Homework 6 (v2)

Problem 1

Create a graph with 3 nodes and 3 edges and write constraints for a 3-coloring. Convert the 3-coloring to a rank 1 constraint system.

let $G = (V, E)$ be a graph with 3 nodes V and 3 edges E. where:

$V = v_1, v_2, v_3$ $E = (v_1, v_2), (v_2, v_3), (v_3, v_1)$

Assume we have the colors $1, 2, 3$

for any vertices x, y with an edge $(x, y) \in E$ we can check it satisfies

$$0 == (2 - x * y) * (3 - x * y) * (6 - x * y)$$

an arithmetic-circuit for a 3-coloring would then be:

$$0 == (2 - v_1 * v_2) * (3 - v_1 * v_2) * (6 - v_1 * v_2) 0 == (2 - v_2 * v_3) * (3 - v_2 * v_3) * (6 - v_2 * v_3) 0 == (2 - v_3$$

if we want to convert this to a rank 1 constraint system, we can do the following for any x, y pair:

$$0 == (2 - x * y) * (3 - x * y) * (6 - x * y)$$
$$\text{this can be rewritten as}$$
$$0 == -x^3 y^3 + 11x^2 y^2 - 36xy + 36$$

we define variables

$$a = x^2 b = x * y c = y^2 d = a * c e = b * c$$

which gives us the following rank 1 constraint system:

$$b = x * y$$
$$a = x * x$$
$$c = y * y$$
$$d = a * c$$

and our other constraint is:

$$0 = x^3 y^3 + 11x^2 y^2 - 36xy + 36 = b * d + 11d - 36b + 36$$

which can be rewritten as:

$$-11d + 36b - 36 = b * d$$

now our witness vector is:

$$W = \begin{bmatrix} x \\ y \\ a \\ b \\ c \\ d \\ e \\ 1 \end{bmatrix}$$

now we can represent this in matrix form as follows:

$$A * W \odot B * W = C * W$$

where:

$$A \odot W = \begin{bmatrix} 1 & x & y & a & b & c & d \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \odot \begin{bmatrix} 1 \\ x \\ y \\ a \\ b \\ c \\ d \end{bmatrix}$$

$$B \odot W = \begin{bmatrix} 1 & x & y & a & b & c & d \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \odot \begin{bmatrix} 1 \\ x \\ y \\ a \\ b \\ c \\ d \end{bmatrix}$$

$$C \odot W = \begin{bmatrix} 1 & x & y & a & b & c & d \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ -36 & 0 & 0 & 0 & 36 & 0 & -11 \end{bmatrix} \odot \begin{bmatrix} 1 \\ x \\ y \\ a \\ b \\ c \\ d \end{bmatrix}$$

Problem 2

Write python code that takes an R1CS matrix A, B, and C and a witness vector w and verifies:

$$Aw \odot Bw - Cw = 0$$

Where $\odot$ is the Hadamard (element-wise) product.
Use this code to check your answer above is correct.

Problem 3

Given an R1CS of the form

$$L[\vec{s}]_1 \odot R[\vec{s}]_2 = O[\vec{s}]_1 \odot [\vec{G_2}]_2$$

Where L, R, and O are n x m matrices of field elements and s is a vector of G1, G2, or G1 points

Write python code that verifies the formula.

You can check the equality of G12 points in Python this way:

```
a = pairing(multiply(G2, 5), multiply(G1, 8))
b = pairing(multiply(G2, 10), multiply(G1, 4))
eq(a, b)
```

Hint: Each row of the matrices is a separate pairing.

Hint: When you get s encrypted with both G1 and G2 generators, you don't know whether or not they have the same discrete logarithm. However, it is straightforward to check using another equation. Figure out how to discover if sG1 == sG2 if you are given the elliptic curve points but not s.

Solidity cannot multiply G2 points, do this assignment in Python.

Problem 4

Why does an R1CS require exactly one multiplication per row?

How does this relate to bilinear pairings?