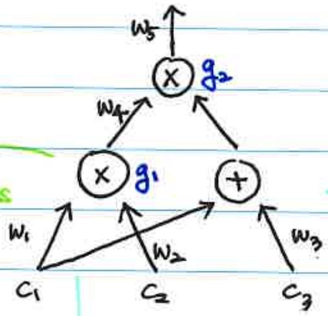
__Example.__

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

express as an arithmetic circuit.



multiplication gates have exactly two input wires

→ do not label the wires going from addition to multiplication gate.

(the addition gate.

⇒ w_1 and w_3 : both right inputs of g_2.

the same output can go into more than 1 gates.

For our circuit, a legal assignment is of the form: $(c_1, \cdots, c_5)$ where $c_4 = c_1 \cdot c_2$

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

$\therefore$ what Alice wants to prove is that she knows a legal assignment $(c_1, \cdots, c_5)$ s.t. $c_5 = 7$

Suppose g_1 is associated with $1 \in \mathbb{F}_p$ and g_2 with $2 \in \mathbb{F}_p$.

Then, $t(x) = (x-1)(x-2)$.

$v_1(g_1) = 1$	$v_1(g_2) = 0$	$w_1(g_1) = 0$	$w_1(g_2) = 1$
$v_2(g_1) = 0$	$v_2(g_2) = 0$	$w_2(g_1) = 1$	$w_2(g_2) = 0$
$v_3(g_1) = 0$	$v_3(g_2) = 0$	$w_3(g_1) = 0$	$w_3(g_2) = 1$
$v_4(g_1) = 0$	$v_4(g_2) = 1$	$w_4(g_1) = 0$	$w_4(g_2) = 0$
$v_5(g_1) = 0$	$v_5(g_2) = 0$	$w_5(g_1) = 0$	$w_5(g_2) = 0$

$y_1(g_1) = 0$	$y_1(g_2) = 0$
$y_2(g_1) = 0$	$y_2(g_2) = 0$
$y_3(g_1) = 0$	$y_3(g_2) = 0$
$y_4(g_1) = 1$	$y_4(g_2) = 0$
$y_5(g_1) = 0$	$y_5(g_2) = 1$

$\Rightarrow v_1(x) = w_2(x) = y_4(x) = 2 - x$

$\Rightarrow v_4(x) = w_1(x) = w_3(x) = y_5(x) = x - 1$

Given fixed values $(c_1, \cdots, c_5)$, we use them as coefficients to define V, W, Y, P.