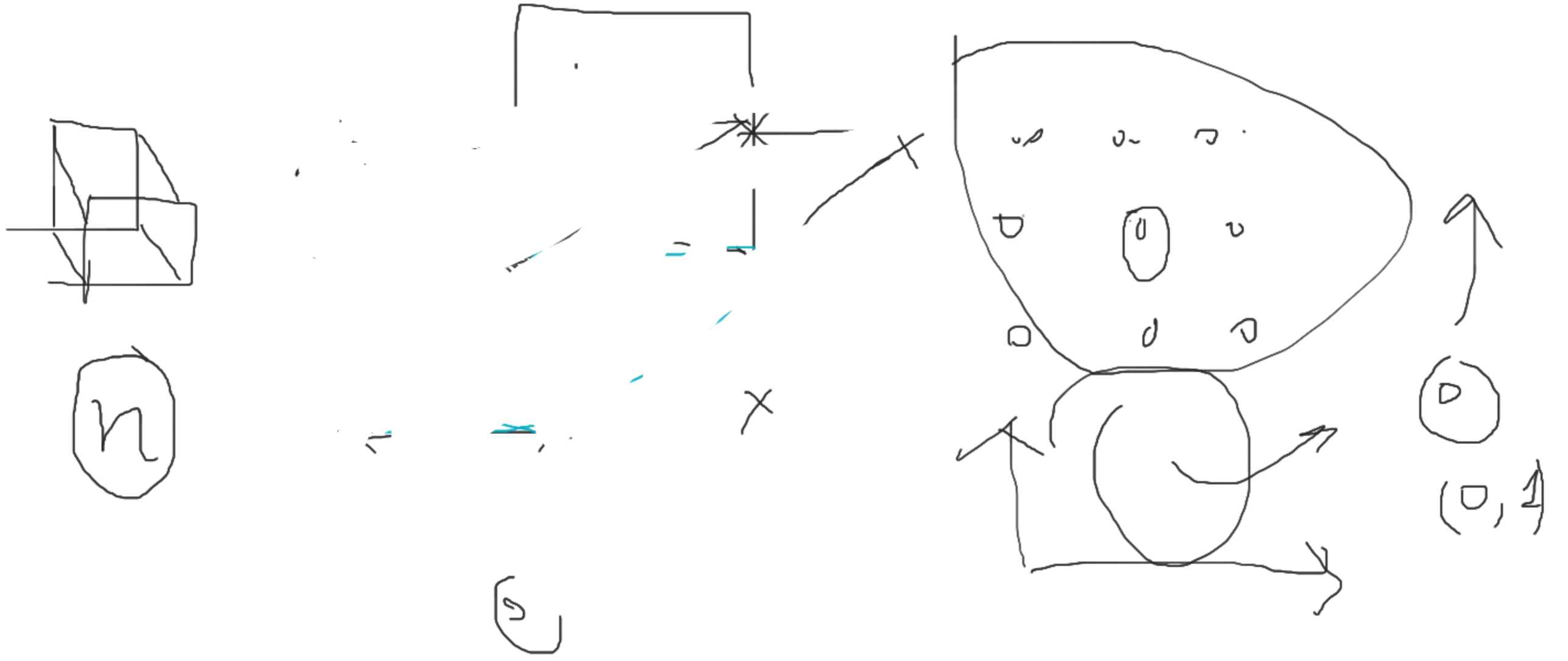
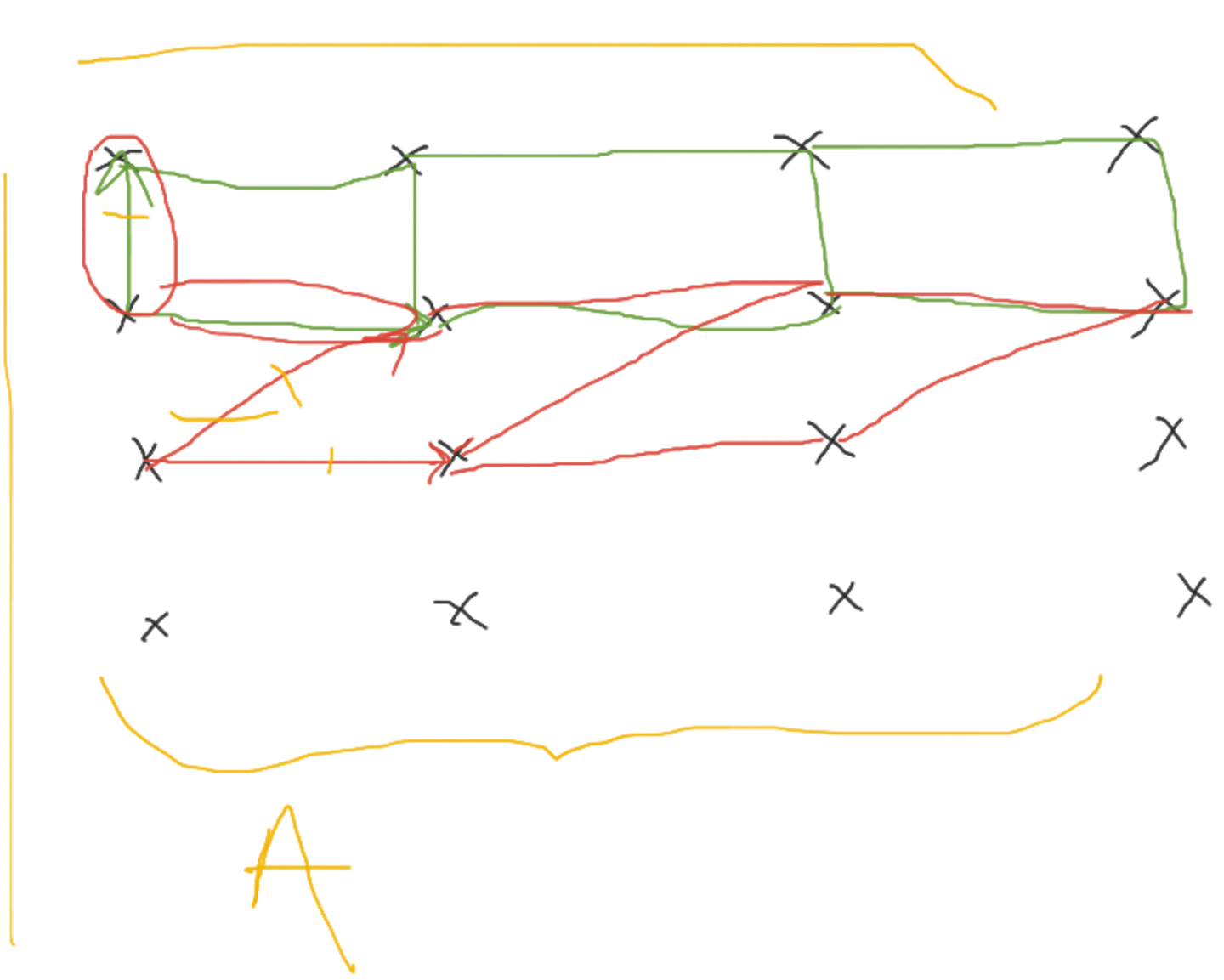
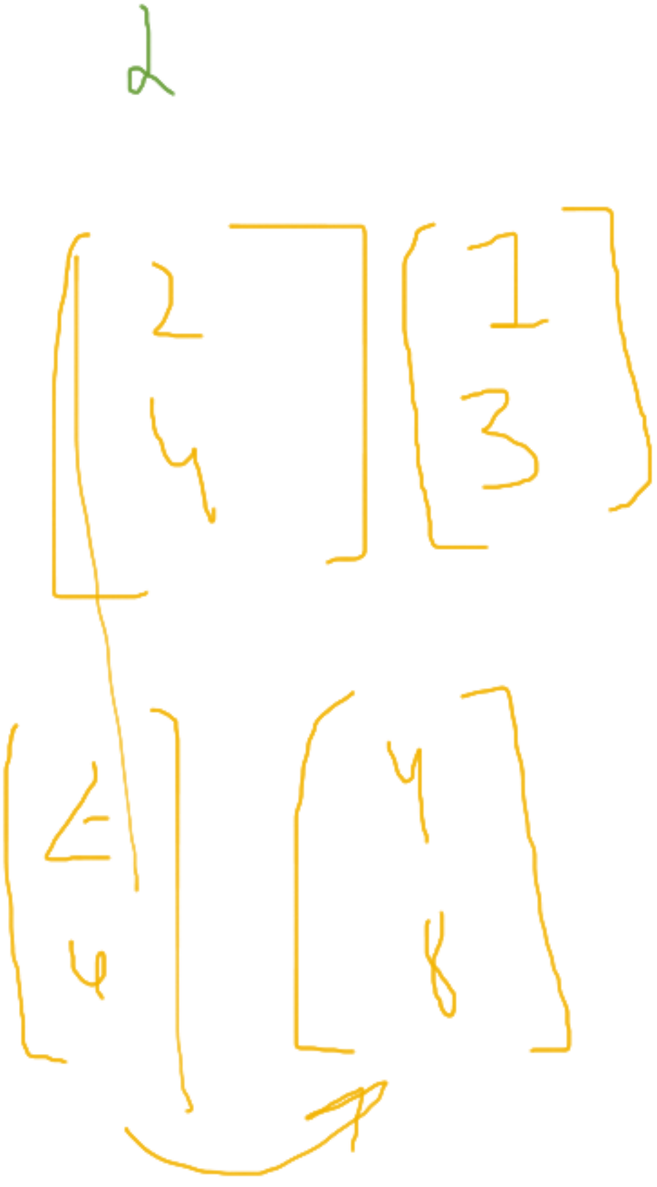
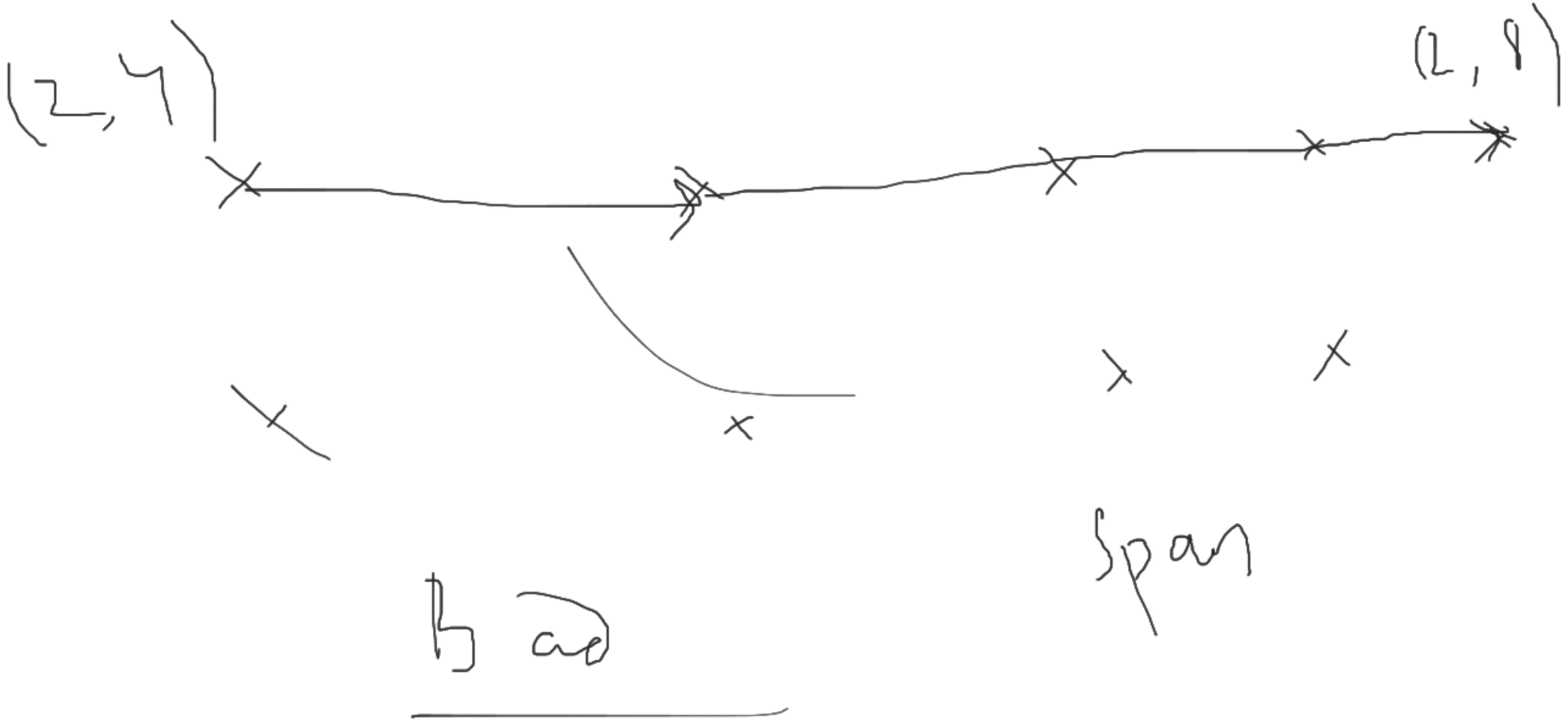
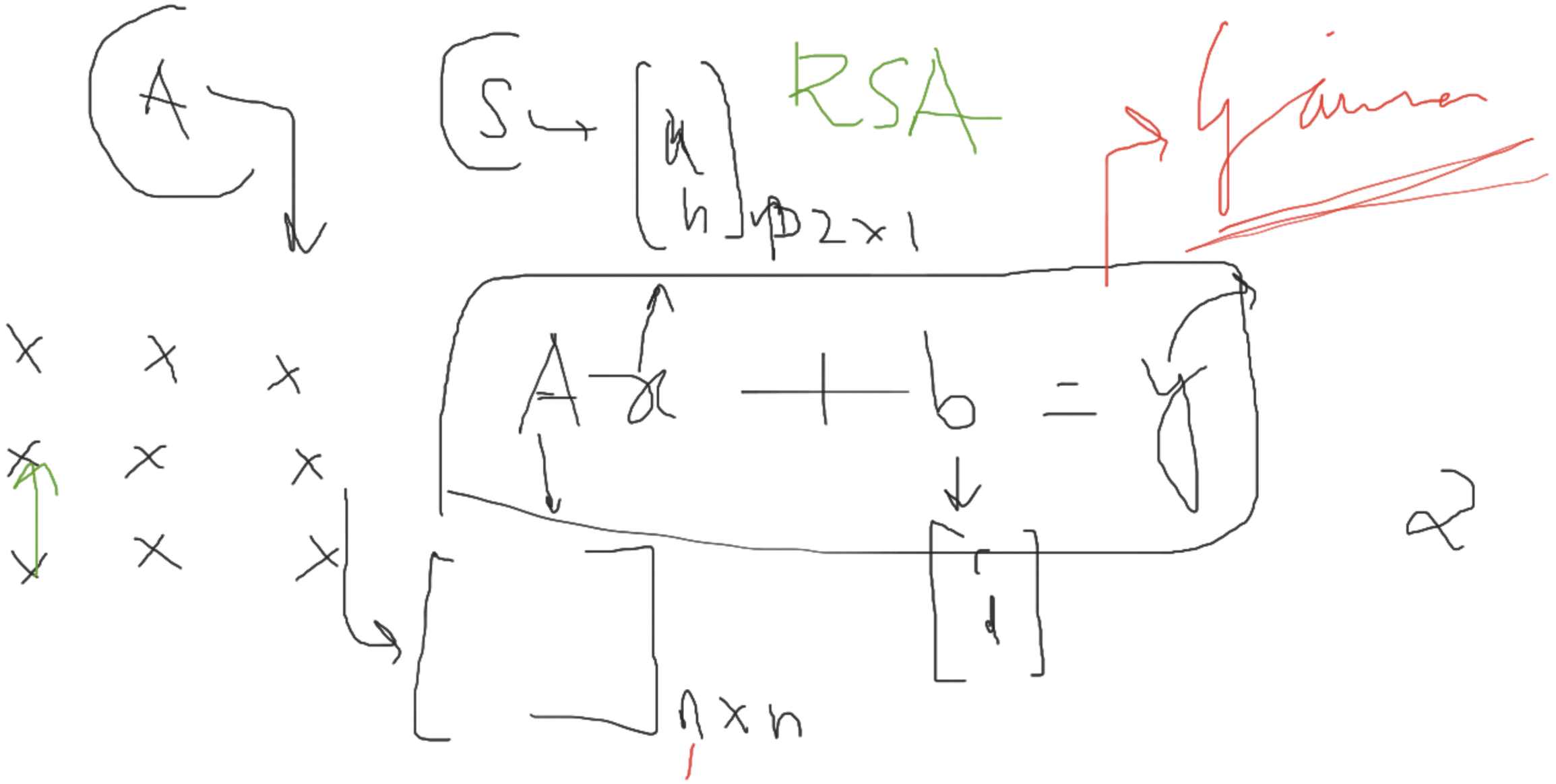
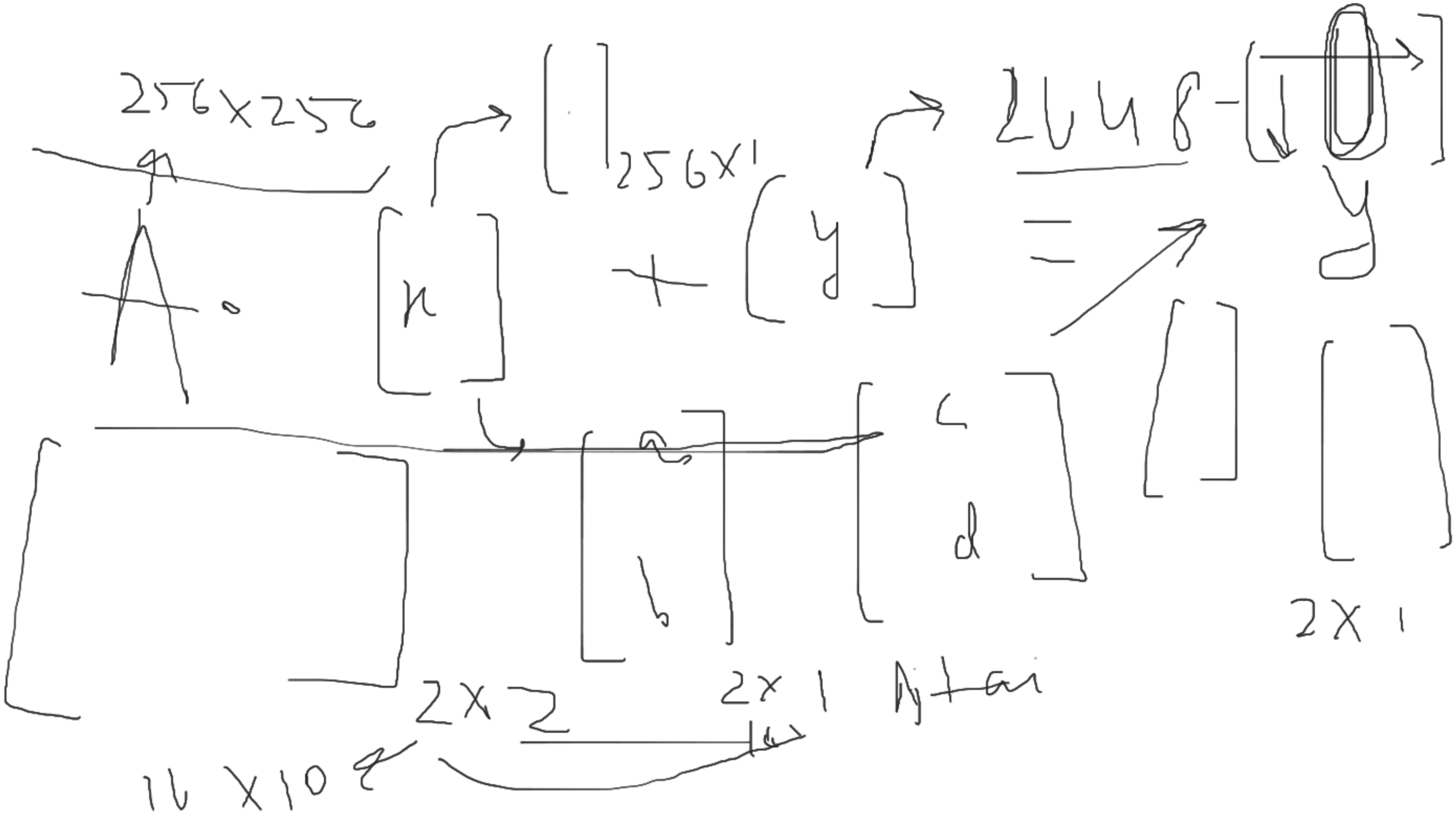



A




(2, 6)
(2, 9)
span
basis


A
S
RSA
2 x 1
A x + b = y
n x n
1


256x256
A
256x1
x
y
2448
a
b
c
d
2x1
2x2
2x1 Aktari
16 x 10

SVP

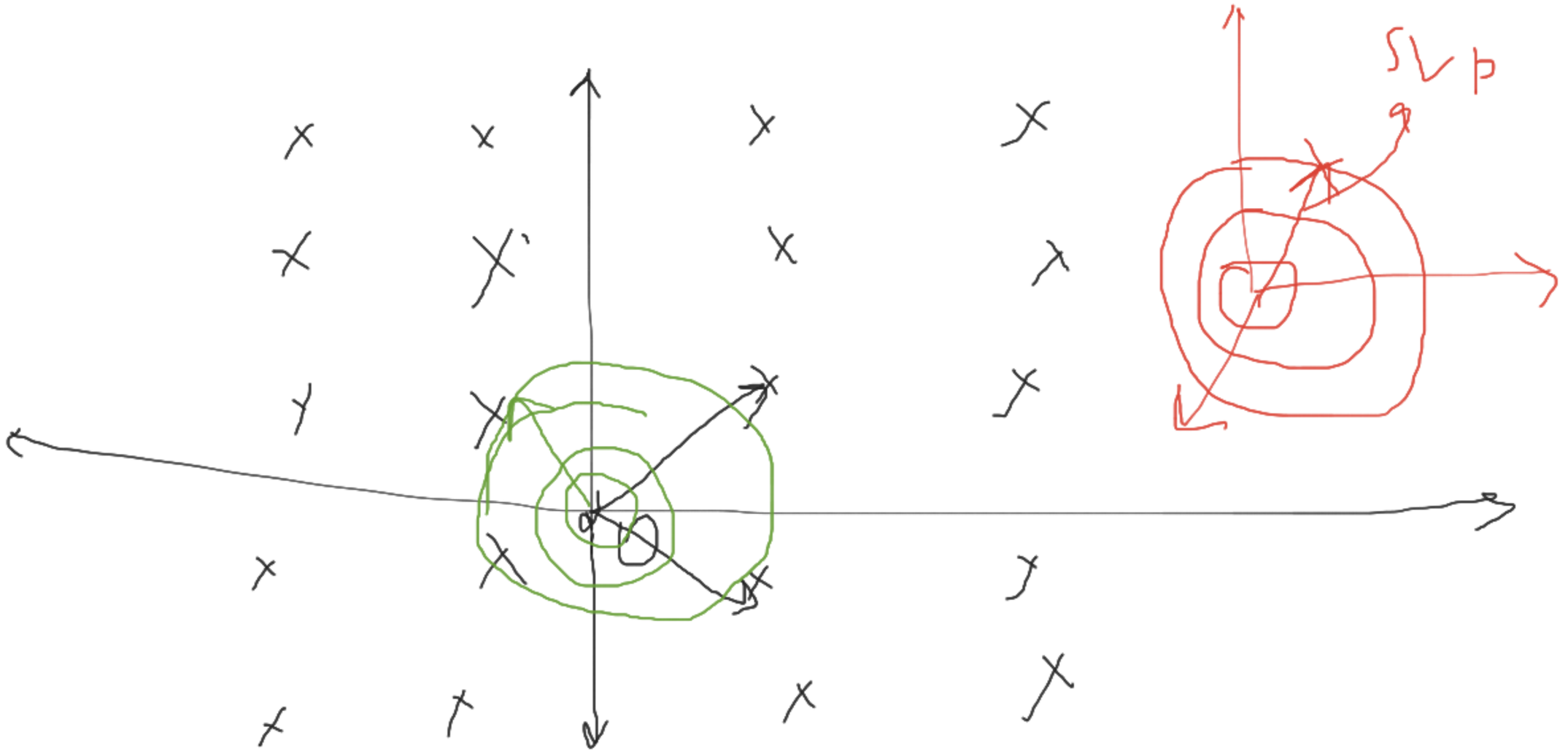
$Ax + bx = y$

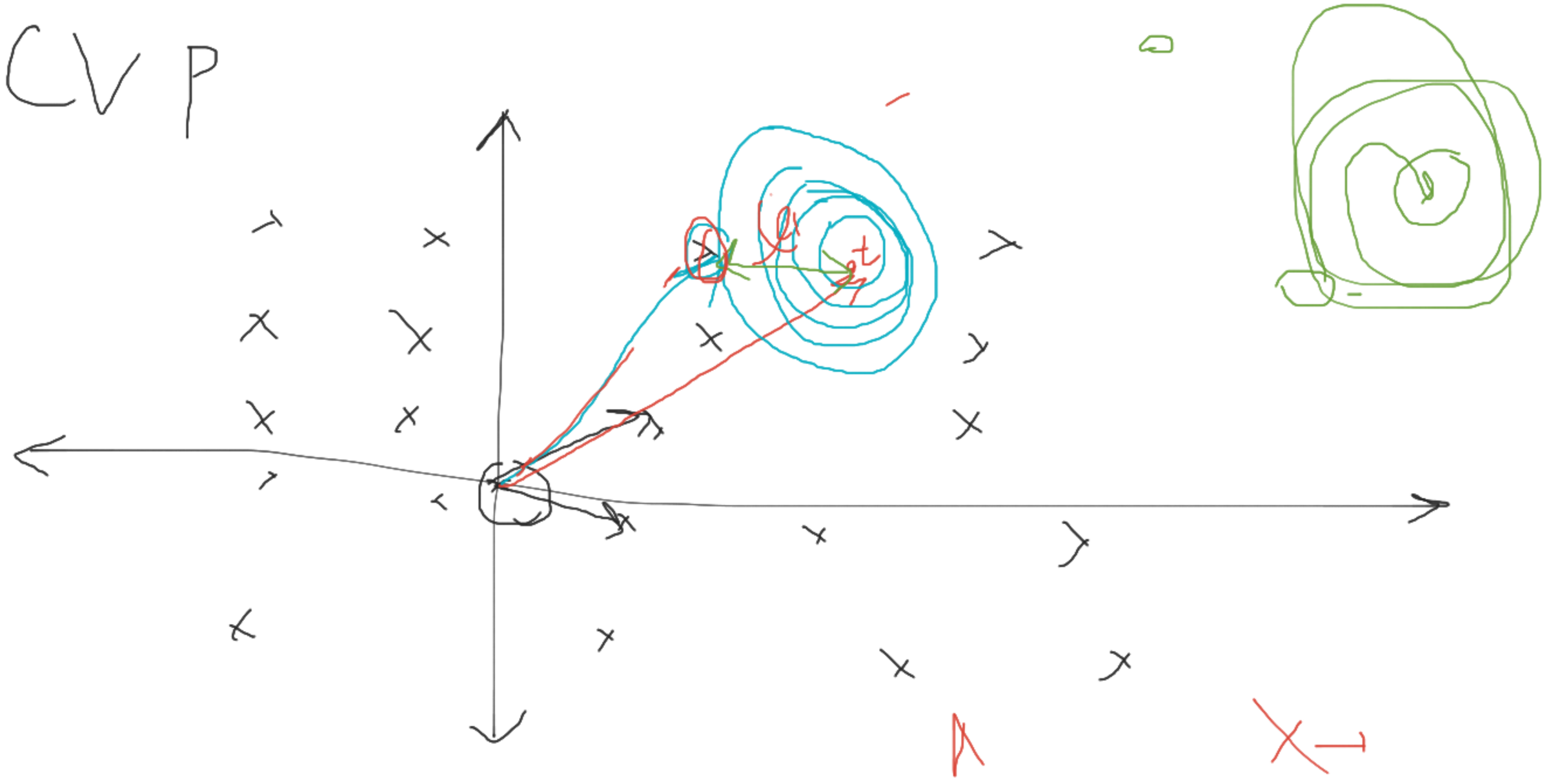
find x

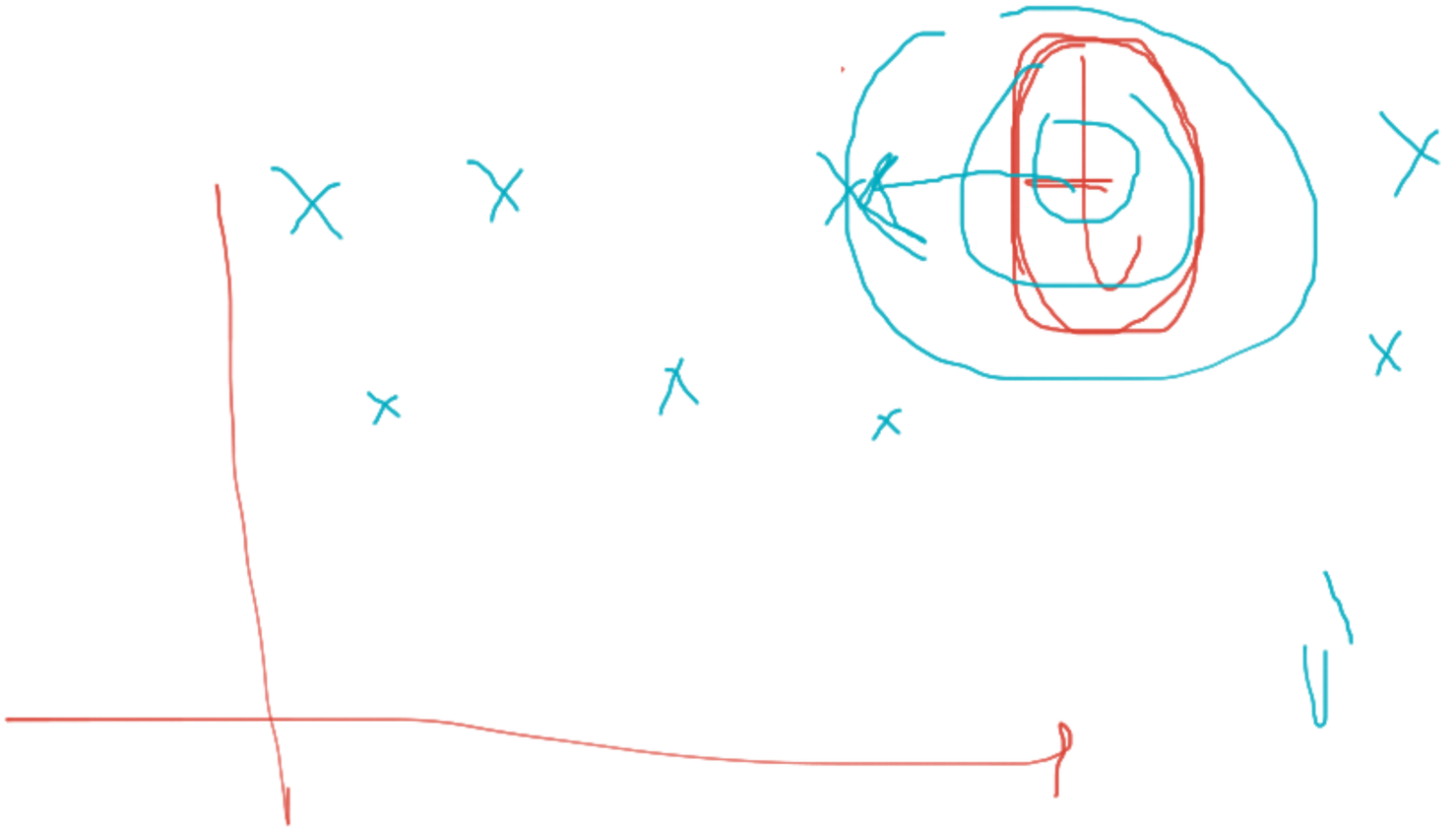
$[\,]\ [\,]\ [\,]$

$Ax + b = 0$

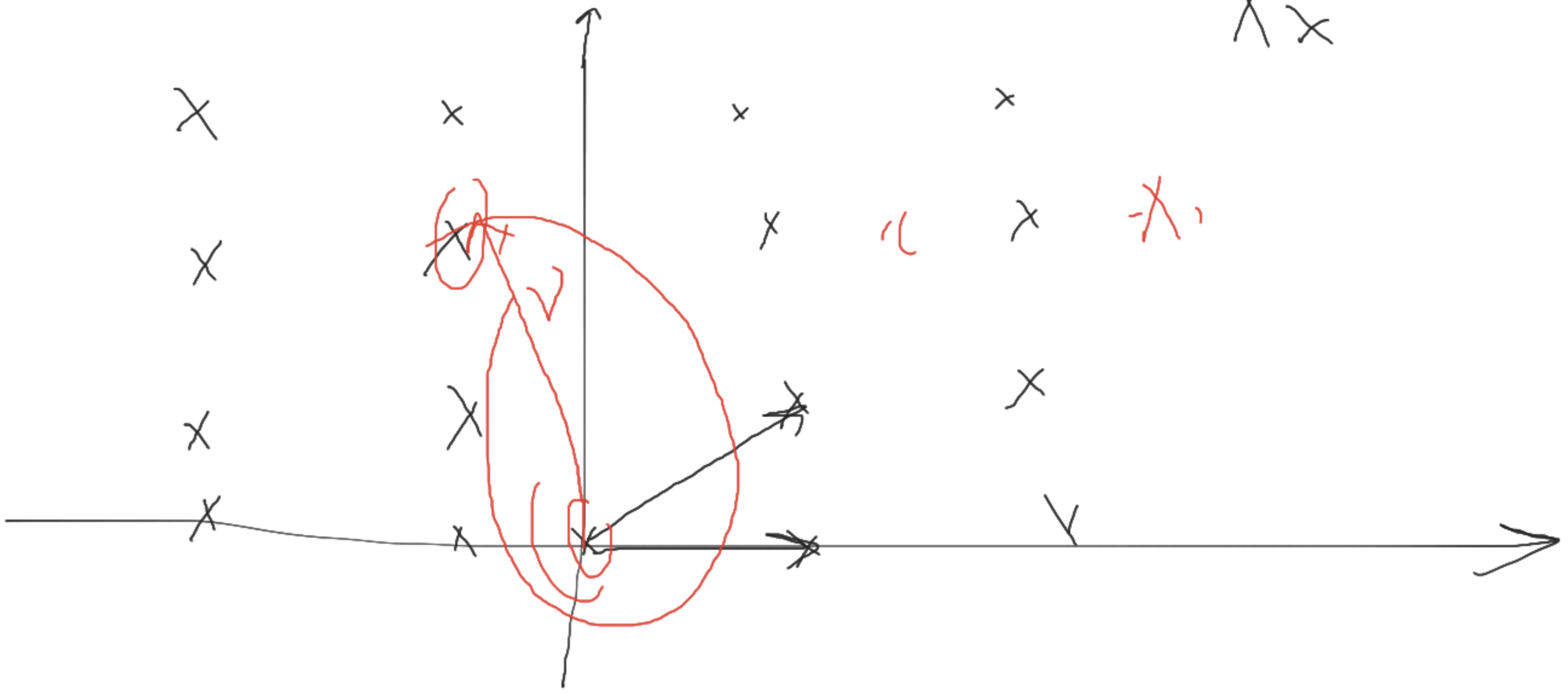
$Ax + tb = y$

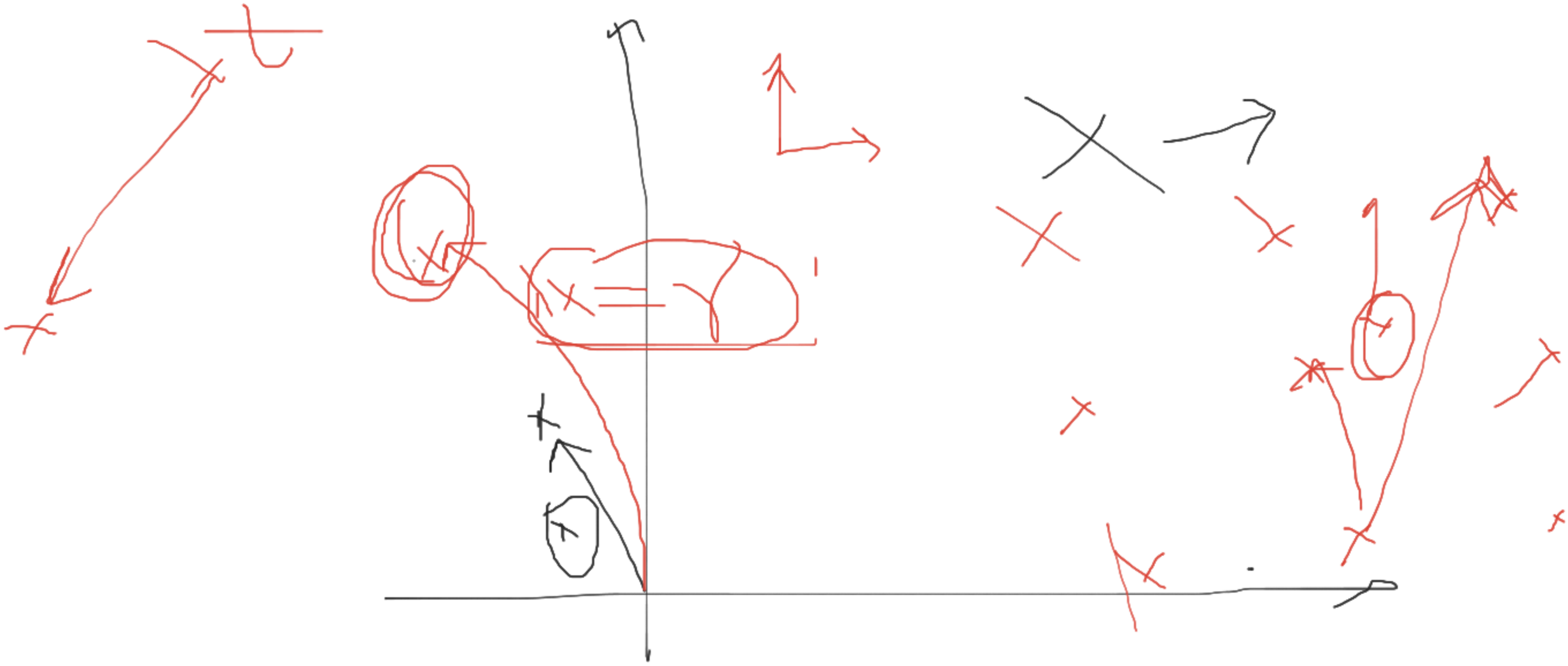

SLp

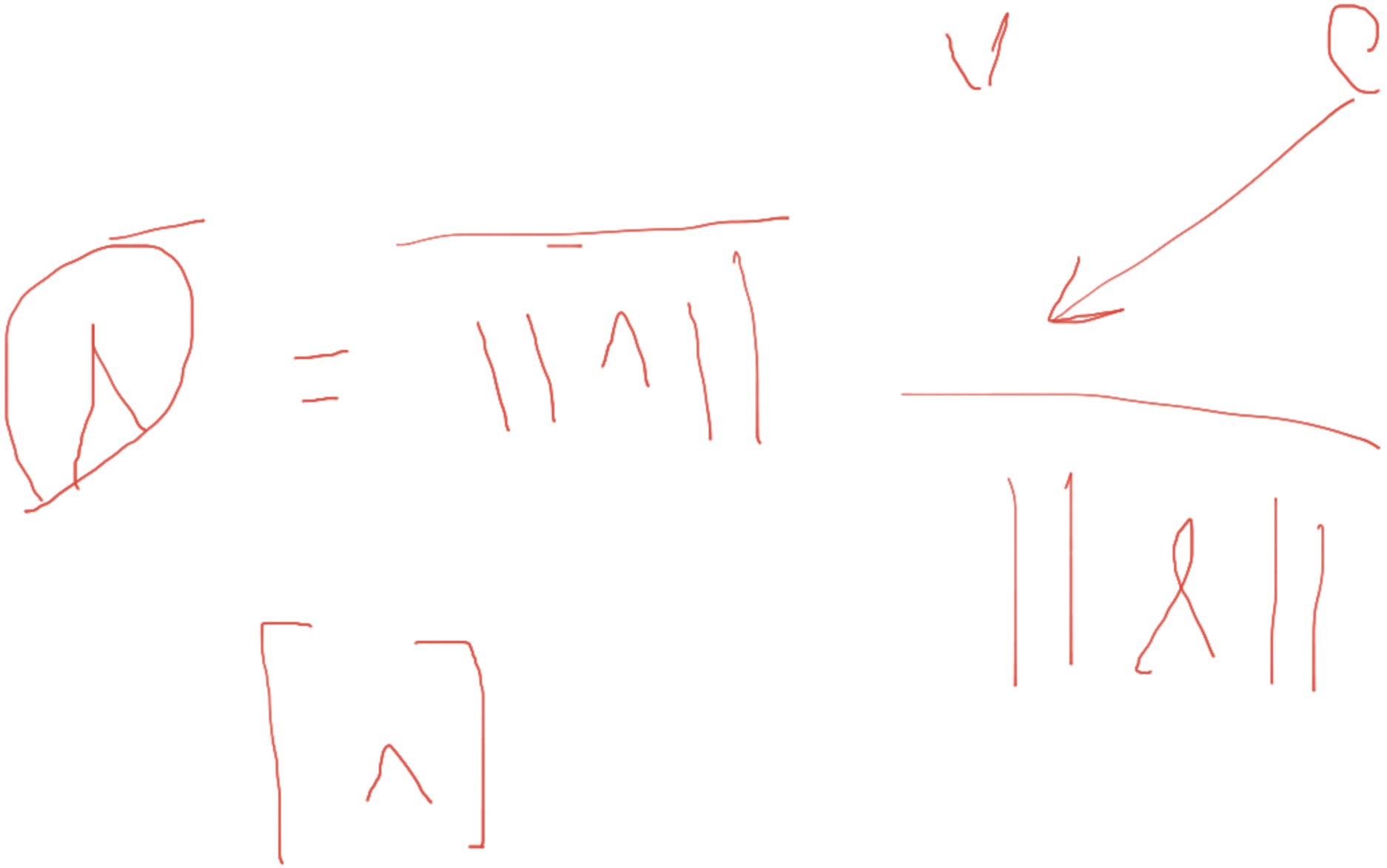

CV P
t

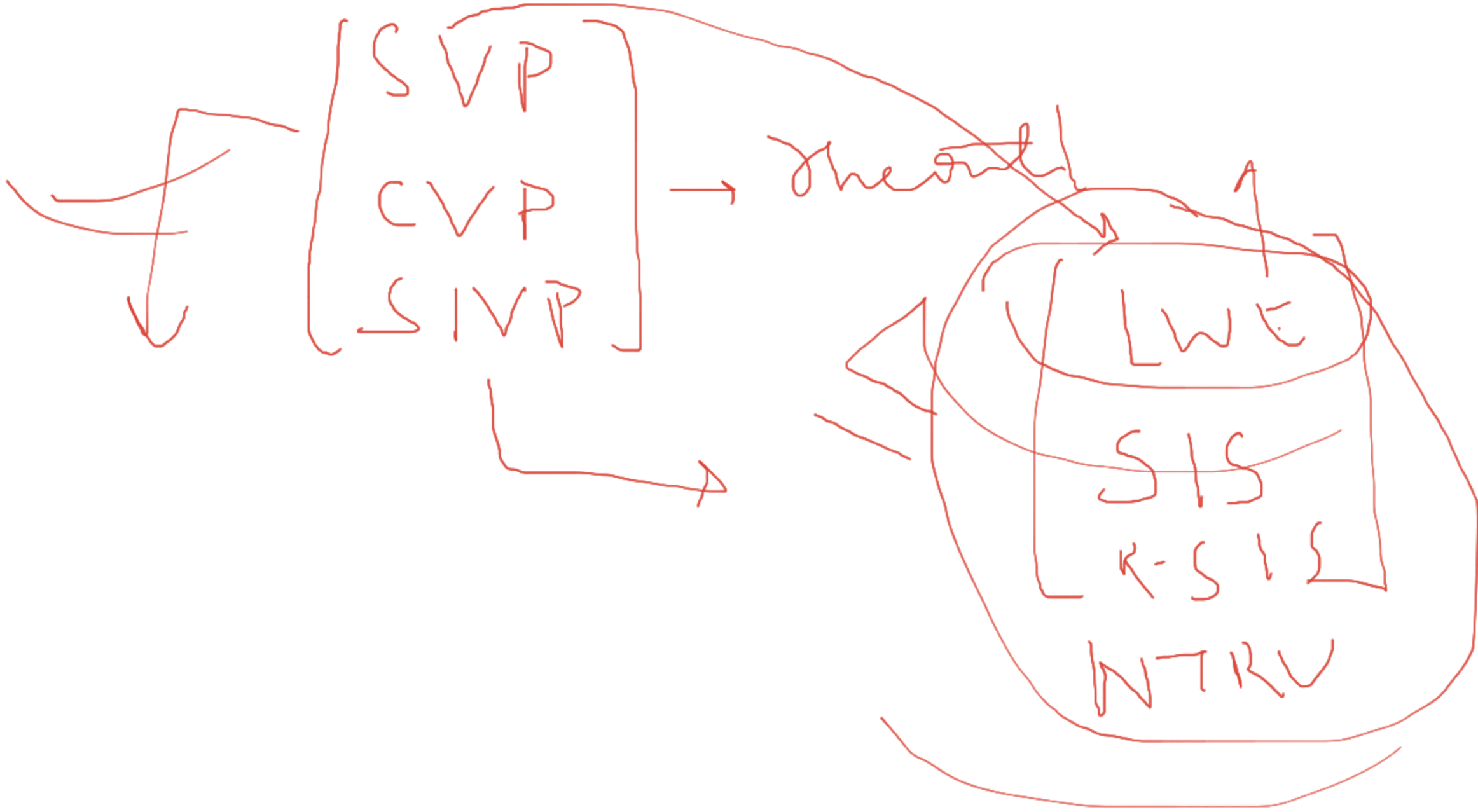


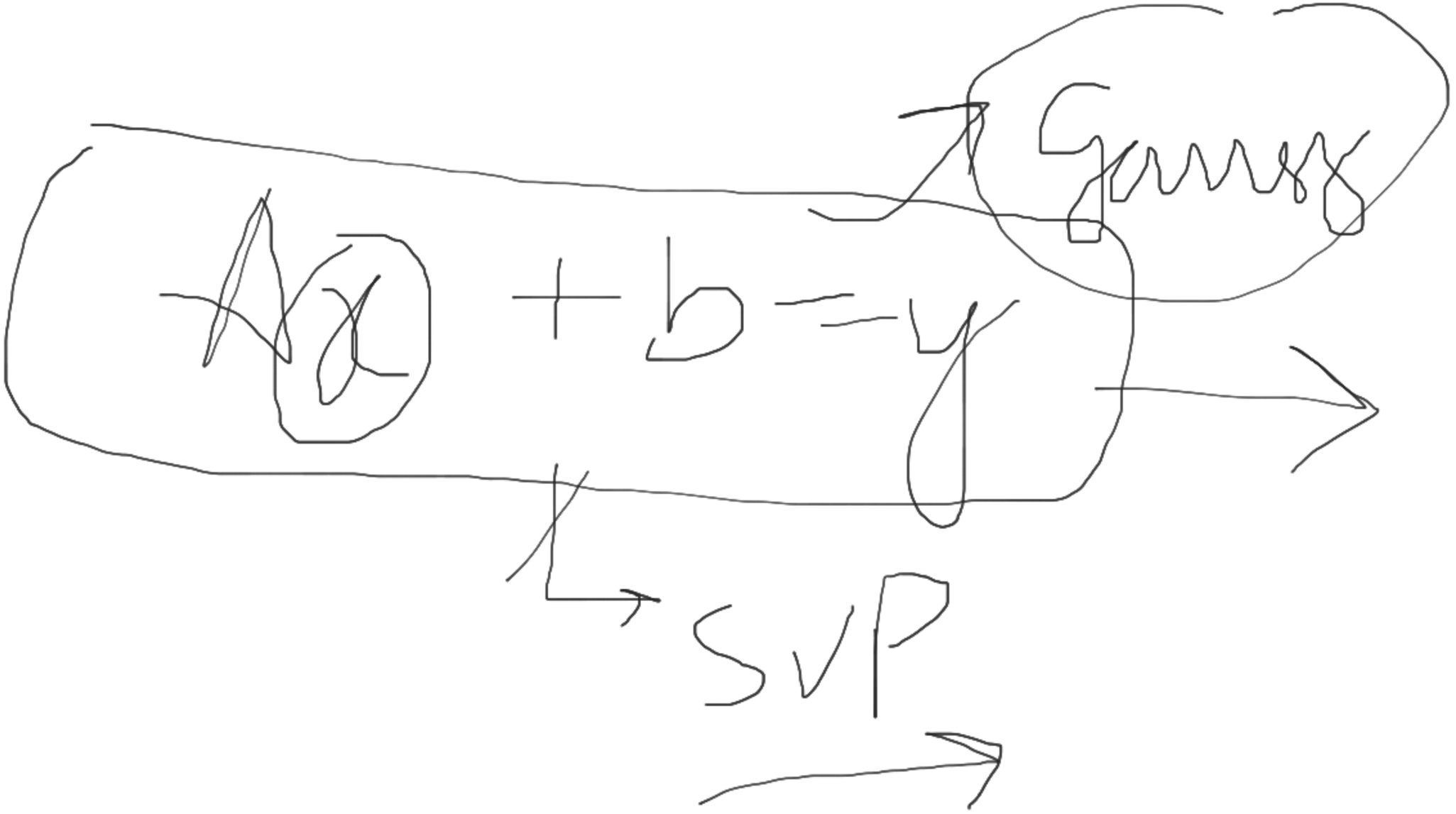
3 V-approx SVP



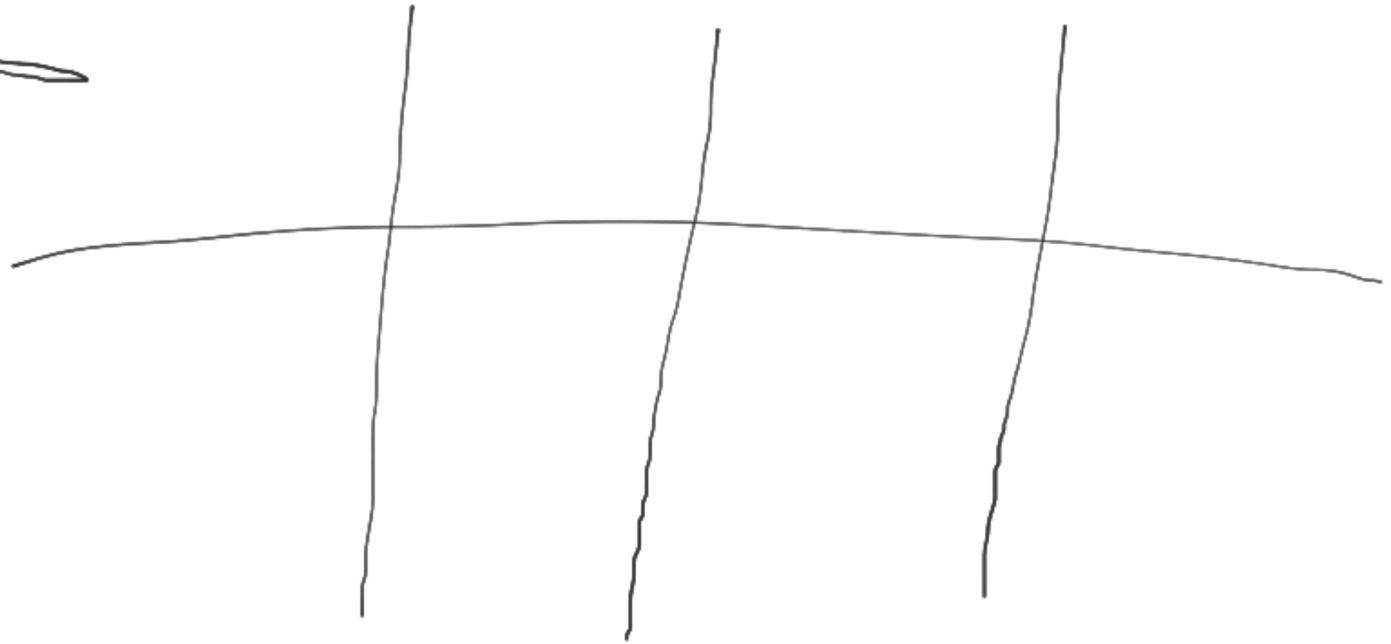


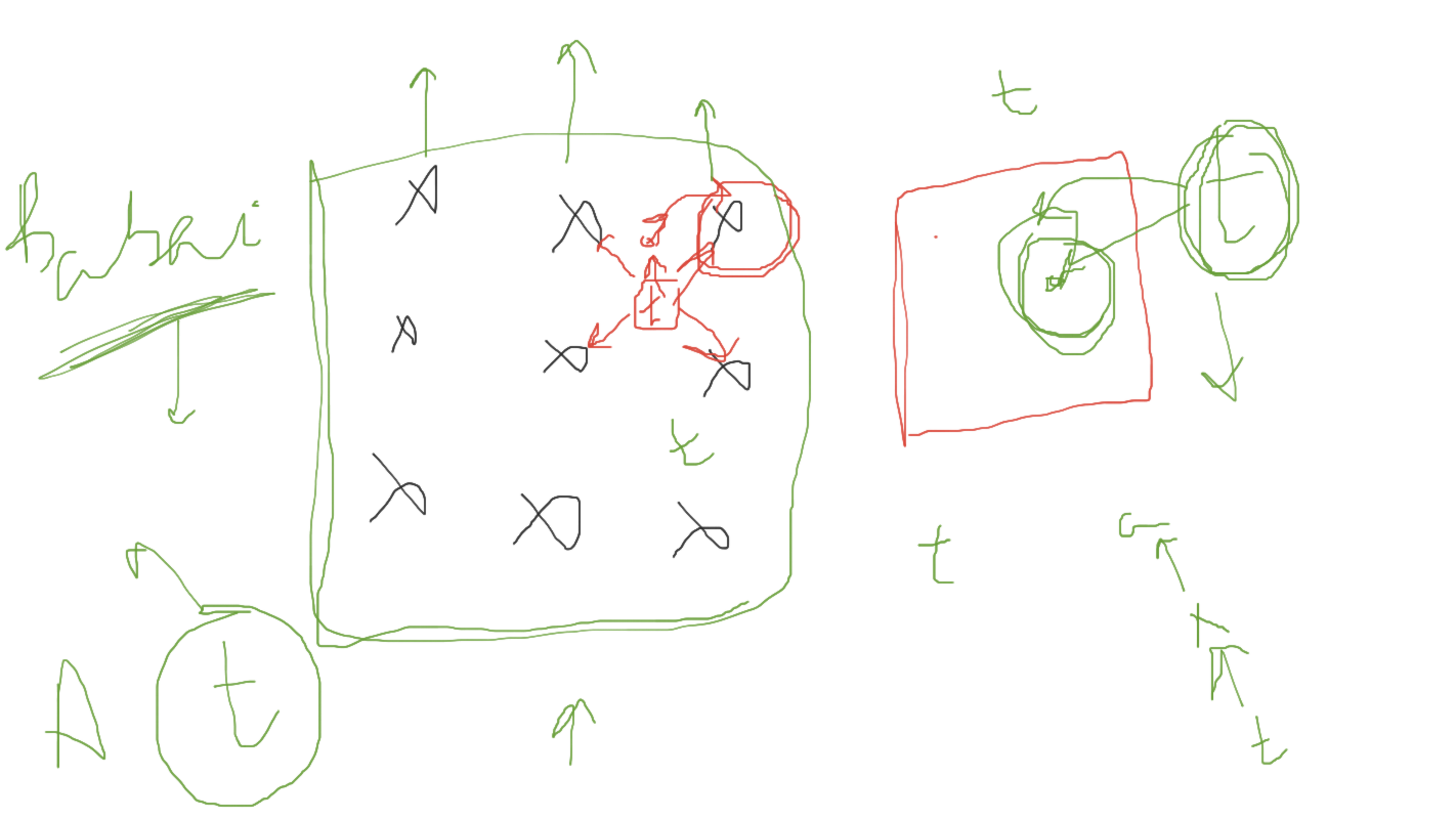


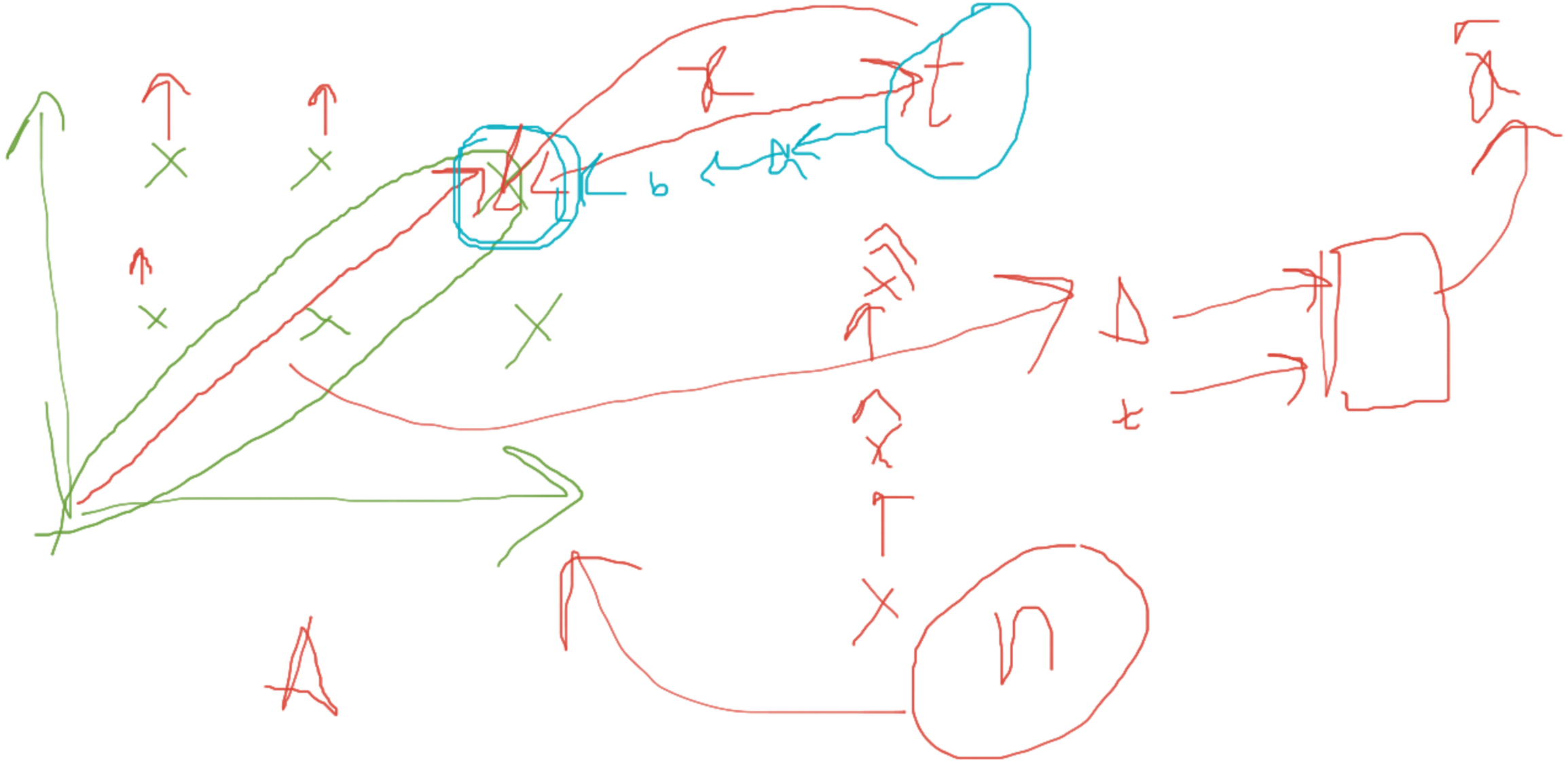

SVP
CVP
SIVP
LWE
SIS
K-SIS
NTRU

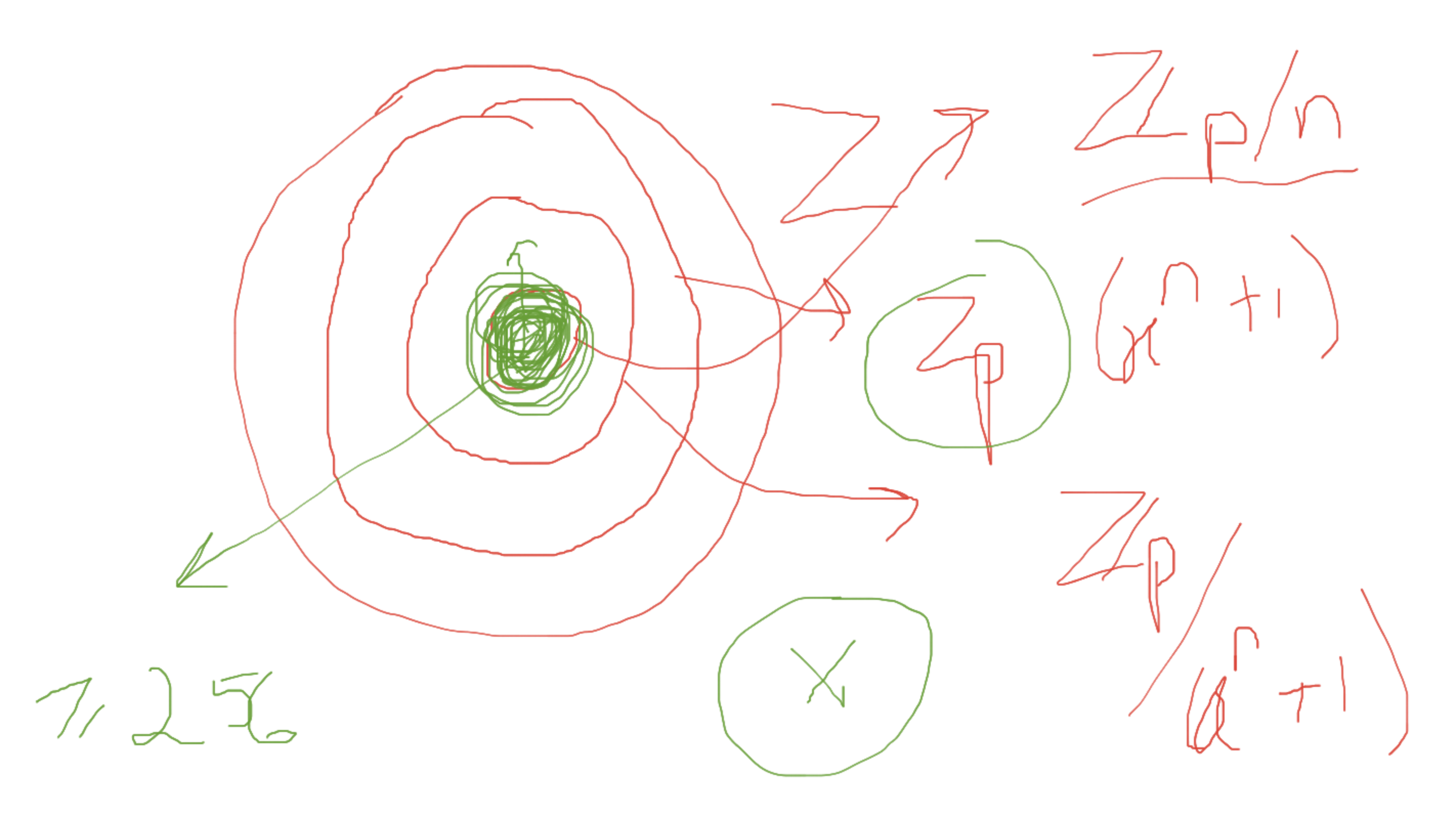

Ax + b = y
Softmax
SVP

CVP





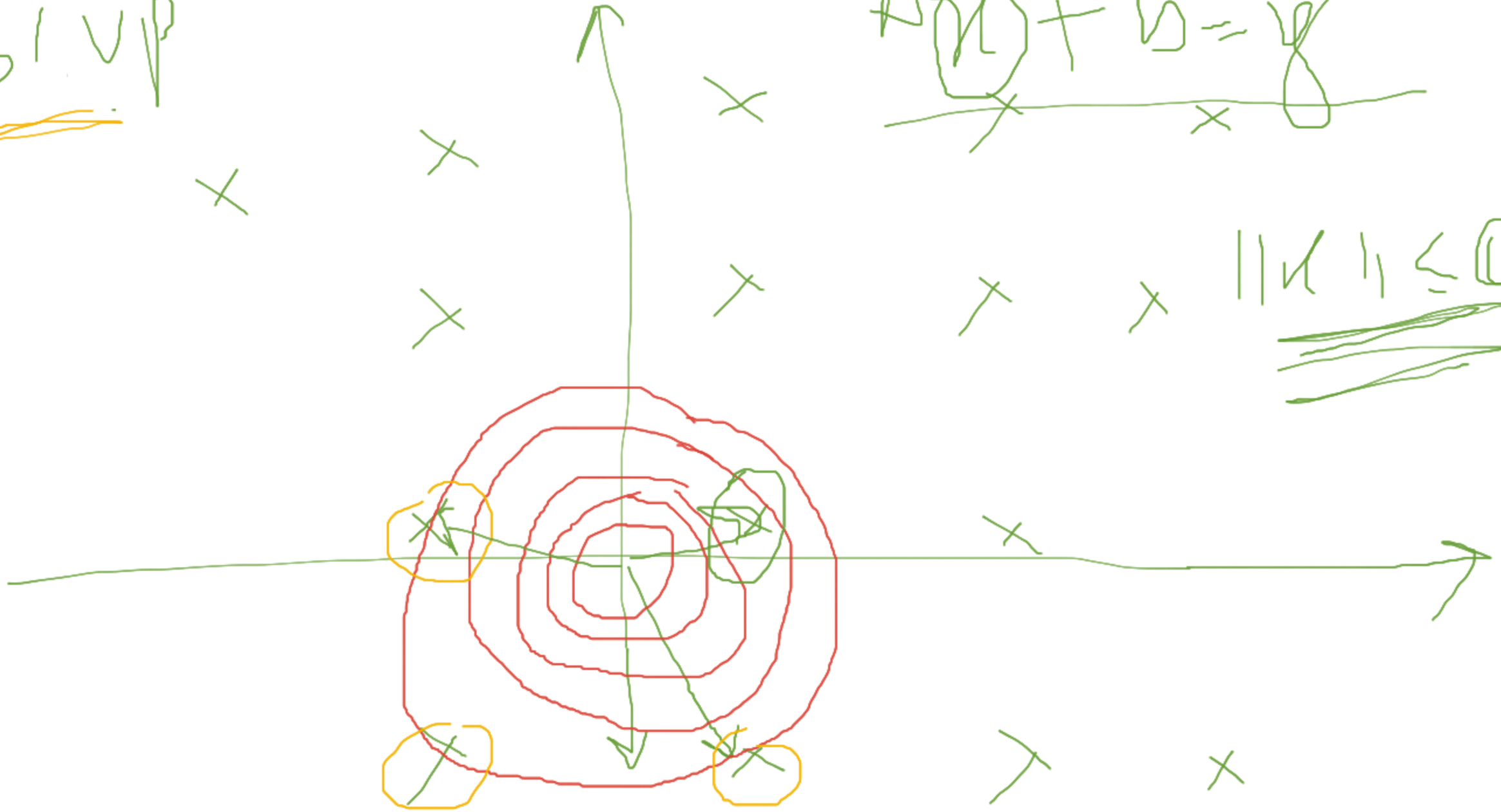


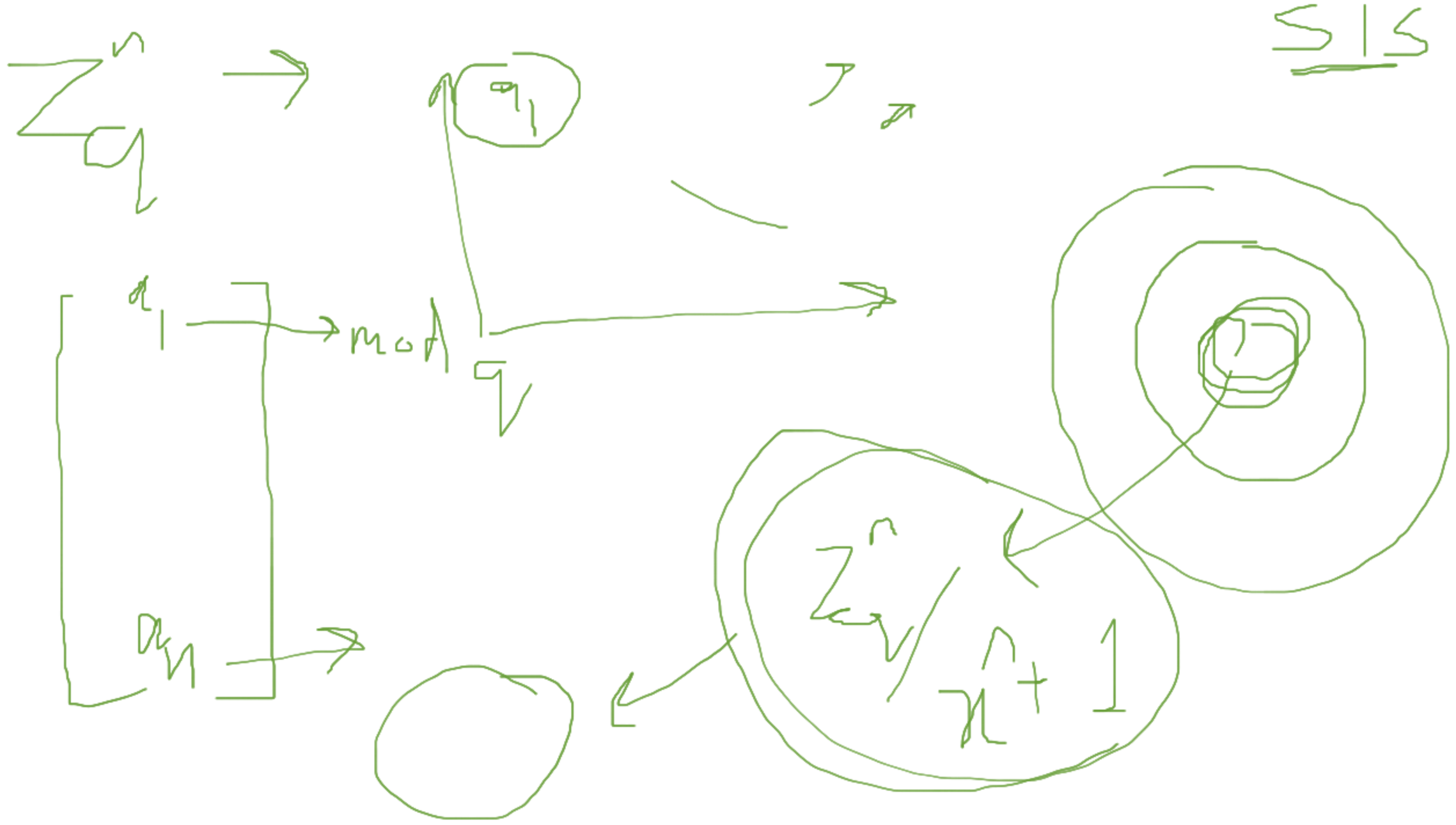

Z_{p^n}
(p^n+1)
Z_p
Z_{p^r}
(p^r+1)
X

Sup

$Ax + b = y$

$\|x\| \leq 1$




S | S
mod