The Sum-Check Problem

Given an m-variable polynomial $g: \mathbb{F}_q^m \to \mathbb{F}_q$ over a finite field (arithmetic modulo q).

Known bound on the degree of each variable: $\deg_{x_i}(g) \leq d_i$ for $i = 1, \ldots, m$.

Prover provides H and wants to convince the Verifier that:

$$H = \sum_{b_1 \in \{0,1\}} \sum_{b_2 \in \{0,1\}} \cdots \sum_{b_m \in \{0,1\}} g(b_1, b_2, \ldots, b_m)$$

The Sum-Check Protocol

Start: P sends an integer S, claiming to be the sum H.

Round 1: P sends (the coefficients of) a univariate polynomial $S_1(X_1)$, claiming $S_1 = H_1$, where

$$H_1(X_1) = \sum_{b_2 \in \{0,1\}} \cdots \sum_{b_m \in \{0,1\}} g(X_1, b_2, \ldots, b_m)$$

V checks $\deg(S_1) \leq d_1$ and $S_1(0) + S_1(1) = S$.

Then, V samples a random $r_1 \in \mathbb{F}_q$ and sends it to P.

Round $i > 1$ ($i \leq m$): P sends a univariate polynomial $S_i(X_i)$, claiming $S_i = H_i$, where

$$H_i(X_i) = \sum_{b_{i+1} \in \{0,1\}} \cdots \sum_{b_m \in \{0,1\}} g(r_1, \ldots, r_{i-1}, X_i, b_{i+1}, \ldots, b_m)$$

V checks $\deg(S_i) \leq d_i$ and $S_i(0) + S_i(1) = S_{i-1}(r_{i-1})$.

Then, V samples a random $r_i \in \mathbb{F}_q$ and sends it to P.

Final check: V checks $S_m(r_m) = g(r_1, \ldots, r_m)$.

Reject if any check fails. Otherwise accept.

Example: Honest Prover

Let $g(X_1, X_2) = X_1X_2 + X_2$. The true sum is $H =$ _____

Start: P sends $S = H$.

Round 1: P sends polynomial

$S_1(X_1) = H_1(X_1) =$ _____

V checks $S_1(0) + S_1(1) = S$: _____

Suppose V samples $r_1 = 1$ and sends to P. $S_1(r_1) =$ ___

[Then, check $S_1 = H_1$ by checking $S_1(r_1) = H_1(r_1)$.]

Round 2: P sends polynomial

$S_2(X_2) = H_2(X_2) =$ _____

V checks $S_2(0) + S_2(1) = S_1(r_1)$: _____

Suppose V samples $r_2 = 2$. $S_2(r_2) =$ ___

Final check: V computes and checks $g(r_1, r_2) = S_2(r_2)$: _____

All checks passed: accept.

Example: Cheating Prover

Question: In this example, which check fails?

Let $g(X_1, X_2) = X_1X_2 + X_2$. The true sum is $H =$ _____

Start: P sends $S = 0$, claiming to be H (a false claim).

Round 1: P sends polynomial

$$S_1(X_1) = 2X_1 - 1 \qquad \text{(but } H_1(X_1) = X_1 + 1\text{)}$$

V checks $S_1(0) + S_1(1) = S$. Pass this check? _____

Suppose V samples $r_1 = 1$ and sends to P. What is $S_1(r_1)$? ____

Round 2: P sends polynomial

$$S_2(X_2) = X_2 \qquad \text{(but } H_2(X_2) = 2X_2\text{)}$$

V checks $S_2(0) + S_2(1) = S_1(r_1)$. Pass this check? _____

Suppose V samples $r_2 = 2$. What is $S_2(r_2)$? ____

Final check: V computes and checks $g(r_1, r_2) = S_2(r_2)$. Pass this check? _____