4/9/18
DA

Example of Sumcheck Protocol

$\phi = (\bar{x}_1 \vee x_3) \wedge (x_1 \vee \bar{x}_2)$

Choose prime $p = 13 > 2^3$.

(*) Claim: $\#\phi = 4$ (# satisfying assignments)

Compute: P_ϕ

$(\bar{x}_1 \vee x_3) \Rightarrow 1 - x_1(1-x_3) = 1 - x_1 + x_1 x_3$

$(x_1 \vee \bar{x}_2) \Rightarrow 1 - x_2(1-x_1) = 1 - x_2 + x_1 x_2$

So

$$P_\phi = (1 - x_1 + x_1 x_3) \cdot (1 - x_2 + x_1 x_2)$$

Then $$\#\phi = \sum_{b_1=0,1} \sum_{b_2=0,1} \sum_{b_3=0,1} P_\phi(b_1, b_2, b_3)$$

Step 1: Prove $$4 = \sum_{b_1=0,1} \sum_{b_2=0,1} \sum_{b_3=0,1} P_\phi(b_1, b_2, b_3)$$

Prover computes $h_1(x_1)$:

$$h_1(x_1) = \sum_{b_2=0,1} \sum_{b_3=0,1} P_\phi(x_1, b_2, b_3)$$

$$= P_\phi(x_1, 0, 0) + P_\phi(x_1, 0, 1) + P_\phi(x_1, 1, 0) + P_\phi(x_1, 1, 1)$$

$$= (1 - x_1) \cdot 1 + 1 \cdot 1 + (1 - x_1) \cdot x_1 + 1 \cdot x_1$$

$$h_1(x_1) = 2 + x_1 - x_1^2$$ to Verifier

Verifier checks

$h_1(0) + h_1(1) = 2 + 2 = 4$ check ✓

Chooses random $q_1 = 7$, so

$$P_\phi(7, x_2, x_3) = (-6 + 7x_3) \cdot (1 + 6x_2)$$

$$= (7 + 7x_3) \cdot (1 + 6x_2) \pmod{13}$$

$$h_1(7) = 2 + 7 - 49 = 12 \pmod{13}$$

4/9/18
DA

Step 2: Prove $12 = \sum_{b_2=0,1} \sum_{b_3=0,1} (7+7X_3)\cdot(1+6X_2) \pmod{13}$

Prover computes $h_2(X_2)$:

$$h_2(X_2) = \sum_{b_3=0,1} (7+7b_3)\cdot(1+6X_2)$$

$$= 7\cdot(1+6X_2) + 4\cdot(1+6X_2)$$

$h_2(X_2) \equiv 8+9X_2 \pmod{13}$ and sends it to Verifier

Verifier checks

$h_2(0)+h_2(1) = 8+8+9 = 12 \pmod{13}$ ✓

and chooses a random $a_2 = 4$

$$P_\phi(7,4,X_3) = (7+7X_3)\cdot(1+24)$$

$$= 6+6X_3 \pmod{13}$$

$$h_2(4) = 8+36 = 5 \pmod{13}$$

Step 3: Prove $5 = \sum_{b_3=0,1} (6+6X_3)$

This is the base case, Verifier checks

$(6+6\cdot0)+(6+6\cdot1) = 18 \equiv 5 \pmod{13}$

and ACCEPTS Claim ⊛