

Sum-check and categories

A. Sorokin

January 9, 2026

Setting

Let \mathbb{F}_{17} be the finite field with 17 elements. Consider the polynomial

$$f(x, y, z, w) = 2x + xyz + 3w \in \mathbb{F}_{17}[x, y, z, w],$$

with the fixed variable order

$$x \prec y \prec z \prec w.$$

The goal of the sum-check protocol is to verify a claimed value

$$S = \sum_{(x,y,z,w) \in \{0,1\}^4} f(x, y, z, w)$$

using a logarithmic number of rounds and low-degree checks.

High-Level Idea

The sum-check protocol reduces a multivariate sum over the Boolean hypercube to a sequence of univariate polynomial identities. At each round, one variable is “summed out”, and the verifier checks consistency of partial sums.

Round 1: Eliminating x

The following example explains the ideas of sum-check protocol. Define the univariate polynomial

$$g_1(X) = \sum_{y,z,w \in \{0,1\}} f(X, y, z, w).$$

Prover computes a polynomial:

$$\begin{aligned} g_1(X) &= \sum_{y,z,w} (2X + Xyz + 3w) \\ &= 2X \cdot 8 + X \sum_{y,z,w} yz + 3 \sum_{y,z,w} w \\ &= 16X + 2X + 12 \\ &= 18X + 12 \equiv X + 12 \pmod{17}. \end{aligned}$$

The verifier checks:

$$g_1(0) + g_1(1) \stackrel{?}{=} S.$$

The verifier then samples a random $r_1 \in \mathbb{F}_{17}$ and fixes $x := r_1$.

Round 2: Eliminating y

Prover computes a polynomial

$$g_2(Y) = \sum_{z,w \in \{0,1\}} f(r_1, Y, z, w)$$

so it is

$$\begin{aligned} g_2(Y) &= \sum_{z,w} (2r_1 + r_1 Y z + 3w) \\ &= 4(2r_1) + 2r_1 Y + 6 \\ &= 8r_1 + 2r_1 Y + 6. \end{aligned}$$

The verifier checks:

$$g_2(0) + g_2(1) \stackrel{?}{=} g_1(r_1).$$

Then a random $r_2 \in \mathbb{F}_{17}$ is chosen and $y := r_2$ is fixed.

Round 3: Eliminating z

Prover computes a polynomial

$$g_3(Z) = \sum_{w \in \{0,1\}} f(r_1, r_2, Z, w).$$

and it is

$$\begin{aligned} g_3(Z) &= \sum_w (2r_1 + r_1 r_2 Z + 3w) \\ &= 4r_1 + 2r_1 r_2 Z + 3. \end{aligned}$$

The verifier checks:

$$g_3(0) + g_3(1) \stackrel{?}{=} g_2(r_2).$$

Then a random $r_3 \in \mathbb{F}_{17}$ is chosen and $z := r_3$ is fixed.

Round 4: Eliminating w

Prover computes a polynomial

$$g_4(W) = f(r_1, r_2, r_3, W) = 2r_1 + r_1 r_2 r_3 + 3W.$$

The verifier checks:

$$g_4(0) + g_4(1) \stackrel{?}{=} g_3(r_3).$$

Final check. Finally, verifier checks

$$g(r_1, r_2, r_3, r_4) \stackrel{?}{=} g_4(r_4).$$

Conclusion

If all checks pass, the verifier is convinced that the claimed sum S is correct. Each round enforces naturality of summation with respect to substitution, and soundness follows from the low degree of the intermediate polynomials.

Core fact: commutation of evaluation and summation

Statement

Let F be any commutative semiring. Let

$$f(x'_1, \dots, x'_m, x_1, \dots, x_n, x''_1, \dots, x''_k)$$

be an F -valued function of $m + n + k$ variables.

For any fixed evaluation point $(r_1, \dots, r_m) \in F^m$, evaluation in the variables (x'_1, \dots, x'_m) commutes with summation over (x''_1, \dots, x''_k) :

$$\begin{aligned} & \sum_{(x''_1, \dots, x''_k) \in \{0,1\}^k} f(r_1, \dots, r_m, x_1, \dots, x_n, x''_1, \dots, x''_k) \\ &= \left(\sum_{(x''_1, \dots, x''_k) \in \{0,1\}^k} f(x'_1, \dots, x'_m, x_1, \dots, x_n, x''_1, \dots, x''_k) \right) \Big|_{x'_i = r_i}. \end{aligned}$$

Equivalently,

$$\text{eval}_{(r_1, \dots, r_m)} \left(\sum_{x''_1, \dots, x''_k} f \right) = \sum_{x''_1, \dots, x''_k} \left(\text{eval}_{(r_1, \dots, r_m)} f \right).$$

Categorical interpretation

For any (small) category \mathbf{C} over a cosmos \mathcal{V} and evaluation at any objects $C_1, C_2, C_3, C_4 \in \mathbf{C}$ the following diagram commutes:

$$\begin{array}{ccccccc} \mathbf{C}^4 & \xrightarrow{\text{ev}_1} & \mathbf{C}^3 & \xrightarrow{\text{ev}_2} & \mathbf{C}^2 & \xrightarrow{\text{ev}_3} & \mathbf{C} \xrightarrow{\text{ev}_4} \mathcal{V} \\ \downarrow f^W & & \downarrow f^W & & \downarrow f^W & & \downarrow f^W \\ \mathbf{C}^3 & & \mathbf{C}^2 & & \mathbf{C} & \xrightarrow{\text{ev}_3} & \mathcal{V} \\ \downarrow f^Z & & \downarrow f^Z & & \downarrow f^Z & & \\ \mathbf{C}^2 & & \mathbf{C} & \xrightarrow{\text{ev}_2} & \mathcal{V} & & \\ \downarrow f^Y & & \downarrow f^Y & & & & \\ \mathbf{C} & \xrightarrow{\text{ev}_1} & \mathcal{V} & & & & \\ \downarrow f^X & & & & & & \\ \mathcal{V} & & & & & & \end{array}$$

The idea is that for any functor $F : \mathbf{C} \rightarrow \mathcal{V}$ and any object $C \in \mathbf{C}$ the coYoneda lemma holds:

$$\int^X \mathbf{C}_C^X \otimes F_X \simeq F_C$$

and coends commute whenever any of them exists:

$$\int^X \int^Y T \simeq \int^Y \int^X T$$

where T is a functor of two variables.

Categorical version of sum-check

