Constructing a QAP Q for an arithmetic circuit C

For each multiplication gate g in C, pick an arbitrary root $r_g \in \mathbb{F}$

Define the target polynomial $t(x) = \prod (x - r_g)$.

Label an index $k \in \{1, \cdots, m\}$ to each input of the circuit

each output from a multiplication gate.

Let $\mathcal{V}$ be the set of polynomials encoding the left input into each gate.

e.g., $v_k(r_g) = \begin{cases} 1 & \text{if } k\text{-th wire is a left input to gate } g. \\ 0 & \text{otherwise.} \end{cases}$

Let $\mathcal{W}$ be the set of polynomials encoding the right input into each gate.

$\mathcal{Y}$ encode the output.

If we consider a particular gate g and its root r_g,

$$\underbrace{\left(\sum_{k=1}^{m} c_k \cdot v_k(r_g)\right)}_{V(x)} \cdot \underbrace{\left(\sum_{k=1}^{m} c_k \cdot w_k(r_g)\right)}_{W(x)} = \left(\sum_{\text{left}} c_k\right) \cdot \left(\sum_{\text{right}} c_k\right)$$

$$= c_g \cdot y_k(r_g) = c_g.$$

⇒ the output value of the gate is equal to the product of its input.