Example of P fooling V in Sumcheck

4/12/18
DA

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

[Recall $\#\phi = 4$] Prime $p = 13 > 2^3$

However, P wants V to accept the Incorrect Claim: $\#\phi = 5$.

* assumption

Suppose P could guess* that V will choose $a_1 = 7$. Then P could engineer a polynomial $s_1(X_1)$ as follows:

let $s_1(X_1) = aX_1^2 + bX_1 + c \pmod{13}$

P needs $s_1(0) + s_1(1) = 5 \pmod{13}$

and $s_1(7) = h_1(7) \pmod{13}$

where $h_1(X_1) = 2 + X_1 - X_1^2$ is the correct polynomial

So $s_1(0) + s_1(1) = a + b + 2c \pmod{13}$

and $s_1(7) = 49a + 7b + c \pmod{13}$

$= 10a + 7b + c \pmod{13}$

Solving the simultaneous equations

$a + b + 2c = 5 \pmod{13}$

$10a + 7b + c = 12 \pmod{13}$

We find that $s_1(X_1) = 1 + 2X_1 + X_1^2$ will work:

$s_1(0) = 1$

$s_1(1) = 4$ so $s_1(0) + s_1(1) = 5$

and $s_1(7) = 1 + 14 + 49$

$= 12 \pmod{13}$

Then the next check will be correct:

Step 2 Prove $12 = \sum_{b_2=0,1} \sum_{b_3=0,1} (7 + 7x_3) \cdot (1 + 6x_2) \pmod{13}$

So P can make V accept $\#\phi = 5$ in this case.