GROTH 16

START:

$$x^3 + x + 5 = 35$$

find x

① Use only + - · / x FLATTENING

~~$y = x \cdot x \cdot x$~~ $y = x \cdot x \cdot x$

~~$x \cdot x \cdot x + 5 = 35$~~ $x \cdot x \cdot x + x + 5 = 35$

$y + x + 5 = 35$

Flattening — something = something operation something

flattening means creating gates

G1 sym_1 = x · x

G2 y = sym_1 · x

G3 sym_2 = y + x

G4 ~out = sym_2 + 5

n

(2)

Gates to R1CS

~~Not~~ rank-1 constraint system

⇓

sequence of groups of three vectors (a, b, c)

and the solution to an R1CS is a vector s, where

s must satisfy the equation $s.a * s.b - s.c = 0$

where $.$ represents the dot product

A		B		C	
1	5	1	1	1	0
3	0	3	0	3	0
35	0	35	0	35	1
9	0	9	0	9	0
27	0	27	0	27	0
30	1	30	0	30	0

$1 \cdot 5 + 30 \cdot 1$ (A) $\quad 1 \cdot 1$ (B) $\quad 35 \cdot 1$ (C)

$$35 \cdot 1 - 35 = 0$$

Variable mapping

[one, x, out, sym_1, y, sym_2]

[1, 3, 35, 9, 27, 30]

GATE #1

sym_1 = x · x

9 = 3 · 3

3 · 3 − 9 = 0

A B C

	A		B		C
1	0	1	0	1	0
3	1	3	1	3	0
35	0	35	0	35	0
9	0	9	0	9	1
27	0	27	0	27	0
30	0	30	0	30	0

a = [0, 1, 0, 0, 0, 0]

b = [0, 1, 0, 0, 0, 0]

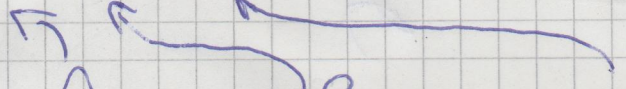
c = [0, 0, 0, 1, 0, 0]

GATE #2

$y = sym\_1 \cdot x$

$27 = 9 \cdot 3$

$9 \cdot 3 - 27 = 0$



A		B		C	
1	0	1	0	1	0
3	0	3	1	3	0
35	0	35	0	35	0
9	1	9	0	9	0
27	0	27	0	27	1
30	0	30	0	30	0

$a = [0, 0, 0, 1, 0, 0]$

$b = [0, 1, 0, 0, 0, 0]$

$c = [0, 0, 0, 0, 1, 0]$

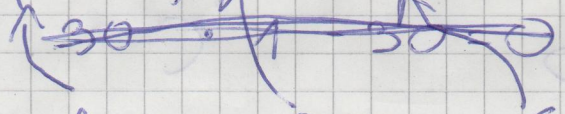
GATE #3

sym-2 = y + x

30 = 27 + 3

27 + 3 − 30 = 0

$(\overset{A}{27}+\overset{B}{3})\cdot\overset{C}{1}-30=0$



	A		B		C
1	0	1	1	1	0
3	1	3	0	3	0
35	0	35	0	35	0
9	0	9	0	9	0
27	1	27	0	27	0
30	0	30	0	30	1

a = [0, 1, 0, 0, 1, 0]

b = [1, 0, 0, 0, 0, 0]

c = [0, 0, 0, 0, 0, 1]

GATE #4

$\sim out = sym\_2 + 5$

$35 = 30 + 5$

$30 + 5 - 35 = 0$

$(\overset{A}{30}+5) \cdot \overset{B}{1} - \overset{C}{35} = 0$

A		B		C	
1	5	1	1	1	0
3	0	3	0	3	0
35	0	35	0	35	1
9	0	9	0	9	0
27	0	27	0	27	0
30	1	30	0	30	0

$a = [5, 0, 0, 0, 0, 1]$

$b = [1, 0, 0, 0, 0, 0]$

$c = [0, 0, 1, 0, 0, 0]$

R1C5

$$a = \begin{bmatrix} 0,1,0,0,0,0 \\ 0,0,0,1,0,0 \\ 0,1,0,0,1,0 \\ 5,0,0,0,0,1 \end{bmatrix}$$

$$b = \begin{bmatrix} 0,1,0,0,0,0 \\ 0,1,0,0,0,0 \\ 1,0,0,0,0,0 \\ \text{[illegible]} \\ 1,0,0,0,0,0 \end{bmatrix}$$

$$c = \begin{bmatrix} 0,0,0,1,0,0 \\ 0,0,0,0,1,0 \\ 0,0,0,0,0,1 \\ 0,0,1,0,0,0 \end{bmatrix}$$

(3) R1CS to QAP

QAP - quadratic assignment problem

four groups of three vectors of length six

↓

six groups of three degree-3 polynomials

where evaluating the ~~polyn~~ polynomials at each x coordinate represents one of the constraints.

If we evaluate the polynomials at $x=1$, then we get our first set of vectors, if $x=2$ then second and so on...

Transformation is done by Lagrange ~~interpol~~ interpolation.

Lagrange interpolation EXAMPLE

I points: (1,3), (2,2), (3,4)

Lagrange points: 2 → 0, 4 → 0

(1,3), (2,0), (3,0)

$y = (x-2)\cdot(x-3)$

(p1) $y = (1-2)\cdot(1-3)$

$y = (-1)\cdot(-2)$

$y = 2$ should be 3

(p2) $y = (2-2)\cdot(2-3)$

$y = 0$

(p3) $y = (3-2)\cdot(3-3)$

$y = 0$

II Rescale (p1) $y = (x-2)\cdot(x-3)$ to make $x=1$ be $y=3$

$(x-2)\cdot(x-3) / ((1-2)\cdot(1-3)) =$

$= 1.5\cdot x^2 - 7.5\cdot x + 9$

(p1) $y = 1\frac{1}{2}x^2 - 7\frac{1}{2}x + 9$ $\quad x=1 \quad y=?$

$y = 1\frac{1}{2} - 7\frac{1}{2} + 9$

$y = -6 + 9$

$y = 3$ correct

(p2) $x = 2$

$y = 1\frac{1}{2}x^2 - 7\frac{1}{2}x + 9$

$y = 1\frac{1}{2} \cdot 2^2 - 7\frac{1}{2} \cdot 2 + 9$

$y = \frac{3}{2} \cdot 4 - \frac{15}{2} \cdot 2 + 9$

$= \frac{12}{2} - \frac{30}{2} + 9$

$y = 6 - 15 + 9$

$y = -9 + 9$

$y = 0$ correct

(p3) $x = 3$

$y = 1\frac{1}{2}x^2 - 7\frac{1}{2}x + 9$

$= \frac{3}{2} \cdot 3^2 - \frac{15}{2} \cdot 3 + 9$

$= \frac{3}{2} \cdot 9 - \frac{15}{2} \cdot 3 + 9$

$= \frac{27}{2} - \frac{45}{2} + 9$

$y = -\frac{18}{2} + 9$

$y = 0$ correct

III Rescade (p2)

IV Rescade (p3)

Final

$$y = 1\frac{1}{2}x^2 - 5\frac{1}{2}x + 7$$

(p1)

$$y = 1\frac{1}{2}\cdot 1^2 - 5\frac{1}{2}\cdot 1 + 7$$
$$y = \frac{3}{2}\cdot 1 - \frac{11}{2}\cdot 1 + 7$$
$$y = \frac{3}{2} - \frac{11}{2} + 7$$
$$y = -\frac{8}{2} + 7$$
$$y = -4 + 7$$
$$y = 3 \quad \text{corect}$$

(p2)

$$y = 1\frac{1}{2}\cdot 2^2 - 5\frac{1}{2}\cdot 2 + 7$$
$$y = \frac{3}{2}\cdot 4 - \frac{11}{2}\cdot 2 + 7$$
$$y = \frac{12}{2} - \frac{22}{2} + 7$$
$$y = 6 - 11 + 7$$
$$y = -5 + 7$$
$$y = 2 \quad \text{corect}$$

(P3)

$y = 1\frac{1}{2} \cdot 3^2 - 5\frac{1}{2} \cdot 3 + 7$

$y = \frac{3}{2} \cdot 9 - \frac{11}{2} \cdot 3 + 7$

$y = \frac{27}{2} - \frac{33}{2} + 7$

$y = -\frac{6}{2} + 7$

$y = -3 + 7$

$y = 4$ correct