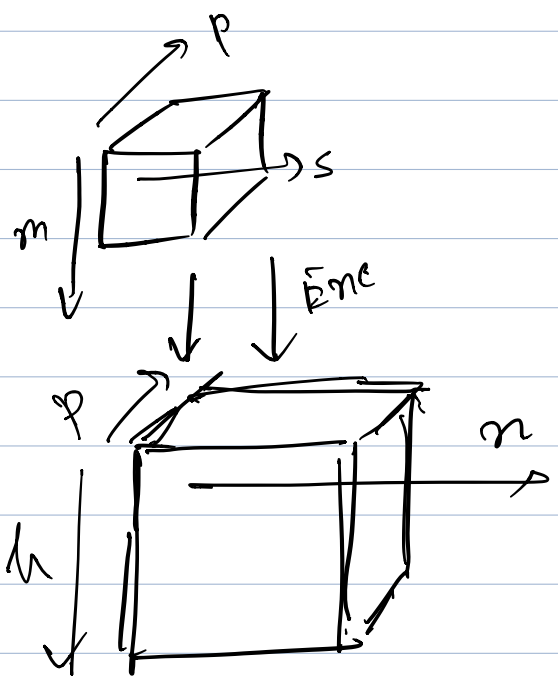
$N = pms$ – circuit size

Soundness – $2^{-\lambda}$

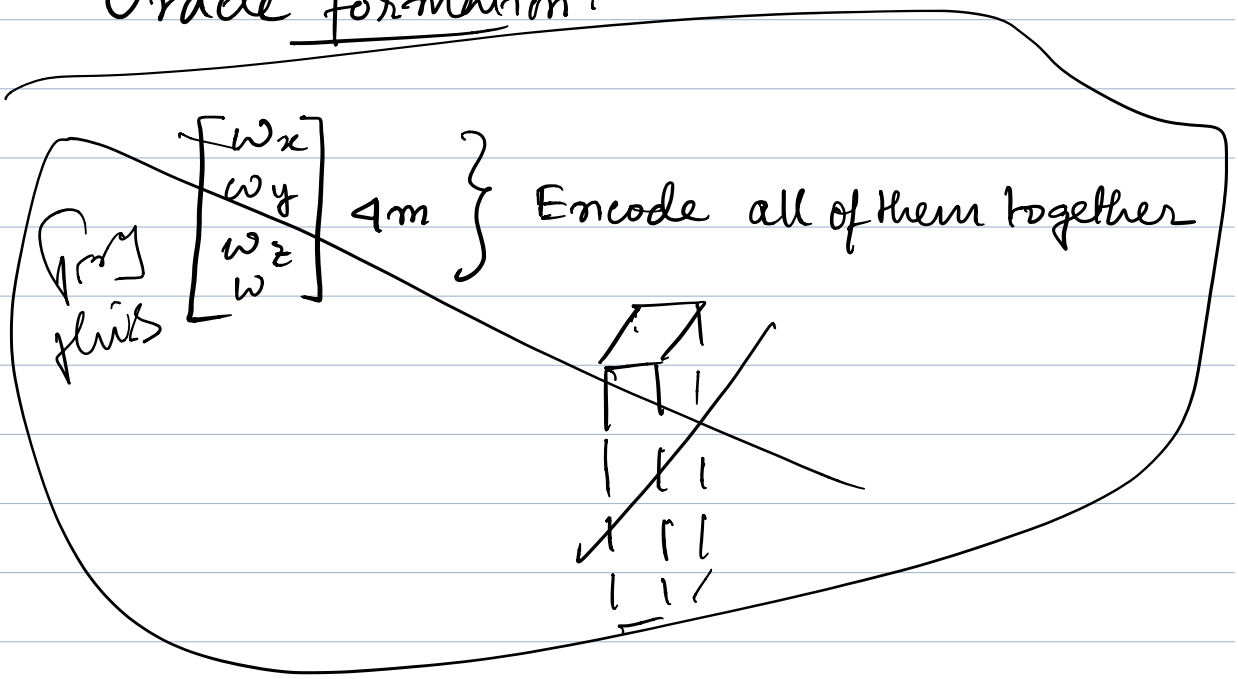
Proof size :



Verifier's time :

Prover's time :

Oracle formation :



Proof size: $4\ell + 3(s+\ell) + t.3p$

$+ t.3p$

$2\ell + t3p + 3pt$

Inner product: $8t(2\log m + 2)$

(Groth inner product)

Total = $16t \log m + 20t + 9\ell + 3s + 12tp$

Verifier's Time:

$O(N) + 8t$

$Aw = xw_x$

$[A\,|\,-I] \begin{bmatrix} w \\ w_x \end{bmatrix} = 0$

$Aw = b$

Check optimization of combining of Lincheck

$O(N) + 4t.\text{mult\_exp}(2m) + 4t.\text{mult\_exp}(m)$

Prover's Complexity:

Encoding time: $4pm(FFT(\ell)+FFT(n)) + 4pn(FFT(m)+FFT(h))$

Commiting time: $p\ell.mult\_exp(m) + p(n-\ell).mult\_exp(min(\ell,m))$

Subprotocol: $8tm\ exp$

$t \leftarrow$