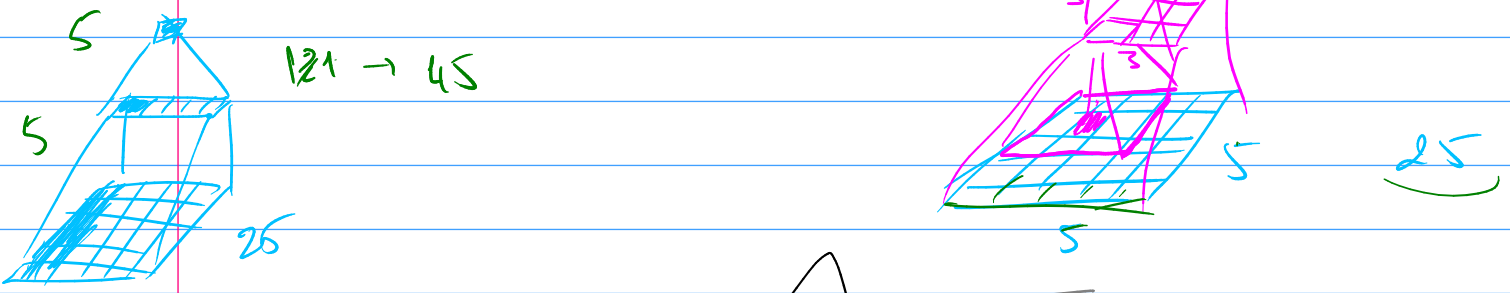
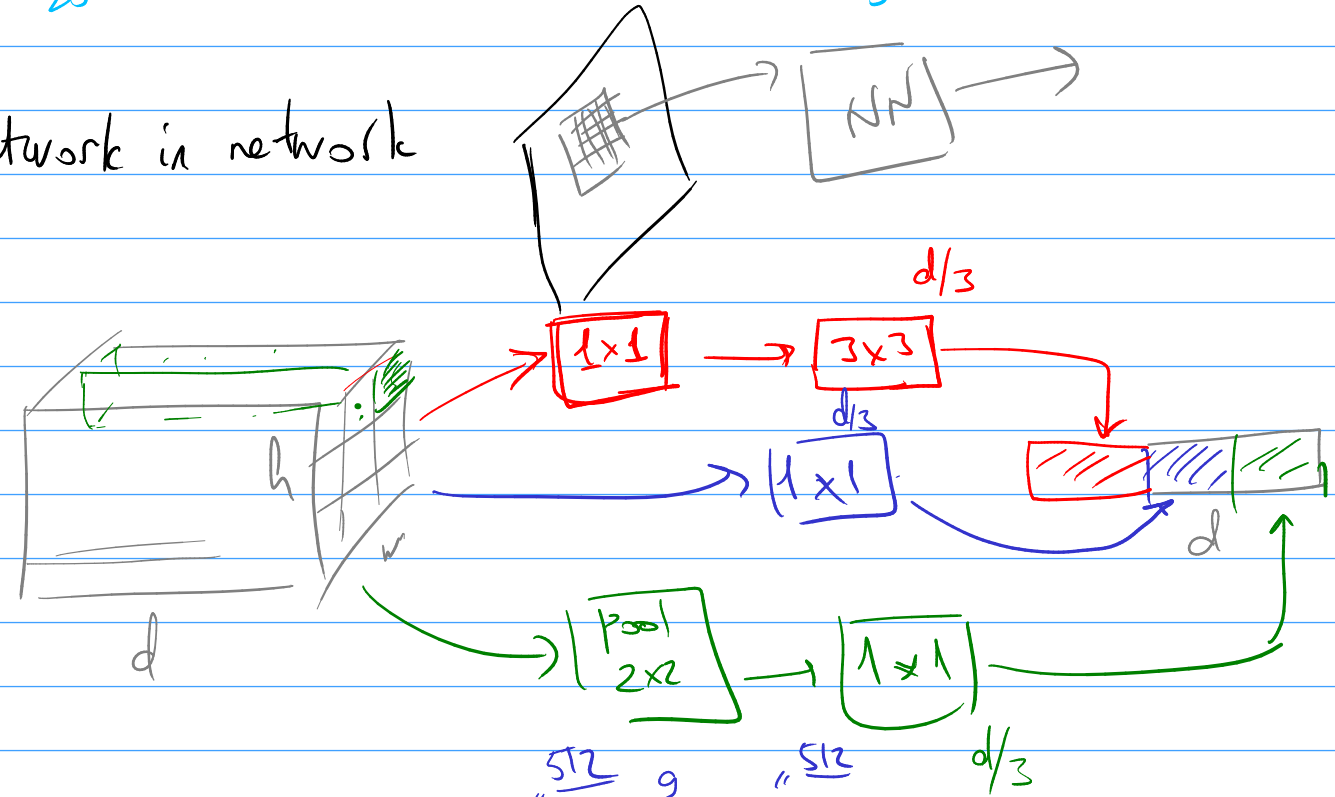


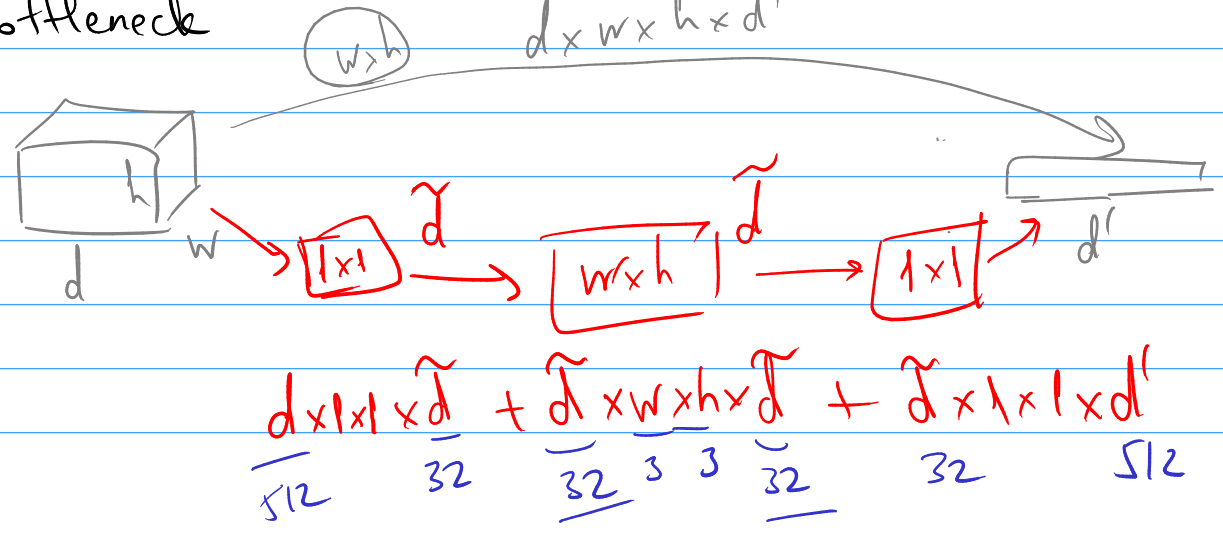
① VGG - Visual Geometry Group



② Network in network



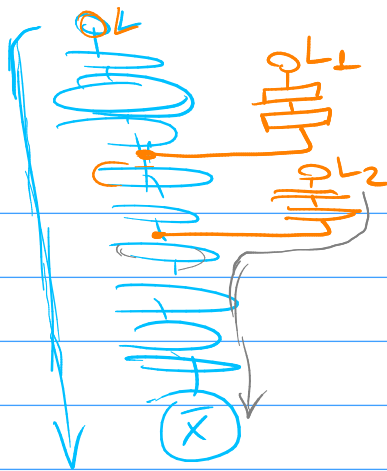
③ Bottleneck



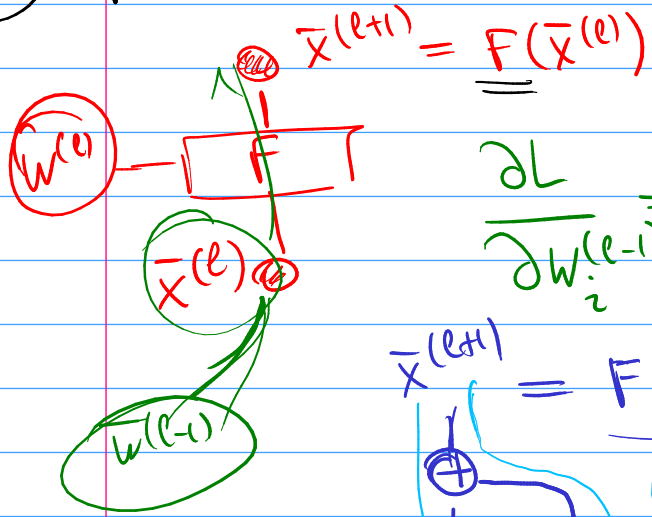
4 Auxiliary Classifiers

$$L = L_1 + \lambda_1 L_2 + \lambda_2 L_3$$

\downarrow \downarrow
 0 0



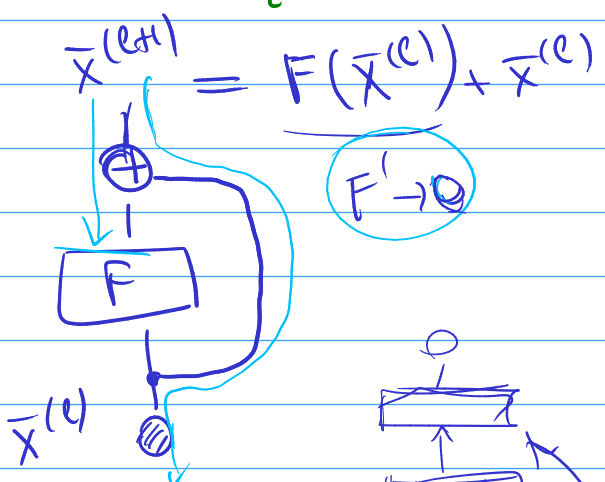
5 Residual connections - Kaiming He



$$\frac{\partial L}{\partial w_i^{(l-1)}} = \sum_j \frac{\partial x_j^{(l)}}{\partial w_i^{(l-1)}} \cdot \frac{\partial L}{\partial x_j^{(l)}}$$

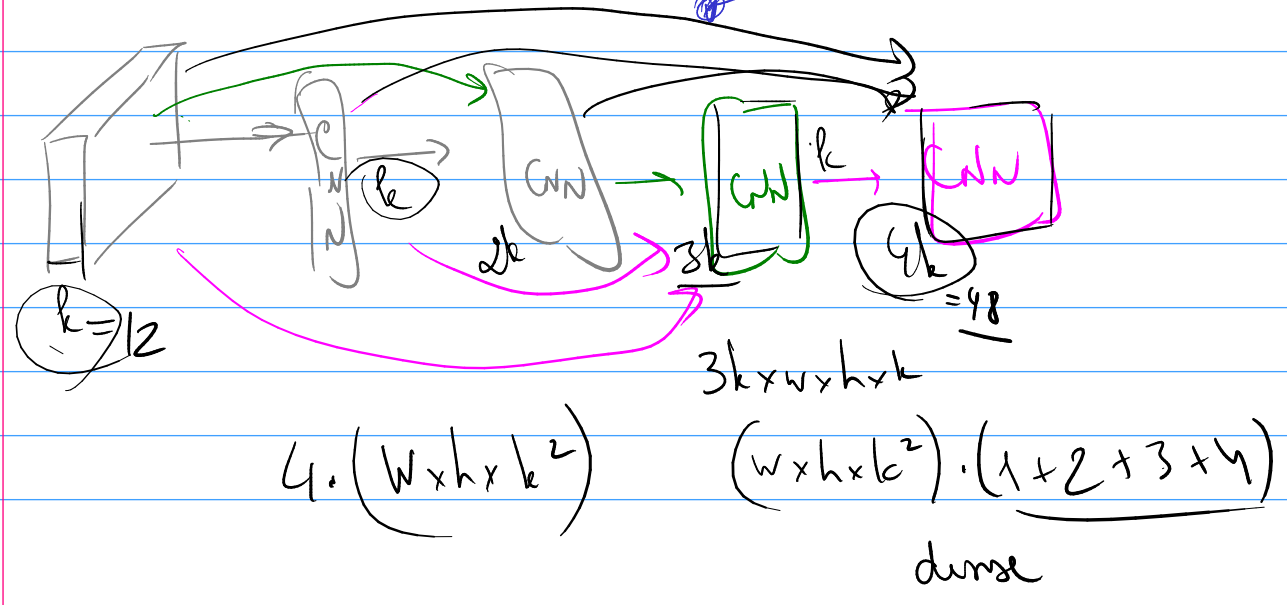
$$= \sum_j \frac{\partial L}{\partial x_j^{(l+1)}} \frac{\partial x_j^{(l+1)}}{\partial x_j^{(l)}}$$

$\frac{\partial L}{\partial x_j^{(l+1)}} \frac{\partial x_j^{(l+1)}}{\partial x_j^{(l)}} = 1$

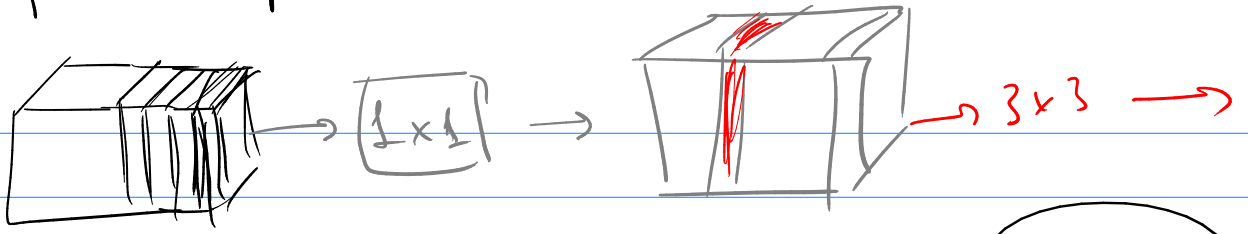


$$\frac{\partial x^{(l+1)}}{\partial x^l} \rightarrow 1$$

6 DenseNet

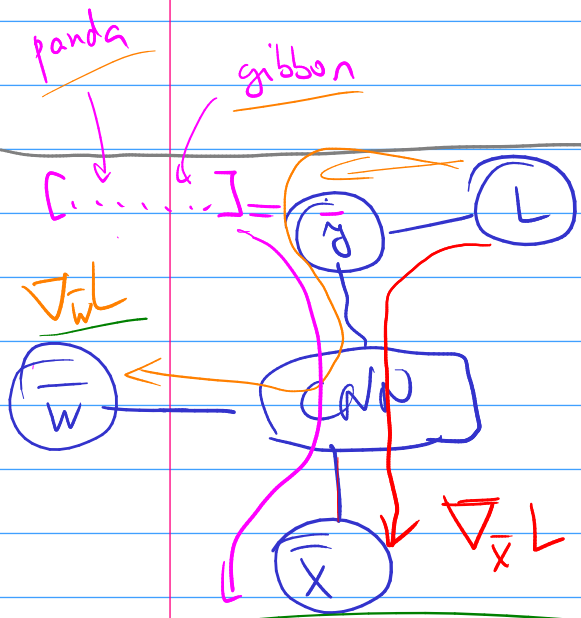


⑦ Depthwise separable convolutions

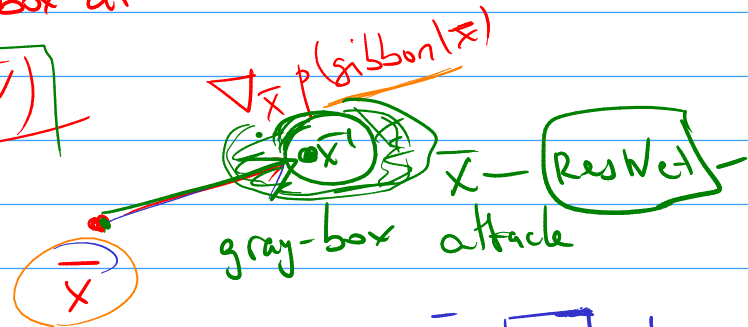


tSNE

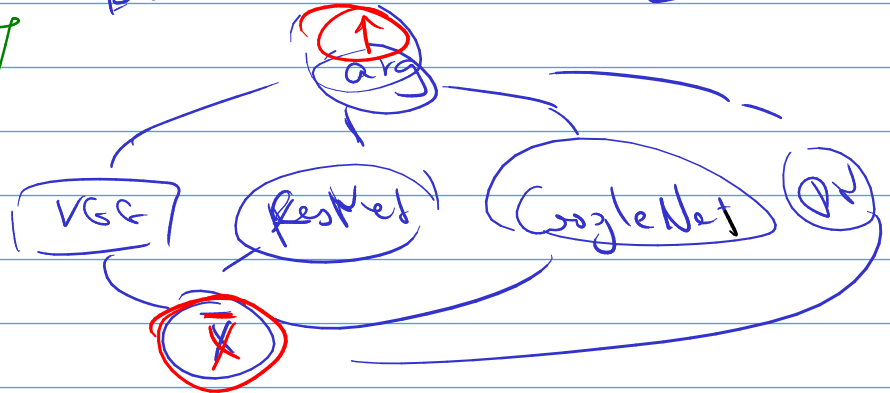
PCA \rightarrow ICA



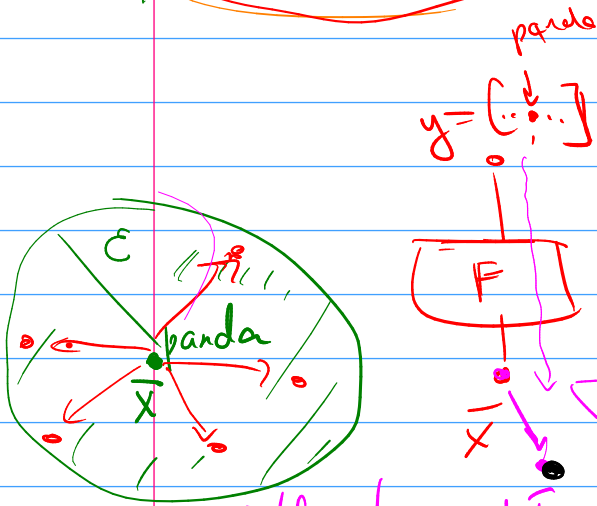
white-box attack
 $F(x, \bar{w})$



black-box attack \bar{x}

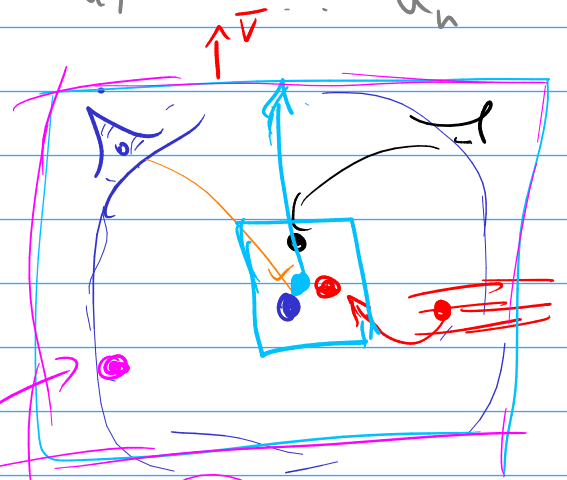
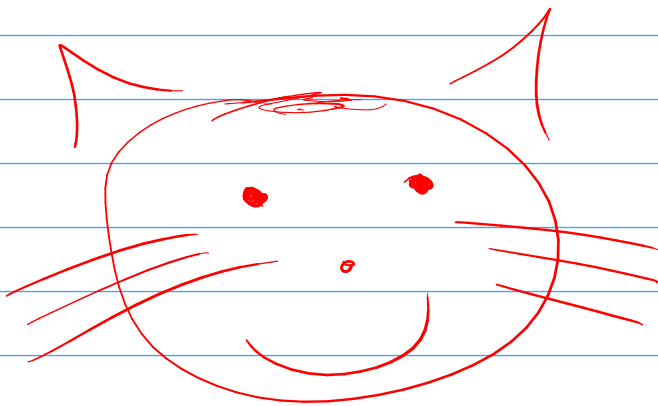
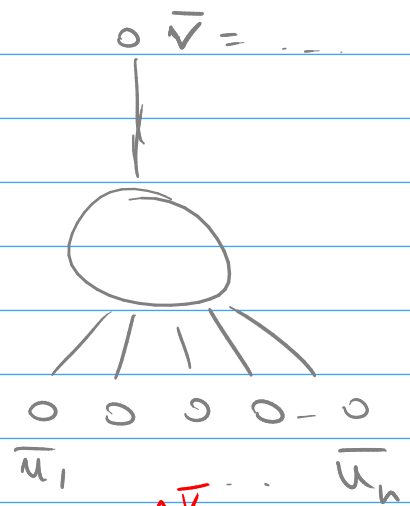
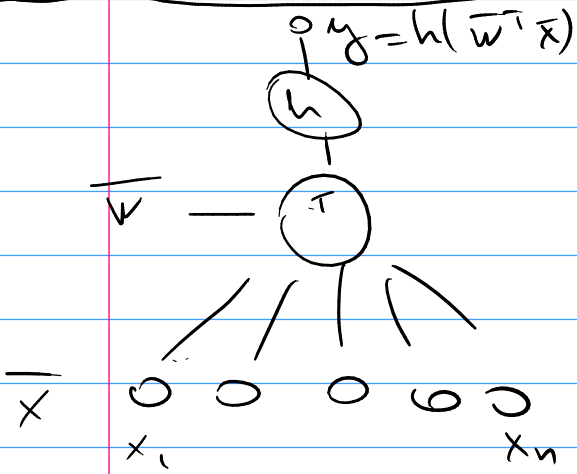
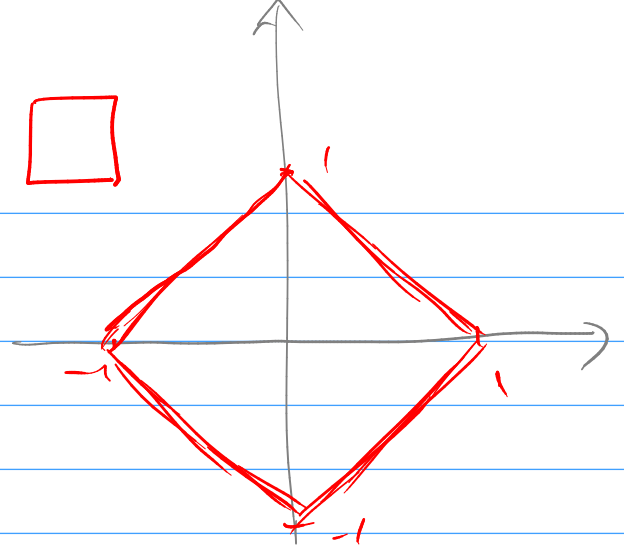
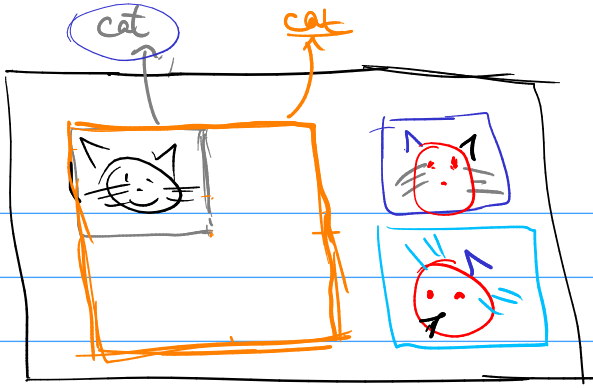


$\nabla_x [p(\text{gibbon}(\bar{x}))]$



Self-adversarial training
 $\bar{x} - \epsilon \nabla_x p(\text{panda}(\bar{x}))$

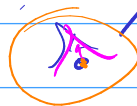
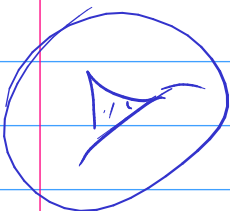
$$L(\bar{x}, y) = L(x, y) + \alpha L(x + \epsilon \nabla_x L(x, y), y)$$



$(0, 0, 0)$

$\bar{u}_1 = (c, x, y, d, \alpha, \dots)$

$\bar{u}_2 = (c, \dots)$



Autoencoders

