbb{F}, L, |H|-1) \stackrel{?}{=} 1$

If $(A,B,C,u) \notin RICS(\mathbb{F})$ then one of two cases holds.

Case 1: $\hat{f}_A|_H \circ \hat{f}_B|_H \neq \hat{f}_C|_H$

Hence $\hat{f}_A(x)\cdot\hat{f}_B(x) - \hat{f}_C(x) \neq \hat{h}(x)\,V_H(x)$.

So $\Pr_{s\leftarrow L}\left[f_A(s)\cdot f_B(s) - f_C(s) = h(s)V_H(s)\right] \leq \frac{2|H|-2}{|L|} + 4\delta$.

Input consistency is accounted for:
$\Delta(f_w, \hat{f}_w) \leq \delta \to \Delta(f, \hat{f}) \leq \delta$
where $\hat{f}(x) := \hat{f}_w(x)\cdot V_{H_{in}}(x) + \hat{u}(x)$

Case 2: $\exists M \in \{A,B,C\}$ $\hat{f}_M|_H \neq M\cdot\hat{f}|_H$

Hence, except w.p. $\leq \frac{|H|-1}{|\mathbb{F}|}$ over $\sigma \in \mathbb{F}$, $\widehat{pow(\sigma)}(x)\cdot\hat{f}_M(x) - \widehat{(M^T pow(\sigma))}(x)\cdot\hat{f}(x) \neq \hat{h}_M(x)\cdot V_H(x) + x\cdot\hat{p}_M(x)$.

So $\Pr_{s\leftarrow L}\left[\widehat{pow(\sigma)}(s)\cdot f_M(s) - \widehat{(M^T pow(\sigma))}(s)\cdot f(s) = h_M(s)\cdot V_H(s) + s\cdot p_M(s)\right] \leq \frac{2|H|-2}{|L|} + 4\delta$.

IOP for R1CS: Efficiency

- round complexity:
  $O(1) + k_{LDT}$
- proof length (in field elements):
  $O(|L|) + O(\ell_{LDT})$
- query complexity:
  $O(1) + O(q_{LDT})$
- randomness complexity (in bits):
  $O(\log|\mathbb{F}|) + r_{LDT}$
- prover time (in field operations):
  $O(|A|_0 + |B|_0 + |C|_0) + O(|L| \cdot \log|L|) + O(pt_{LDT})$
  (via suitable use of Fast Fourier Transforms)
- verifier time (in field operations):
  $O(|A|_0 + |B|_0 + |C|_0) + O(|L|) + O(vt_{LDT})$

$P((A,B,C,u),w)$

1. $z := (u,w)$, $\forall M \in \{A,B,C\}$ $z_M := Mz$.
2. $\forall M \in \{A,B,C\}$ $f_M := \hat{z}_M(L)$.
3. $h := \hat{h}(L)$ where $\hat{h}(X) := \frac{\hat{z}_A(X)\cdot\hat{z}_B(X) - \hat{z}_C(X)}{V_H(X)}$.
4. $f_w := \hat{w}_*(L)$ where $w_* : H_{aux} \to \mathbb{F}$ is defined as $w_*(a) := \frac{w(a) - \hat{u}(a)}{V_{H_{in}}(a)}$.
5. $\forall M \in \{A,B,C\}$ compute $\hat{p}_M, \hat{h}_M$ s.t.
   $\widehat{pow(\sigma)}(X)\,\hat{z}_M(X) - \widehat{(M^T pow(\sigma))}(X)\,\hat{z}(X) \equiv \hat{h}_M(X) V_H(X) + X\,\hat{p}_M(X)$

$\xrightarrow{f_w, f_A, f_B, f_C, h : L \to \mathbb{F}}$

$f : L \to \mathbb{F}$ is defined as $f(a) := \hat{u}(a) + V_{H_{in}}(a) \cdot f_w(a)$

$\xleftarrow{\sigma \in \mathbb{F}}$

For each $M \in \{A,B,C\}$:
univariate sumcheck for
$\sum_{a \in H} \widehat{pow(\sigma)}(a)\cdot\hat{f}_M(a) - \widehat{(M^T \cdot pow(\sigma))}(a)\cdot\hat{f}(a) = 0$

$\xrightarrow{h_M, p_M : L \to \mathbb{F}}$

$V((A,B,C,u))$

1. Sample $\sigma \leftarrow \mathbb{F}$.
2. Sample $s \leftarrow L$ and check that:
   $f_A(s)\cdot f_B(s) - f_C(s) \stackrel{?}{=} h(s)\cdot V_H(s)$
   $\forall M \in \{A,B,C\}$:
   $\widehat{pow(\sigma)}(s)\cdot f_M(s) - \widehat{(M^T pow(\sigma))}(s)\, f(s) \stackrel{?}{=} h_M(s)\cdot V_H(s) + s\cdot p_M(s)$
3. Low-degree tests:
   $V_{LDT}^{f_w}(\mathbb{F}, L, |H|-|u|) \stackrel{?}{=} 1$ $V_{LDT}^{h}(\mathbb{F}, L, |H|-1) \stackrel{?}{=} 1$
   $\forall M \in \{A,B,C\}$: $V_{LDT}^{f_M}(\mathbb{F}, L, |H|) \stackrel{?}{=} 1$
   $V_{LDT}^{h_M}(\mathbb{F}, L, |H|-1) \stackrel{?}{=} 1$
   $V_{LDT}^{p_M}(\mathbb{F}, L, |H|-1) \stackrel{?}{=} 1$

The soundness analysis tells us that we can set $|L| = \Theta(|H|) = \Theta(n)$.

We will construct a univariate LDT (in the IOP model) with:
$k_{LDT} = O(\log|L|)$, $\ell_{LDT} = O(|L|)$, $q_{LDT} = O(\log|L|)$, $r_{LDT} = O(\log|L| \cdot \log|\mathbb{F}|)$, $pt_{LDT} = O(|L|)$, $vt_{LDT} = O(\log|L|)$.
This will require a "smooth" evaluation domain L.

Bibliography

Linear-length IOPs for Circuit-SAT (& R1CS)

Linear-size IOP for boolean circuit SAT using algebraic-geometry codes

- [BCGRS 2016]: Interactive oracle proofs with constant rate and query complexity, by Eli Ben-Sasson, Alessandro Chiesa, Ariel Gabizon, Michael Riabzev, Nick Spooner.

Today's IOP for R1CS

- [BCRSVW 2018]: Aurora: transparent succinct arguments for R1CS, by Eli Ben-Sasson, Alessandro Chiesa, Michael Riabzev, Nick Spooner, Madars Virza, Nicholas Ward. (▸Video 1), (▸Video 2), (▸Video 3)
- [RR 2020]: Local proofs approaching the witness length, by Noga Ron-Zewi, Ron Rothblum. (▸Video)

Reducing the constant overhead

- [RZ 2021]: An algebraic framework for universal and updatable zkSNARKs, by Carla Ràfols, Arantxa Zapico.

Generalized univariate sumcheck