Univariate Sumcheck Protocol

Table of Contents

Univarate Sumcheck Protocol [1/3]

4.2 Representations of polynomials

We frequently move from univariate polynomials over $\mathbb{F}$ to their evaluations on chosen subsets of $\mathbb{F}$, and back. We use plain letters like f, g, h, π to denote *evaluations* of polynomials, and "hatted letters" $\hat{f}, \hat{g}, \hat{h}, \hat{\pi}$ to denote corresponding polynomials. This bijection is well-defined only if the size of the evaluation domain is larger than the degree. Formally, if $f \in \mathrm{RS}[L, \rho]$ for $L \subseteq \mathbb{F}$, $\rho \in (0, 1]$, then $\hat{f}$ is the unique polynomial of degree less than $\rho|L|$ whose evaluation on L equals f. Likewise, if $\hat{f} \in \mathbb{F}[X]$ with $\deg(f) < \rho|L|$, then $f_L := \hat{f}|_L \in \mathrm{RS}[L, \rho]$ (but we will drop the subscript when the choice of subset is clear from context).

Univariate Sumcheck [1/3]

field, evaluation domain, degree, summation domain, claimed sum

The verifier has oracle access to $f: L \to \mathbb{F}$ s.t. $\deg(\hat{f}) \leq d$ and input $(\mathbb{F}, \underbrace{L, d, H}_{\text{each of these has size } \Omega(n)}, \gamma)$,
and wants to check the claim "$\sum_{a \in H} \hat{f}(a) = \gamma$".

Attempt 1: query f at every $a \in H$ and add up the answers

What if $H \cap L = \emptyset$?

Deriving $\hat{f}(a)$ for a single $a \in H$ requires $d+1 = \Omega(n)$ queries for interpolation.

Even if $H \subseteq L$, $|H| = \Omega(n)$ queries is too many.

[And even if H were small, in the noisy case we would use self-correction, which we don't have.]

Univarate Sumcheck Protocol [2/3]

Univariate Sumcheck [2/3]

field, evaluation domain, degree, summation domain, claimed sum

The verifier has oracle access to $f: L \to \mathbb{F}$ s.t. $\deg(\hat{f}) \leq d$ and input $(\mathbb{F}, L, d, H, \gamma)$, and wants to check the claim "$\sum_{a \in H} \hat{f}(a) = \gamma$".

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

Let $v_H(x) := \prod_{a \in H}(x-a)$ be the vanishing polynomial of the set H.

Divide $\hat{f}(x)$ by $v_H(x)$: $\hat{f}(x) = \hat{h}(x) v_H(x) + \hat{g}(x)$ with $\deg(\hat{g}) < |H|$ & $\deg(\hat{h}) = \deg(\hat{f}) - |H|$

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

Step 2: assume that H is nice and use algebra ← similar to how multivariate sumcheck works for product sets in $\mathbb{F}^n$ rather than all sets

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

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

Hence all monomials $\{x^i\}_{0<i<|H|}$ in $\hat{g}(x)$ sum to zero, and are left with $|H|$ times $g(0)$. ∎

Hence $\sum_{a \in H} \hat{g}(a) = \gamma$ iff $|H| \hat{g}(0) = \gamma$.

[Here we saw the case of multiplicative subgroups. A similar statement holds for additive subgroups.]

6

Univarate Sumcheck Protocol [3/3]

Univariate Sumcheck [3/3]

field, evaluation domain, degree, summation domain, claimed sum

The verifier has oracle access to $f: L \to \mathbb{F}$ s.t. $\deg(\hat{f}) \leq d$ and input $(\mathbb{F}, L, d, H, \gamma)$, and wants to check the claim "$\sum_{a \in H} \hat{f}(a) = \gamma$".

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

Compute $\hat{h}(x)$ with $\deg(\hat{h}) = \deg(\hat{f}) - |H|$ and $\hat{p}(x)$ with $\deg(\hat{p}) < |H| - 1$ s.t.

$\hat{f}(x) \equiv \hat{h}(x) v_H(x) + (x\hat{p}(x) + \gamma/|H|)$

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

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

- test that h is δ-close to degree $d - |H|$ and that p is δ-close to degree $|H| - 1$
- sample $s \leftarrow L$ and check that
  $f(s) = h(s) \cdot v_H(s) + (s\, p(s) + \gamma/|H|)$

Analysis: If $\sum_{a \in H} \hat{f}(a) = \gamma$ then verifier accepts w.p. 1. If $\sum_{a \in H} \hat{f}(a) \neq \gamma$ then distinguish between:

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

② $\tilde{h}$ and $\tilde{p}$ both δ-close to (unique) h and p

$\searrow \hat{f}(x) \not\equiv \hat{h}(x) v_H(x) + (x\hat{p}(x) + \gamma/|H|)$ so identity test accept w.p. $\leq \frac{d}{|L|} + 2\delta$.

[or else $\hat{f}$ would sum to γ]

7

Preliminaries

The Reed–Solomon code. Given a subset L of a field $\mathbb{F}$ and $\rho \in (0, 1]$, we denote by $\mathrm{RS}[L, \rho] \subseteq \mathbb{F}^L$ all evaluations over L of univariate polynomials of degree less than $\rho|L|$. That is, a word $c \in \mathbb{F}^L$ is in $\mathrm{RS}[L, \rho]$ if there exists a polynomial p of degree less than $\rho|L|$ such that $c_a = p(a)$ for every $a \in L$. We denote by $\mathrm{RS}[L, (\rho_1, \ldots, \rho_n)] := \prod_{i=1}^{n} \mathrm{RS}[L, \rho_i]$ the interleaving of Reed–Solomon codes with rates $\rho_1, \ldots, \rho_n$.

R1CS problem

The R1CS relation consists of instance-witness pairs $((A, B, C, v), w)$, where A, B, C are matrices and v, w are vectors over a finite field $\mathbb{F}$, such that $(Az) \circ (Bz) = Cz$ for $z := (1, v, w)$ and "$\circ$" denotes the entry-wise

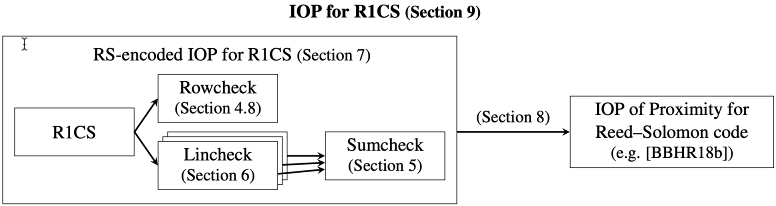

Figure 3: Structure of our IOP for R1CS in terms of key sub-protocols.

- **Rowcheck:** given vectors $x, y, z \in \mathbb{F}^m$, test whether $x \circ y = z$, where "$\circ$" denotes entry-wise product.
- **Lincheck:** given vectors $x \in \mathbb{F}^m, y \in \mathbb{F}^n$ and a matrix $M \in \mathbb{F}^{m \times n}$, test whether $x = My$.

Row check protocol

4.8 Univariate rowcheck

We describe *univariate rowcheck*, a noninteractive RS-encoded IOPP for simultaneously testing satisfaction of a given arithmetic constraint on a large number of inputs. The next definition captures this.

Definition 4.9 (rowcheck relation). *The relation $\mathcal{R}_{\mathrm{ROW}}$ is the set of all pairs $\big((\mathbb{F}, L, H, \rho, \mathsf{w}, \mathsf{c}), (f_1, \ldots, f_{\mathsf{w}})\big)$ where $\mathbb{F}$ is a finite field, L, H are affine subspaces of $\mathbb{F}$ with $L \cap H = \emptyset$, $\rho \in (0,1)$, $\mathsf{w} \in \mathbb{N}$, $\mathsf{c}\colon \mathbb{F}^{\mathsf{w}} \to \mathbb{F}$ is an arithmetic circuit, $f_1, \ldots, f_{\mathsf{w}} \in \mathrm{RS}[L, \rho]$, and $\forall\, a \in H \;\; \mathsf{c}(\hat{f}_1(a), \ldots, \hat{f}_{\mathsf{w}}(a)) = 0$.*

Standard techniques for testing membership in the *vanishing subcode* of the Reed–Solomon code [BS08] directly imply a non-interactive RS-encoded IOPP for the above rowcheck relation. Namely, the system of equations $\{\mathsf{c}(\hat{f}_1(a), \ldots, \hat{f}_{\mathsf{w}}(a)) = 0\}_{a \in H}$ is equivalent via the factor theorem to the statement "there exists $g \in \mathrm{RS}[L, \deg(\mathsf{c})\rho - |H|/|L|]$ such that $\hat{g}(X) \cdot \prod_{a \in H}(X - a) \equiv \mathsf{c}(\hat{f}_1(X), \ldots, \hat{f}_{\mathsf{w}}(X))$". Therefore, the prover could send g to the verifier, who could probabilistically check the identity at a random point of L, with a soundness error of $\deg(\mathsf{c})\rho$. In fact, within the formalism of RS-encoded IOPPs (and given that $L \cap H = \emptyset$) there is no need for the prover to send anything: the verifier can simply check that $p \in \mathrm{RS}[L, \deg(\mathsf{c})\rho - |H|/|L|]$ for the function $p\colon L \to \mathbb{F}$ defined by

$$\forall\, a \in L\,,\; p(a) := \frac{\mathsf{c}(\hat{f}_1(a), \ldots, \hat{f}_{\mathsf{w}}(a))}{\mathbb{Z}_H(a)} \;\; .$$

The maximum rate for the foregoing RS-encoded IOPP is $(\sigma^*, \rho^*) = (\max\{\rho, \deg(\mathsf{c})\rho - |H|/|L|\}, \deg(\mathsf{c}) \cdot \rho)$. Note that the verifier can simulate oracle access to the function p when given oracle access to the witness oracles $f_1, \ldots, f_{\mathsf{w}}$. Each query to p requires evaluating the arithmetic circuit c and the vanishing polynomial $\mathbb{Z}_H$. Throughout, we directly use the above ideas without encapsulating them in "rowcheck sub-protocols".

Proof

Lemma 5.4 ([BC99, Theorem 1], restated)**.** *Let H be an affine subspace of $\mathbb{F}$, and let $\hat{g}(x)$ be a univariate polynomial over $\mathbb{F}$ of degree (strictly) less than $|H| - 1$. Then*

$$\sum_{a \in H} \hat{g}(a) = 0.$$

Definition A.1. *For a field $\mathbb{F}$ of characteristic p, the generalized derivative of a function f in a direction $a \in \mathbb{F}$ is $\Delta_a(f) := \sum_{b \in \mathbb{F}_p} f(X + ba)$. For $a_1, \ldots, a_k \in \mathbb{F}$, we inductively define $\Delta_{a_1,\ldots,a_k}(f) := \Delta_{a_1}(\Delta_{a_2,\ldots,a_k}(f))$.*

Note that if $\mathbb{F}$ has characteristic 2 then this coincides with the directional derivative. If H is a subspace of $\mathbb{F}$ with basis $a_1, \ldots, a_n$ then for any $a_0 \in \mathbb{F}$,

$$\Delta_{a_1,\ldots,a_k}(f)(a_0) = \sum_{a \in H_0} f(a_0 + a) \ . \tag{1}$$

For a natural number $c = \sum_{i=0}^{k} c_i p^i$, $0 \leq c_i < p$, let $\mathsf{wt}(c) = \sum_{i=0}^{k} c_i$.[10] For a polynomial $P(X) = \sum_{j \geq 0} \alpha_j X^j$ define $\mathsf{wt}(P) := \max\{\mathsf{wt}(j) : \alpha_j \neq 0\}$.

Claim A.2. *For any polynomial $P \in \mathbb{F}[X]$ and any $a \in \mathbb{F}$,*

$$\mathsf{wt}(\Delta_a(P)) \leq \max(\mathsf{wt}(P) - (p-1), 0) \ .$$

Moreover, if $\mathsf{wt}(P) < p - 1$, *then* $\Delta_a(P)$ *is identically zero.*

Lemma A.3. *Let $\mathbb{F}$ be a field of characteristic p, and let $P \in \mathbb{F}[X]$ have degree less than $p^k - 1$. Then for any $a_1, \ldots, a_k \in \mathbb{F}$, $\Delta_{a_1,\ldots,a_k}(P)$ is identically zero.*

Proof. We have $\mathsf{wt}(P) < (p-1)k$. By Claim A.2, $\mathsf{wt}(\Delta_{a_2,\ldots,a_k}(P)) < p - 1$, and so $\Delta_{a_1,\ldots,a_k}(P)$ is identically zero. □

Proof of Lemma 5.4. For some $a_0, a_1, \ldots, a_k \in \mathbb{F}$, $H = a_0 + H_0$ where H_0 is the linear subspace with basis $a_1, \ldots, a_k$. By Eq. (1) and Lemma A.3 we conclude $\sum_{a \in H} g(a) = \Delta_{a_1,\ldots,a_k}(g)(a_0) = 0$. □

Claim A.2. *For any polynomial $P \in \mathbb{F}[X]$ and any $a \in \mathbb{F}$,*

$$\mathsf{wt}(\Delta_a(P)) \leq \max(\mathsf{wt}(P) - (p-1), 0) \ .$$

Moreover, if $\mathsf{wt}(P) < p - 1$, then $\Delta_a(P)$ is identically zero.

Proof. By linearity of Δ_a, it suffices to prove the claim for a single monomial; that is, $P(X) = X^c$ for some integer $c \geq 0$. Let $c = \sum_{i=0}^{k} c_i p^i$ be the p-ary expansion of c for some integer k. For a natural number $d = \sum_{i=0}^{k} d_i p^i$ we write $d \leq_p c$ if $d_i \leq c_i$ for all i.

$$\begin{aligned}
\Delta_a(X^c) &= \sum_{b \in \mathbb{F}_p} (X + ba)^c = \sum_{b \in \mathbb{F}_p} \sum_{d=0}^{c} \binom{c}{d} X^d b^{c-d} a^{c-d} \\
&= \sum_{d=0}^{c} \binom{c}{d} X^d a^{c-d} \Big(\sum_{b \in \mathbb{F}_p} b^{c-d} \Big) = \sum_{d=0}^{c} \binom{c}{d} X^d a^{c-d} \Big(\sum_{b \in \mathbb{F}_p} b^{\sum_{i=0}^{k} (c_i - d_i) p^i} \Big) \\
&= \sum_{d=0}^{c} \binom{c}{d} X^d a^{c-d} \Big(\sum_{b \in \mathbb{F}_p} b^{\sum_{i=0}^{k} (c_i - d_i)} \Big) = \sum_{d \leq_p c} \binom{c}{d} X^d a^{c-d} \cdot \Big(\sum_{b \in \mathbb{F}_p} b^{\mathsf{wt}(c) - \mathsf{wt}(d)} \Big) \ ,
\end{aligned}$$

where in the penultimate equality we used that $b^{p^i} = b$ for $b \in \mathbb{F}_p$, and in the last equality we used that $\binom{c}{d} \equiv 0 \pmod{p}$ unless $d \leq_p c$. Recall that for $0 \leq m < p - 1$, $\sum_{b \in \mathbb{F}_p} b^m = 0$. Hence the terms in the above sum where $\mathsf{wt}(c) - \mathsf{wt}(d) < p - 1$ all vanish. Any remaining terms thus have weight at most $\mathsf{wt}(c) - (p-1)$. In particular, if $\mathsf{wt}(c) < p - 1$ then all terms vanish. $\square$