Define $V(x) := \sum c_i \cdot v_i(x)$

$W(x) := \sum c_i \cdot w_i(x)$

$Y(x) := \sum c_i \cdot y_i(x)$

$P(x) := V(x) \cdot W(x) - Y(x)$.

P vanishes on all the target points.

$P(r_g) = 0$ for all g.

Then, $(c_1, \cdots, c_5)$ is a legal assignment iff $P(1) = P(2) = 0$ $\Rightarrow t(x) \mid P(x)$.

Note that $P(1) = V(1) \cdot W(1) - Y(1)$ $\therefore P(s) = t(s) \cdot h(s)$

$= c_1 \cdot v_1(1) \cdot c_2 \cdot w_2(1) - c_4 \cdot y_4(1)$ for some poly. $h(x)$.

$= c_1 \cdot c_2 - c_4 = 0$

$P(2) = V(2) \cdot W(2) - Y(2)$

$= c_4 \cdot v_4(2) \cdot (c_1 \cdot w_1(2) + c_3 \cdot w_3(2)) - c_5 \cdot y_5(2)$

$= c_4 \cdot (c_1 + c_3) - c_5 = 0$.

$\Rightarrow$ "I know c_1, c_2, c_3 s.t. $c_1 \cdot c_2 \cdot (c_1 + c_3) = 7$" is translated into an equivalent statement about polynomials $V(x), W(x), Y(x), P(x)$ using QAP.

For an illegal assignment $(c_1, \cdots, c_m)$, $t(x)$ does not divide $P(x)$.

Suppose Alice wants to prove to Bob she knows $c_1, c_2, c_3 \in \mathbb{F}_p$ s.t. $c_1 \cdot c_2 \cdot (c_1 + c_3) = 7$.

i) Alice computes polynomials $V(x), W(x), Y(x)$, and $h(x)$.

ii) Bob chooses a random point $s \in \mathbb{F}_p$ and computes $Com(t(s))$. how to compute it w/ knowing $t(x)$?

iii) Alice computes $Com(V(s))$, $Com(W(s))$, $Com(Y(s))$, $Com(h(s))$.

and sends to Bob. how to compute it w/o knowing s?

iv) Bob checks $Com(V(s) \cdot W(s) - Y(s)) = Com(t(s) \cdot h(s))$.

if Alice doesn't have a satisfying assignment,

she doesn't find any polynomials $V(x), W(x), Y(x), h(x)$ s.t. $V(x) W(x) - Y(x) = h(x) \cdot t(x)$.

$\Rightarrow$ the last equation does not hold.