Student Worksheet: R1CS and QAP Construction

This worksheet will help you build your understanding of R1CS (Rank-1 Constraint System) and QAP (Quadratic Arithmetic Program) by working through a simple arithmetic example.

# 🧠 Example Computation

Given the expression: z = (x + 1)(y + 2)

1. Draw the arithmetic circuit for this expression.  
2. Label each wire and gate. Use the table below to assign wire indices.

## 📌 Wire Index Table

Fill in the missing values below:

|  |  |
| --- | --- |
| Wire Name | Wire Index |
| x | \_\_\_\_ |
| y | \_\_\_\_ |
| a = x + 1 | \_\_\_\_ |
| b = y + 2 | \_\_\_\_ |
| z = a \* b | \_\_\_\_ |

# ✏️ R1CS Constraints

Write down the constraints for each gate in the form:

⟨uᵢ, d⟩ · ⟨vᵢ, d⟩ = ⟨wᵢ, d⟩

Use the table below to specify each constraint row:

## Constraint Matrix Rows (U, V, W)

Fill in each row vector below (assume vector length = 6).

|  |  |  |  |
| --- | --- | --- | --- |
| Constraint # | U[i] | V[i] | W[i] |
| 1 | [\_\_\_\_, \_\_\_\_, \_\_\_\_, \_\_\_\_, \_\_\_\_, \_\_\_\_] | [\_\_\_\_, \_\_\_\_, \_\_\_\_, \_\_\_\_, \_\_\_\_, \_\_\_\_] | [\_\_\_\_, \_\_\_\_, \_\_\_\_, \_\_\_\_, \_\_\_\_, \_\_\_\_] |
| 2 | [\_\_\_\_, \_\_\_\_, \_\_\_\_, \_\_\_\_, \_\_\_\_, \_\_\_\_] | [\_\_\_\_, \_\_\_\_, \_\_\_\_, \_\_\_\_, \_\_\_\_, \_\_\_\_] | [\_\_\_\_, \_\_\_\_, \_\_\_\_, \_\_\_\_, \_\_\_\_, \_\_\_\_] |
| 3 | [\_\_\_\_, \_\_\_\_, \_\_\_\_, \_\_\_\_, \_\_\_\_, \_\_\_\_] | [\_\_\_\_, \_\_\_\_, \_\_\_\_, \_\_\_\_, \_\_\_\_, \_\_\_\_] | [\_\_\_\_, \_\_\_\_, \_\_\_\_, \_\_\_\_, \_\_\_\_, \_\_\_\_] |

# 📐 QAP Polynomials

Based on your R1CS, write the polynomial expressions:

* - A(X) = ∑ d\_k · u\_k(X)
* - B(X) = ∑ d\_k · v\_k(X)
* - C(X) = ∑ d\_k · w\_k(X)
* - p(X) = A(X) · B(X) - C(X)
* - t(X) = (X - r₁)(X - r₂)... for domain roots

Leave space to write out the polynomials explicitly.