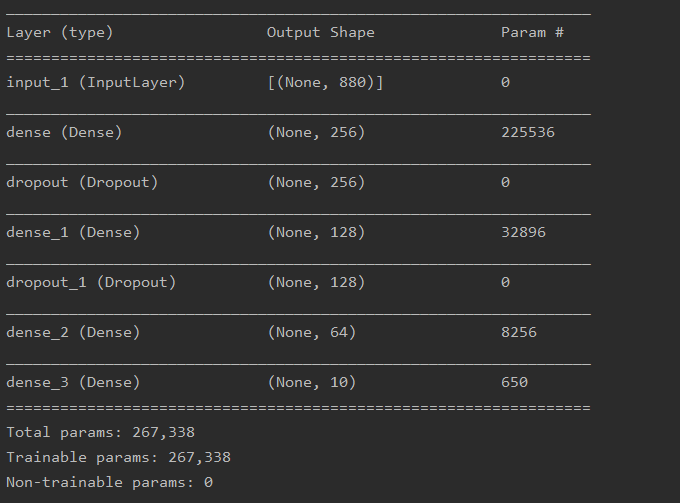
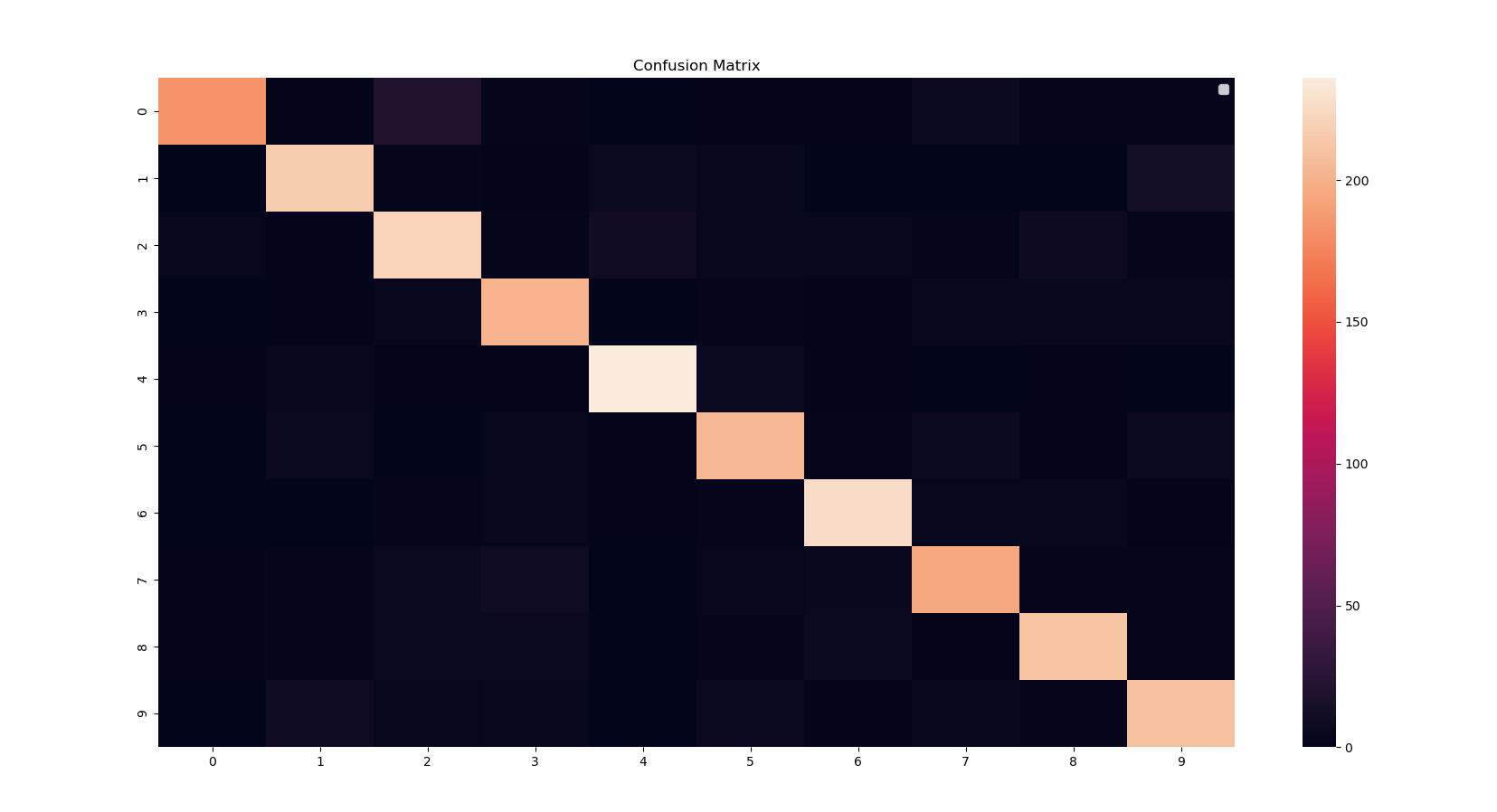


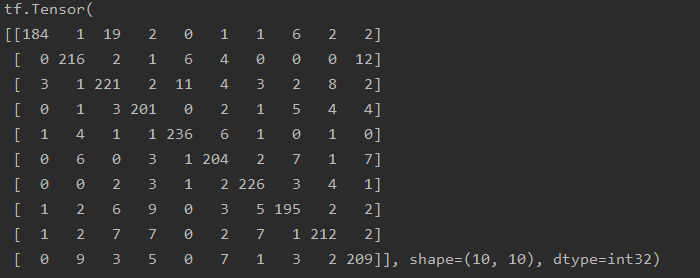
* The model: model\_droput0.5.h5

Batch = 64



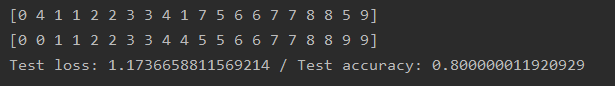
Confusion matrix







Testing with my own voice:



The first row is the prediction, the second one is the ground truth. For each digit there are two types of recording. The first one, corresponding to the first digit, I recorded only one digit at a time; the second digit comes from one recording where I uttered all digits from 0 to 9, then using a script split them.

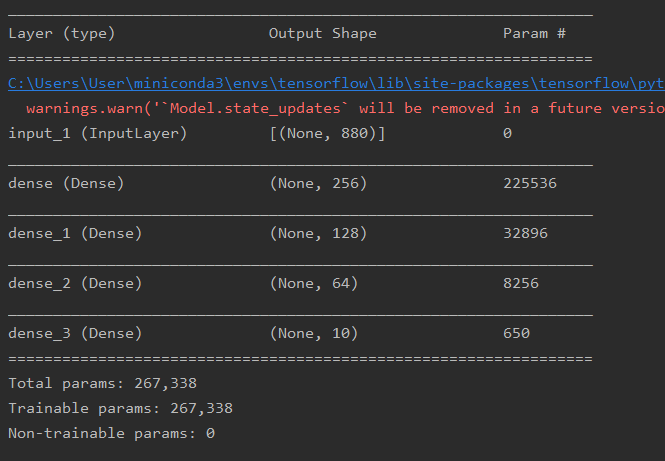
Upper-bound Lipschitz constant:



20.09.2021

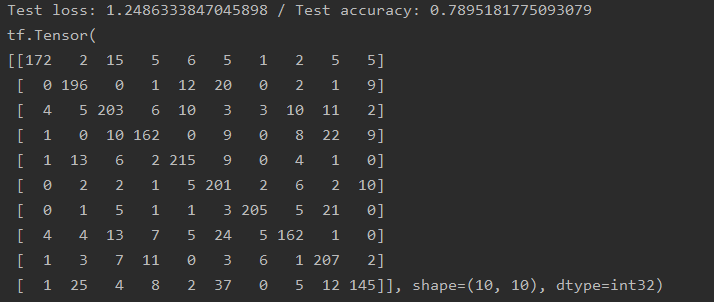
* **Training a constrained model: model\_NoDropout.h5**

**Batch = 64**

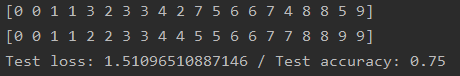
****







For recordings of my voice:

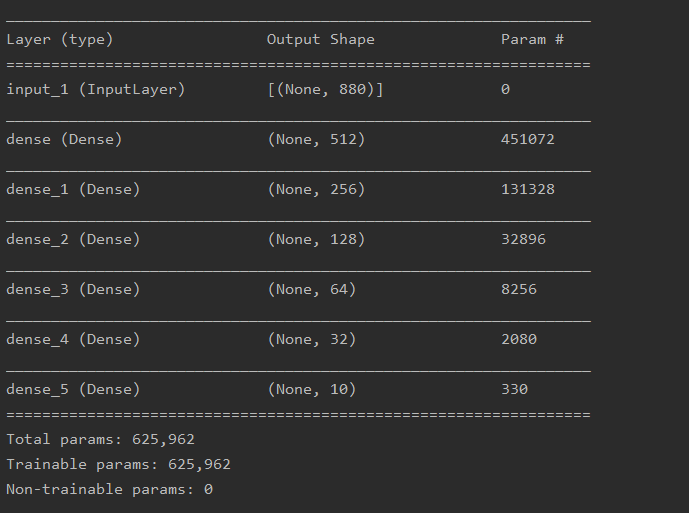


Lipchitz constant:



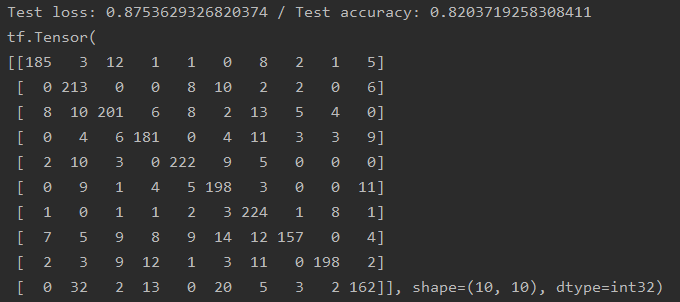
* **Training a constrained more complex model: model\_NoDropout\_moreLayers.h5**

**Batch = 256**

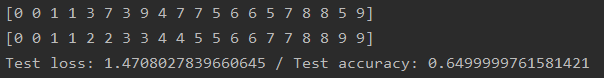








For recordings of my voice:



Lipchitz constant:



* **Training a constrained more complex model: model\_Dropout02\_moreLayers.h5**

**Batch = 64**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Layer (type) Output Shape Param #

=================================================================

input\_1 (InputLayer) [(None, 880)] 0

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

dense (Dense) (None, 512) 451072

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

dropout (Dropout) (None, 512) 0

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

dense\_1 (Dense) (None, 256) 131328

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

dense\_2 (Dense) (None, 128) 32896

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

dense\_3 (Dense) (None, 64) 8256

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

dense\_4 (Dense) (None, 32) 2080

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

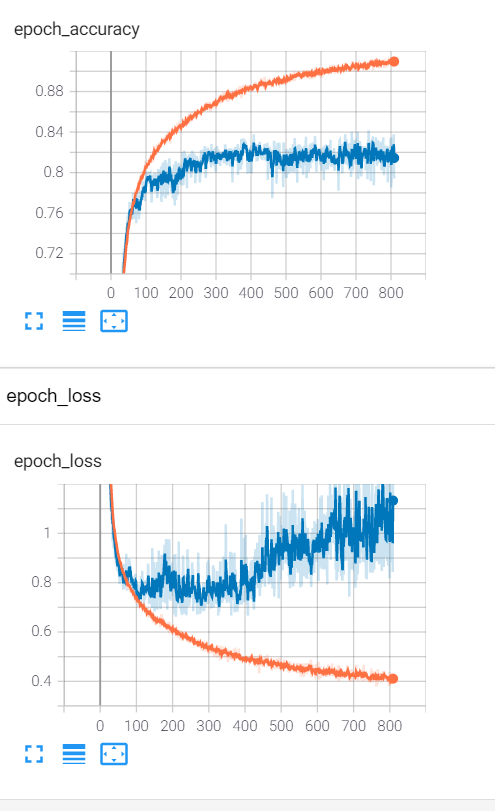
dense\_5 (Dense) (None, 10) 330

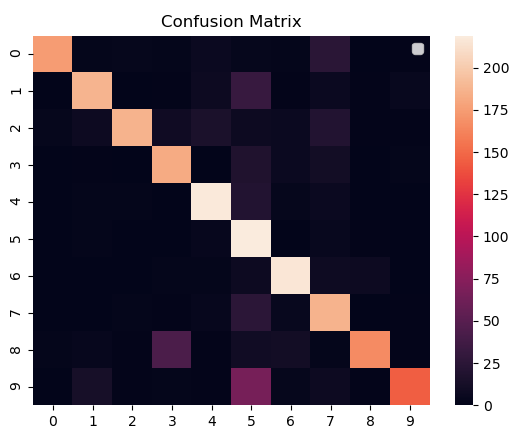
=================================================================

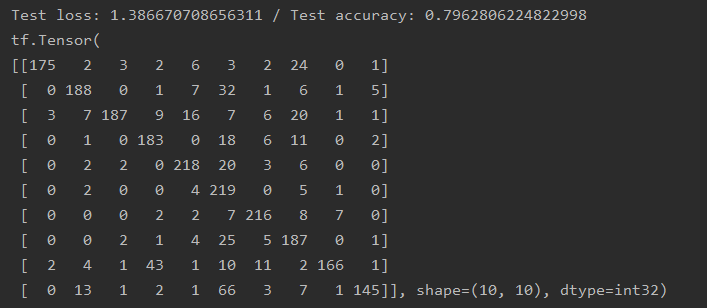
Total params: 625,962

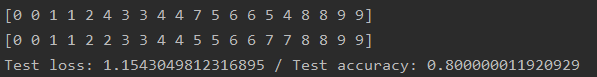
Trainable params: 625,962

Non-trainable params: 0





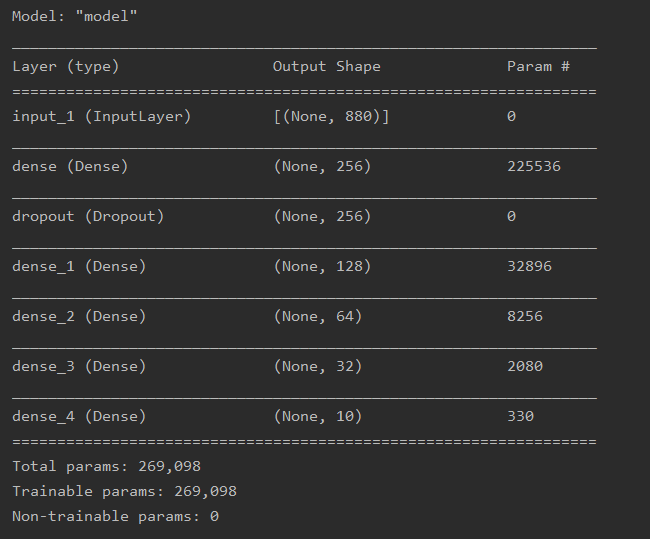


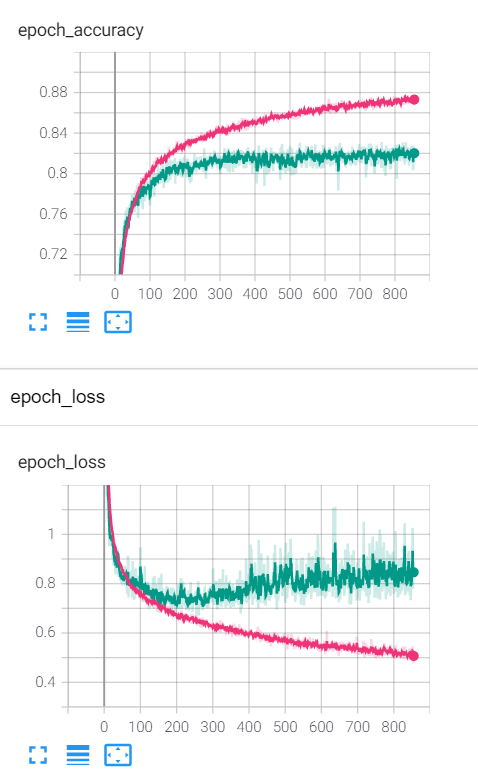


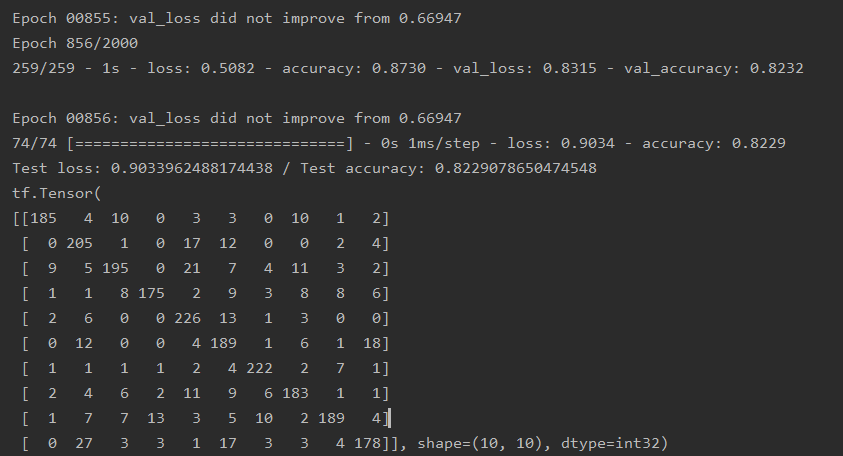


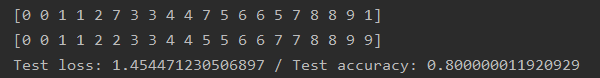
* **Training a constrained more complex model: model\_Dropout02\_moreLayersV2.h5**

**Batch = 64**

****

****

****

****

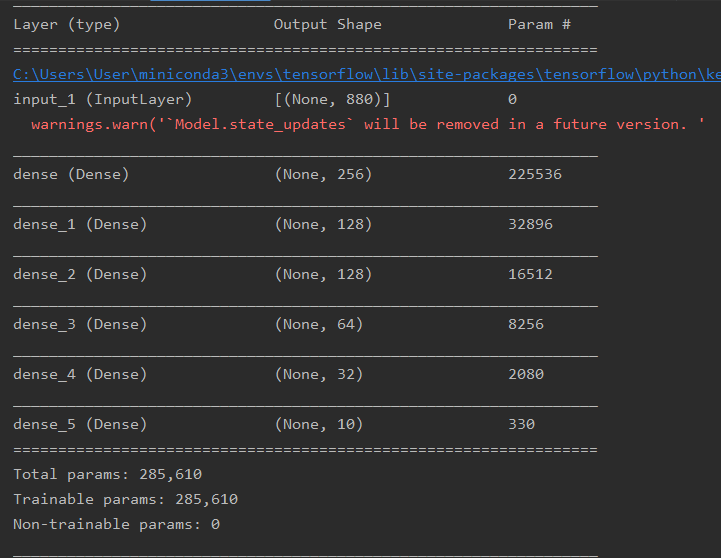
****

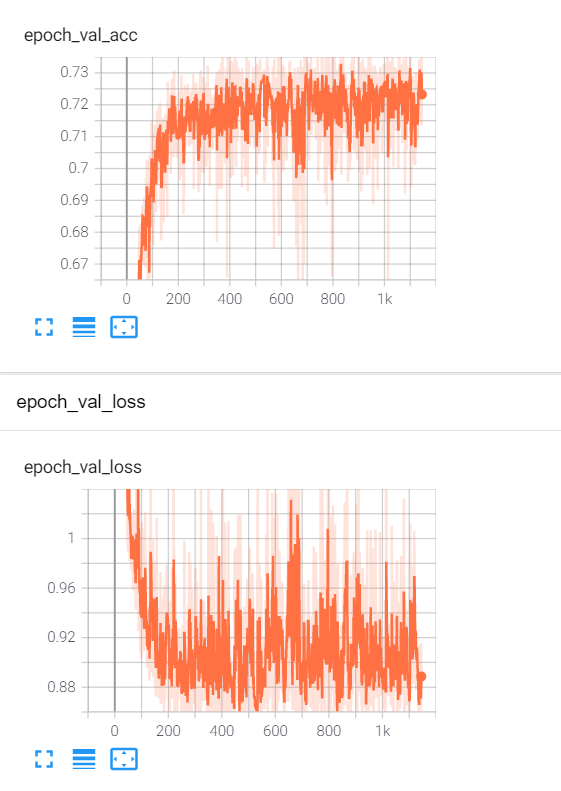
**Training Lipchitz constrained nets**

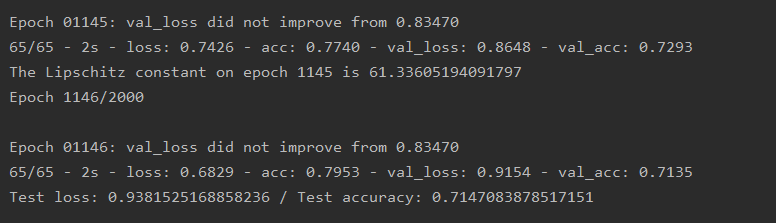
**I only used the callback class because the constraint one was throwing some errors due to the custom constraint.**

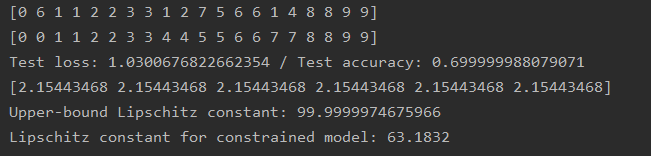
* model\_5layer\_rho100.h5

**batch = 256**

****

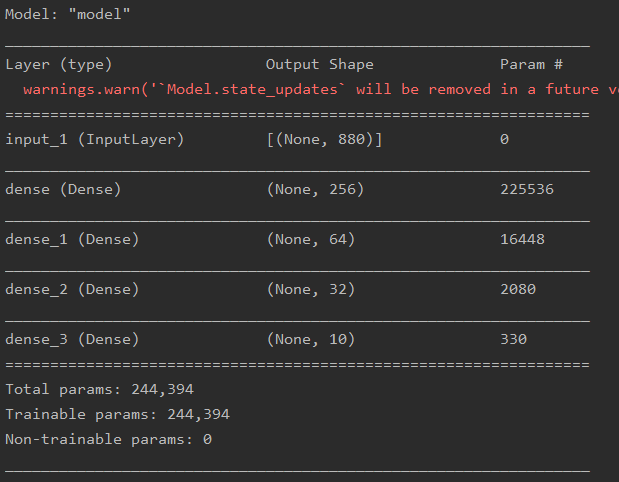
****

****

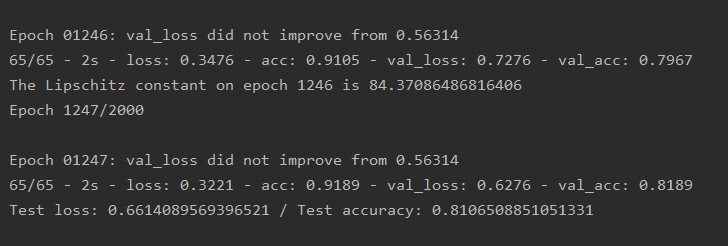
****

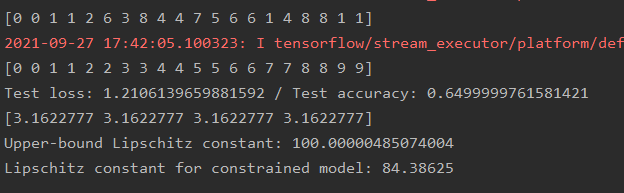
* model\_3layer\_rho100

batch = 256



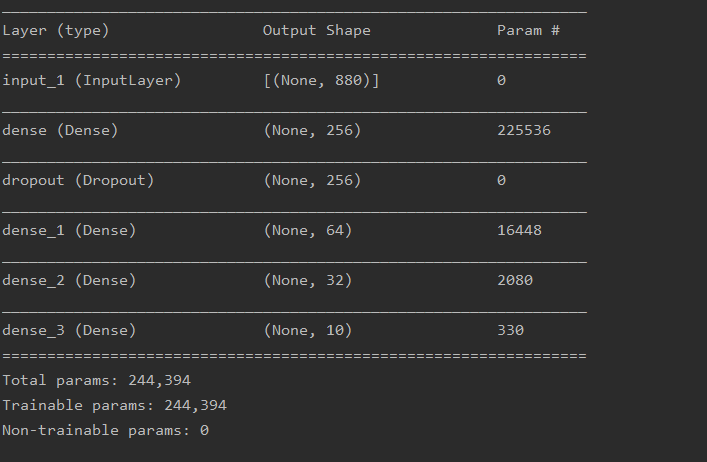


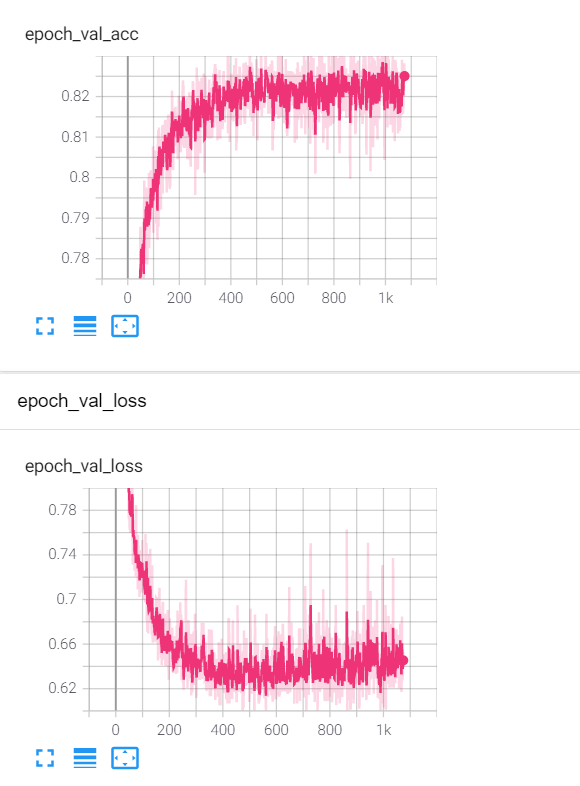


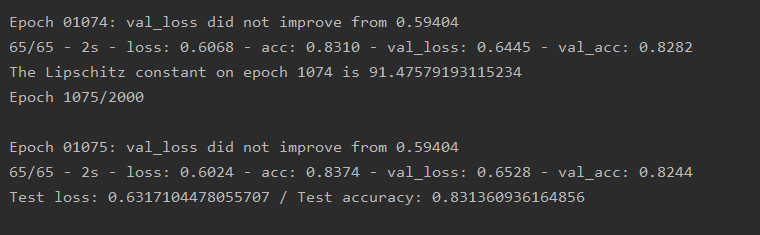


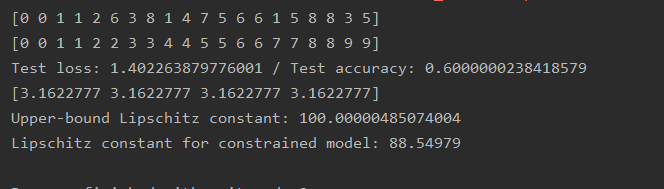
* **model\_3layer\_rho100**

**Batch = 256**

****

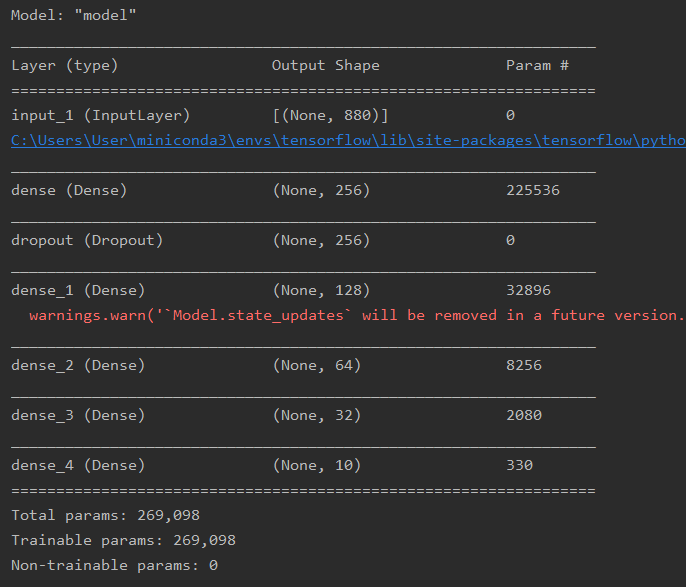
****

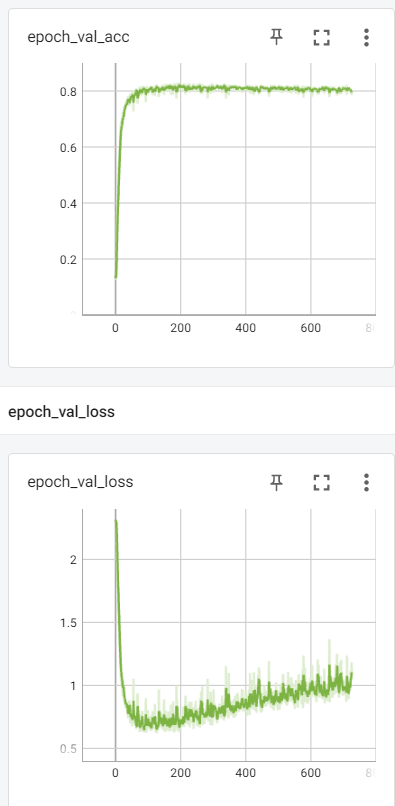
****

****

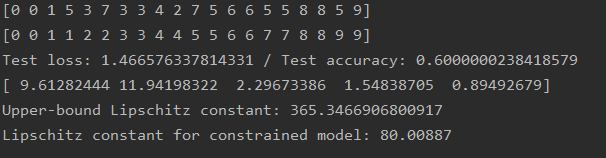
**Training Lipchitz constrained nets using FISTA algorithm**

* **model\_5layerFISTA\_rho80\_droupout.h5**

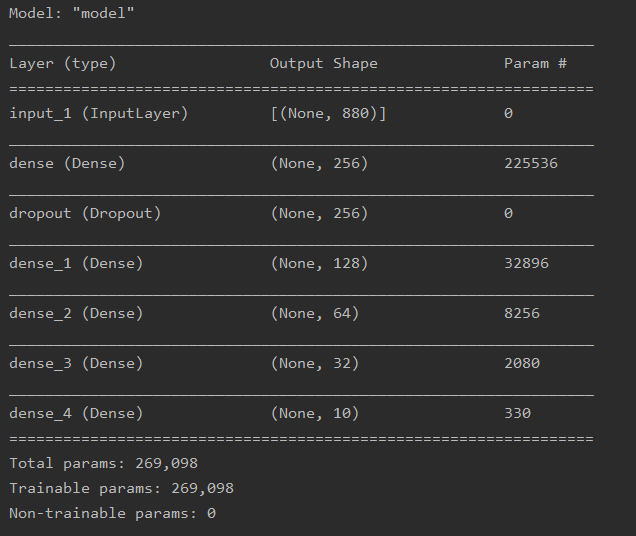
****

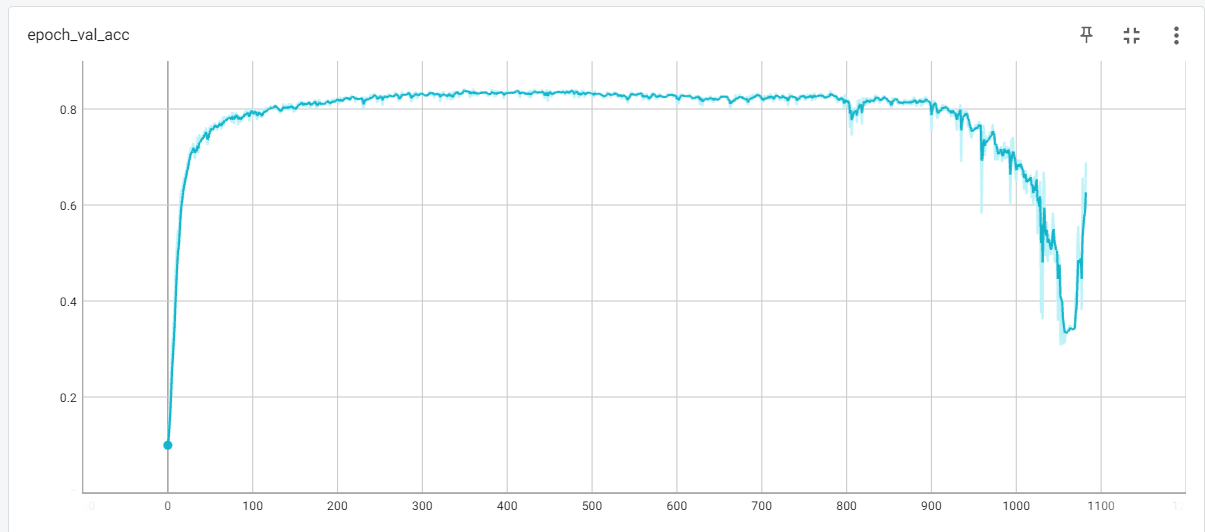
****

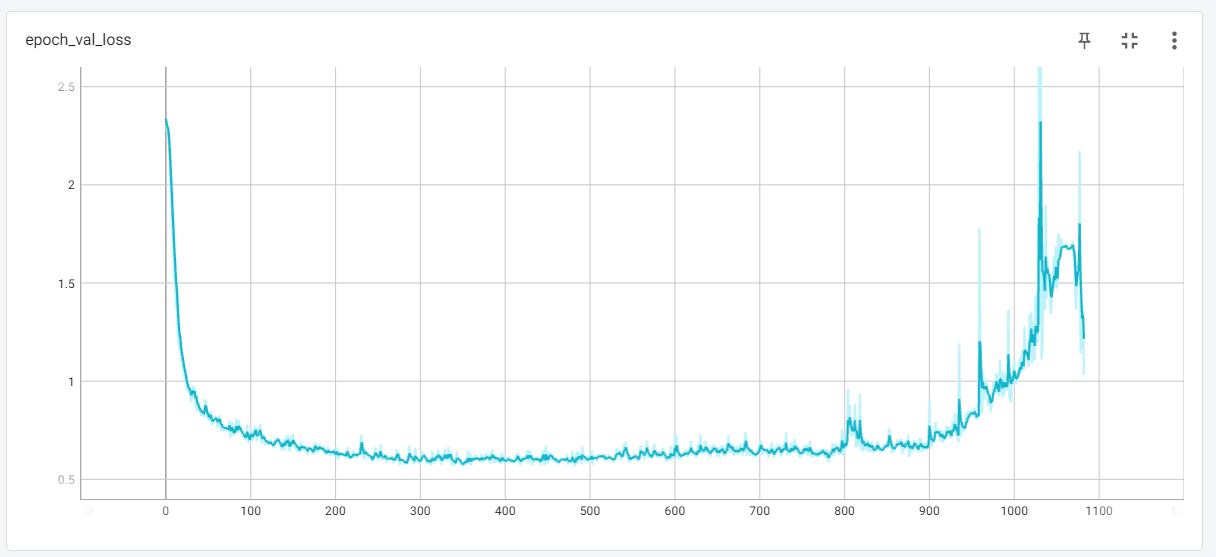
****

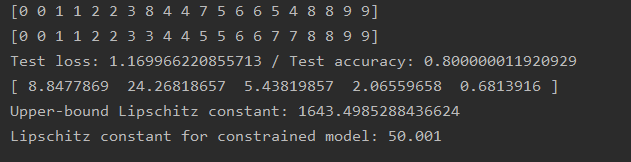
****

* model\_5layerFISTA\_rho50\_droupout.h5

****

****

****

****

****

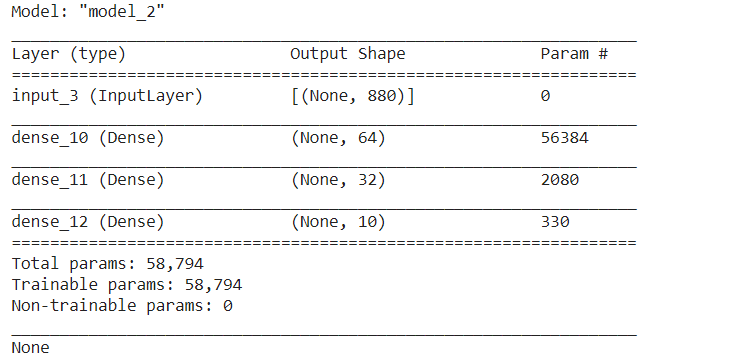
* Sa mai scad rho, ideal sub 10, 5.
* Atacuri: black box (zgomot), white noise (AR toolbox). Grafice black box: precizie vs sigma pt constrans si neconstrans. Grafice with box: precizie vs. confidence.

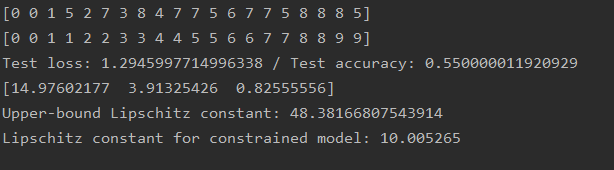
<https://adversarial-robustness-toolbox.readthedocs.io/en/latest/modules/attacks/evasion.html?highlight=fgsm#projected-gradient-descent-pgd>

* Google colab.

Rho = 10

* model\_3layerFISTA\_rho10.h5 A simple model

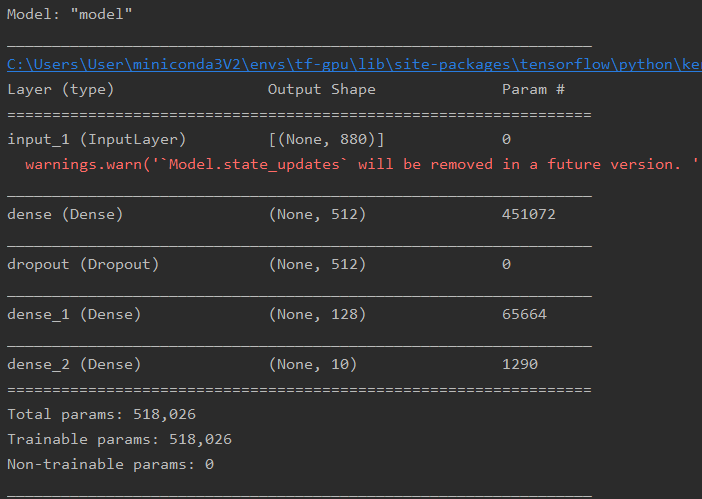








* model\_3layerFISTA\_rho10

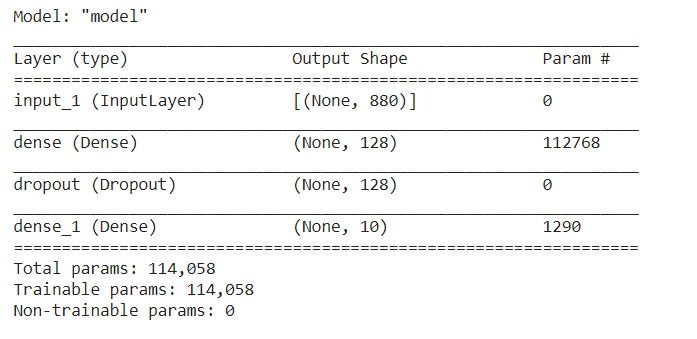


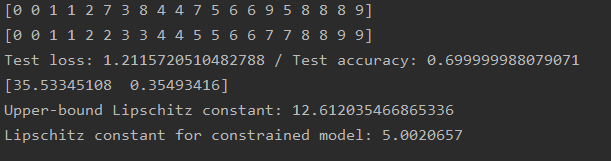




Rho = 5

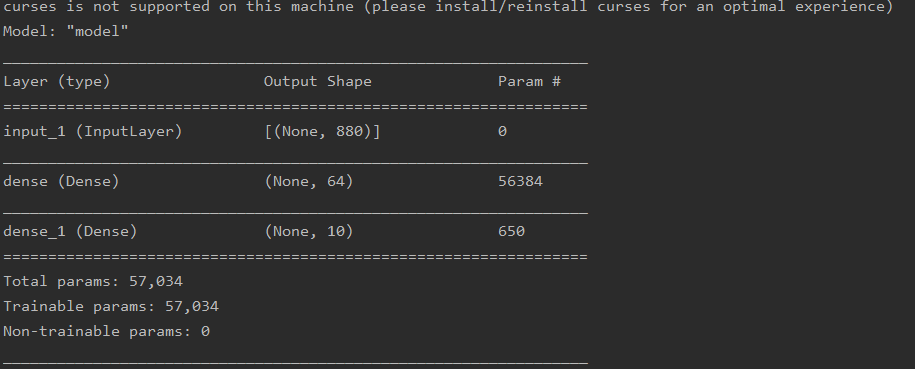
* model1layerFISTA\_rho5\_droupout.h5

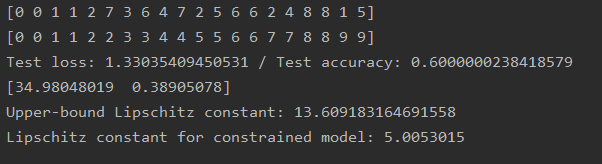






* model\_1layerFISTA\_rho5







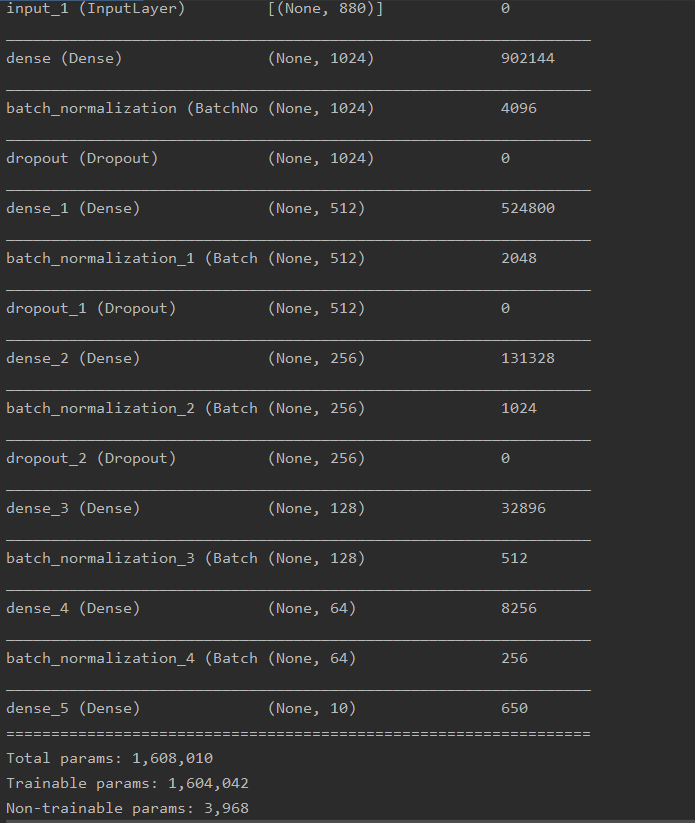


Callback constraint nu merge rulat pe CUDA

Constraint merge rulat pe CUDA. De aceea e diferenta mare de timp.

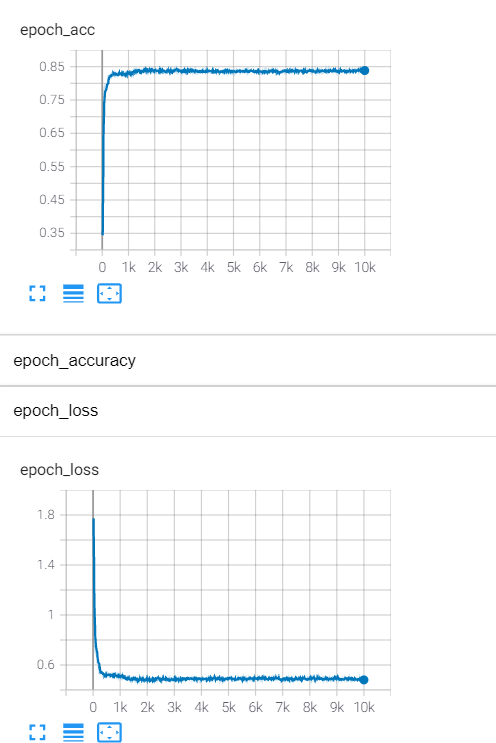
Nu imi dau seama cum as putea sa scriu un constraint care sa aiba acces la celelalte ponderi din retea.

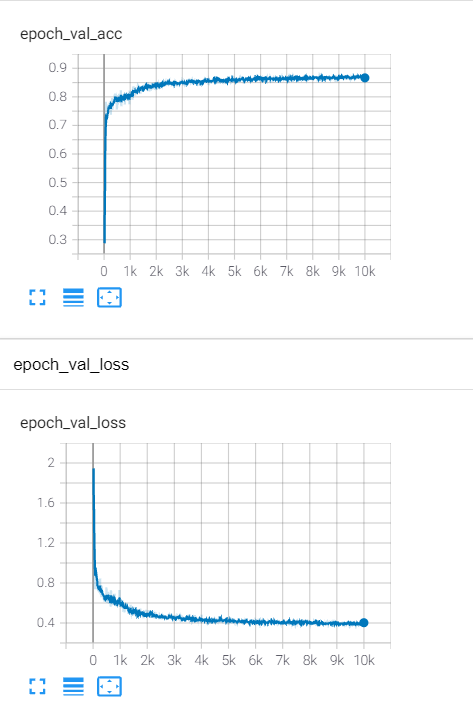
Here only the last layer was constrained.

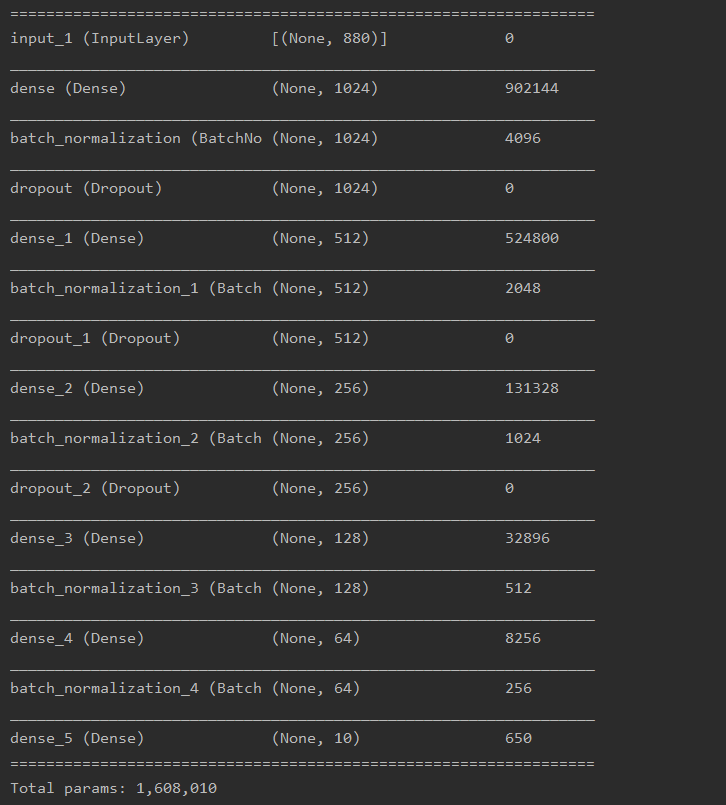




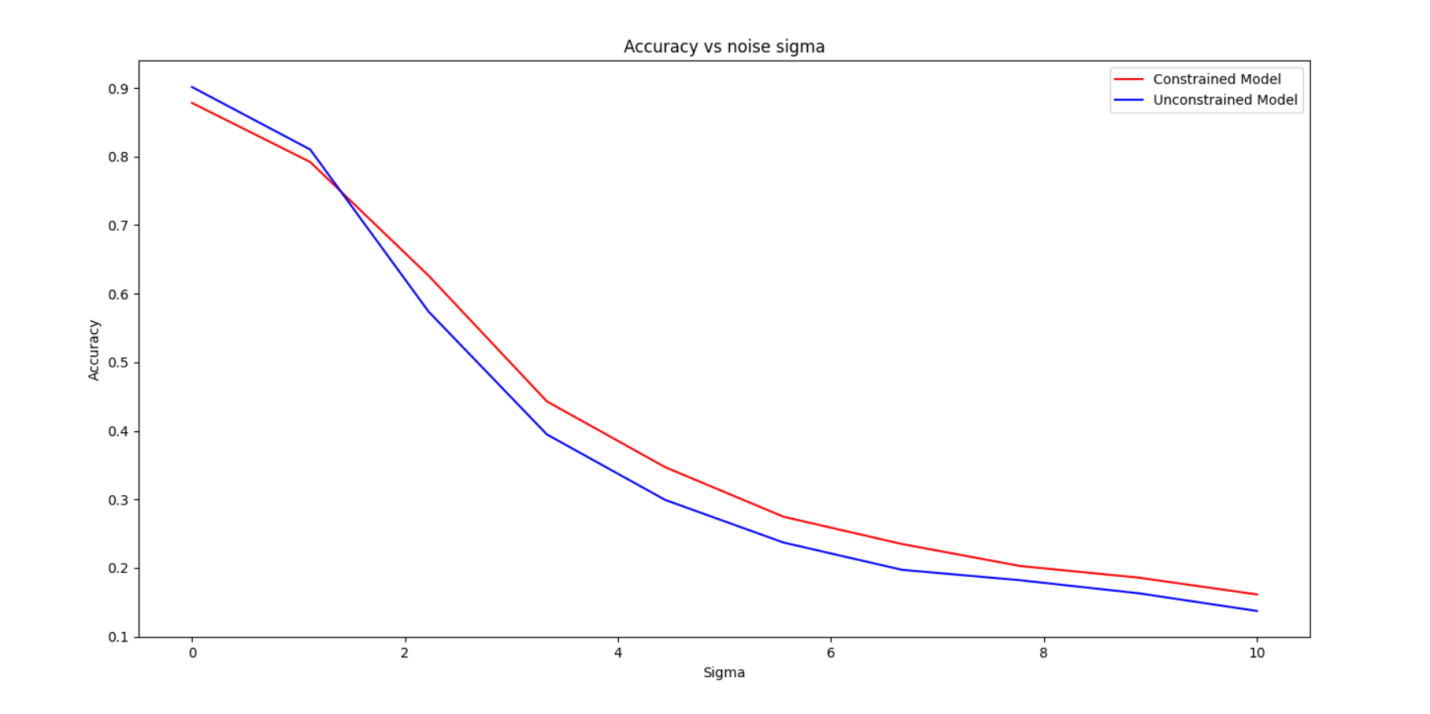
* **model\_test.h5 rho = 10**

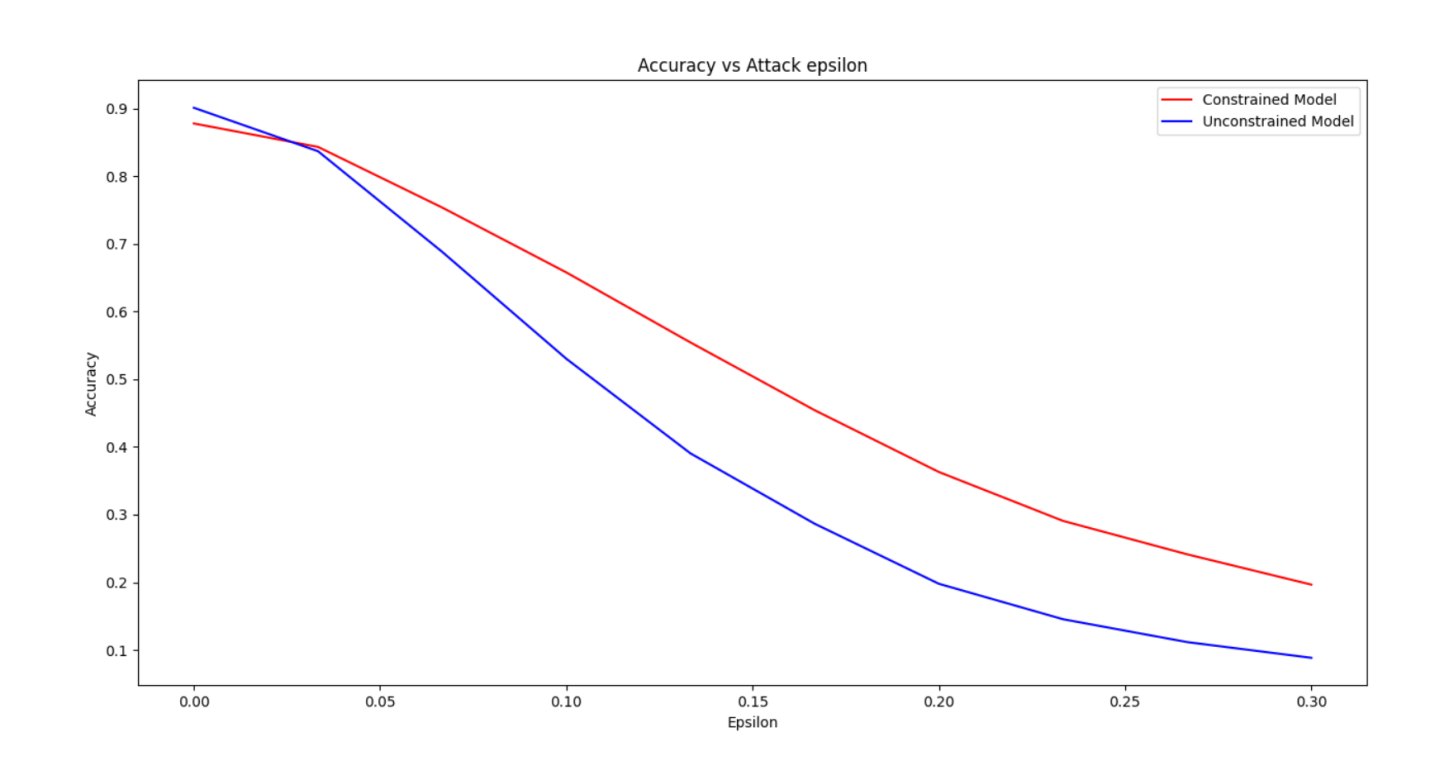
****

****

****

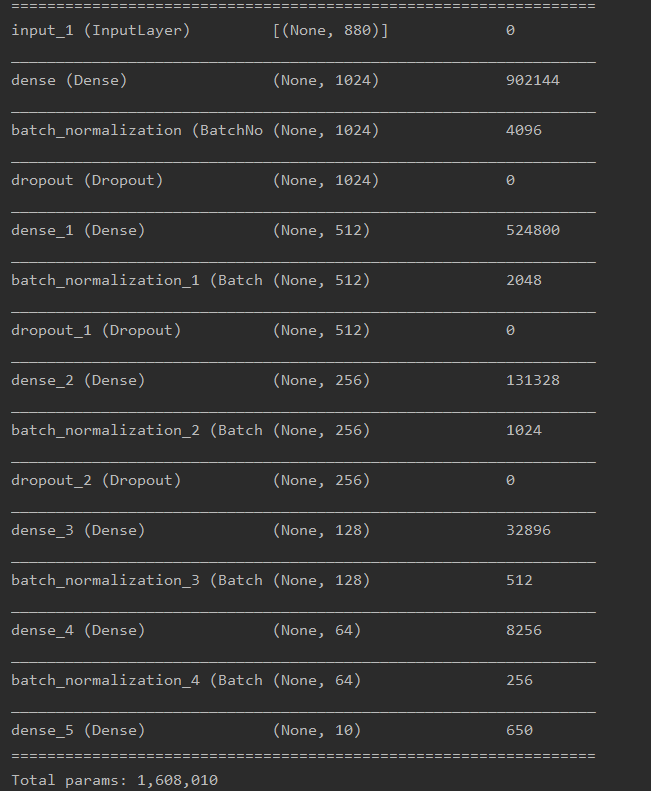
****

****

****

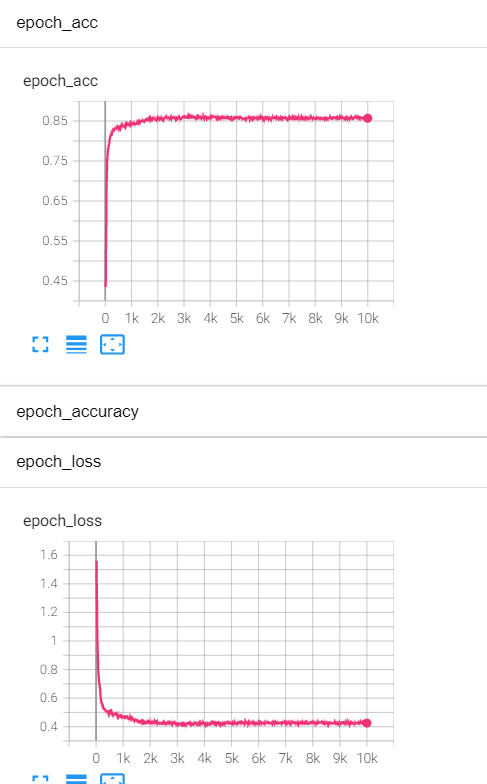
****

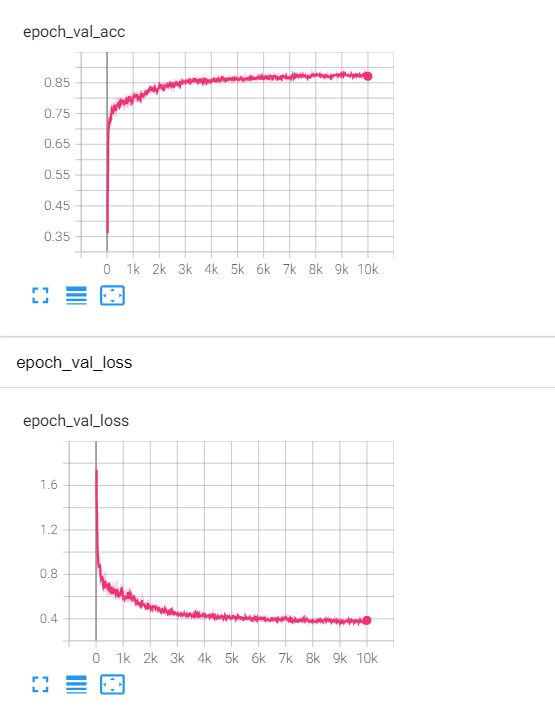
* **model\_constrained\_rho5\_dropout02**

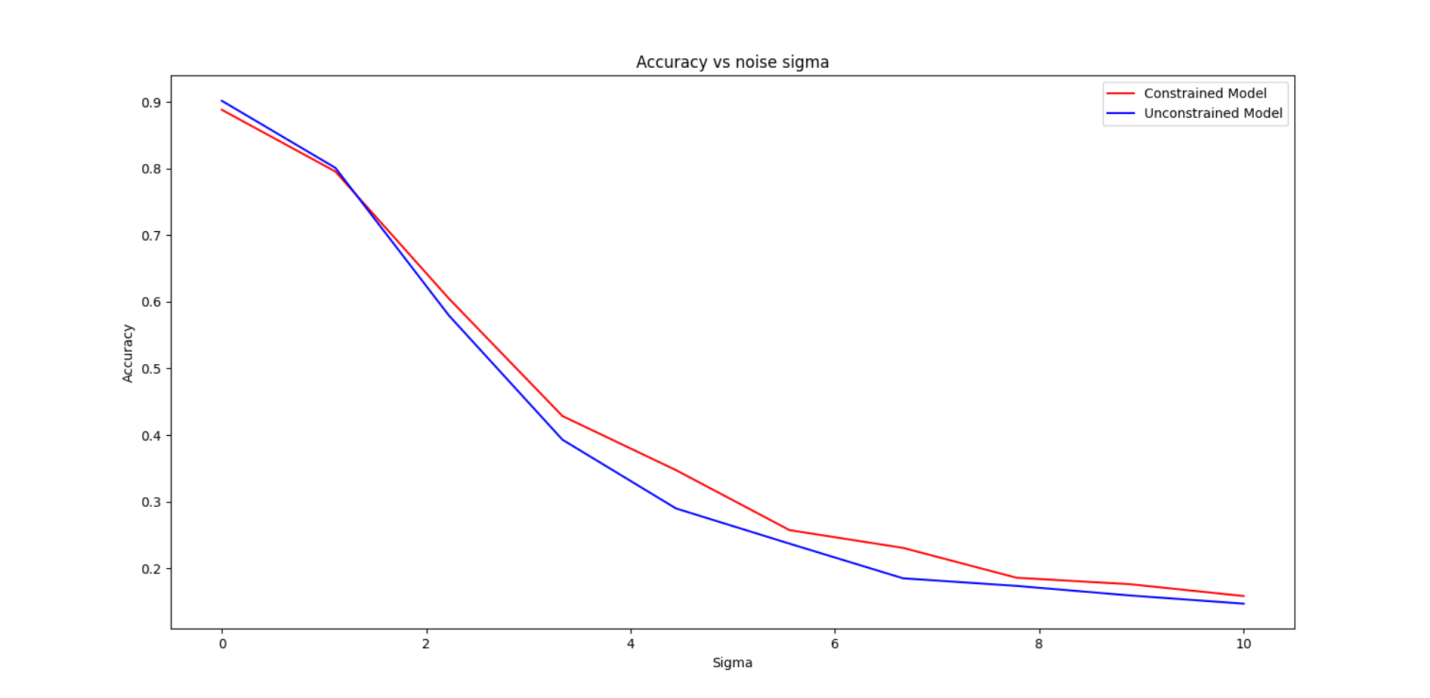
****

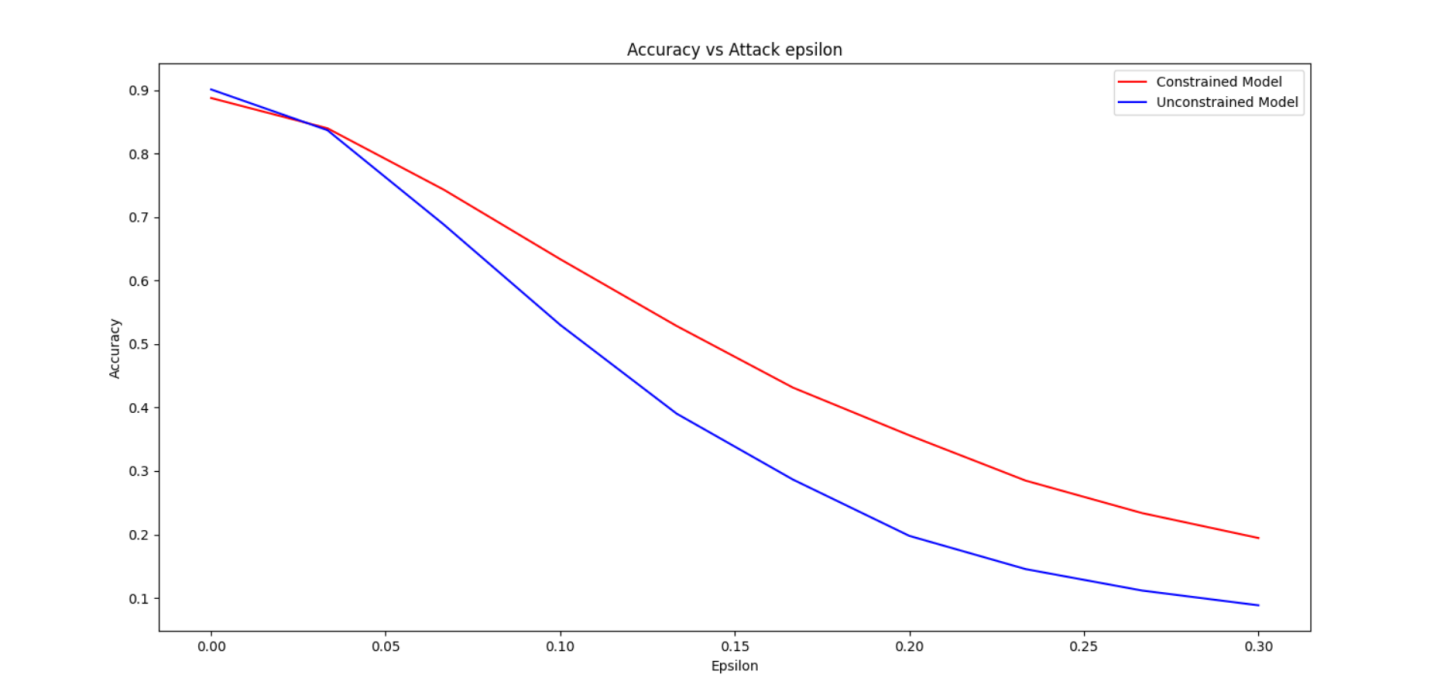




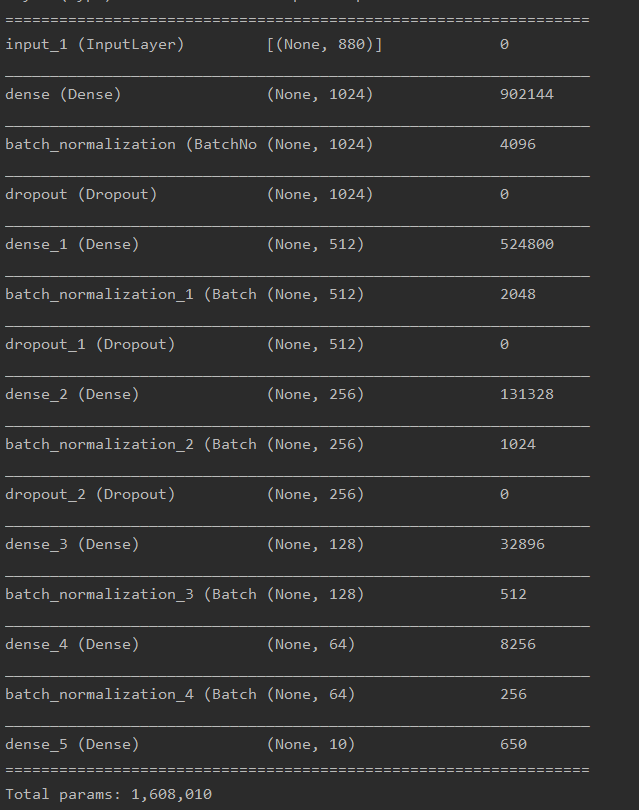




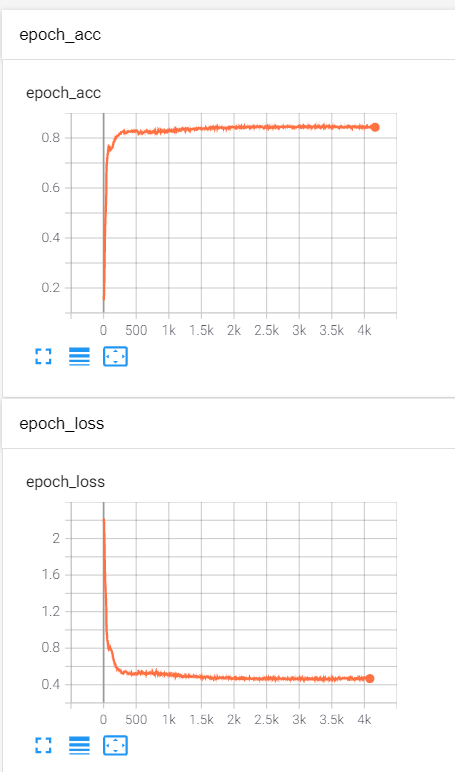


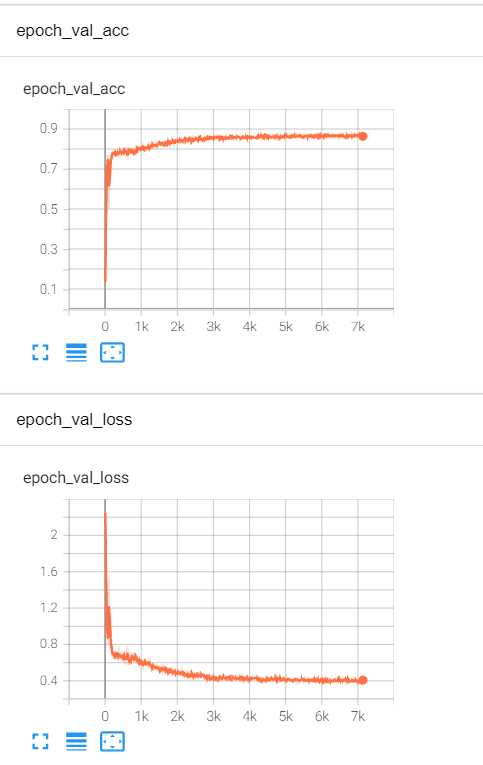


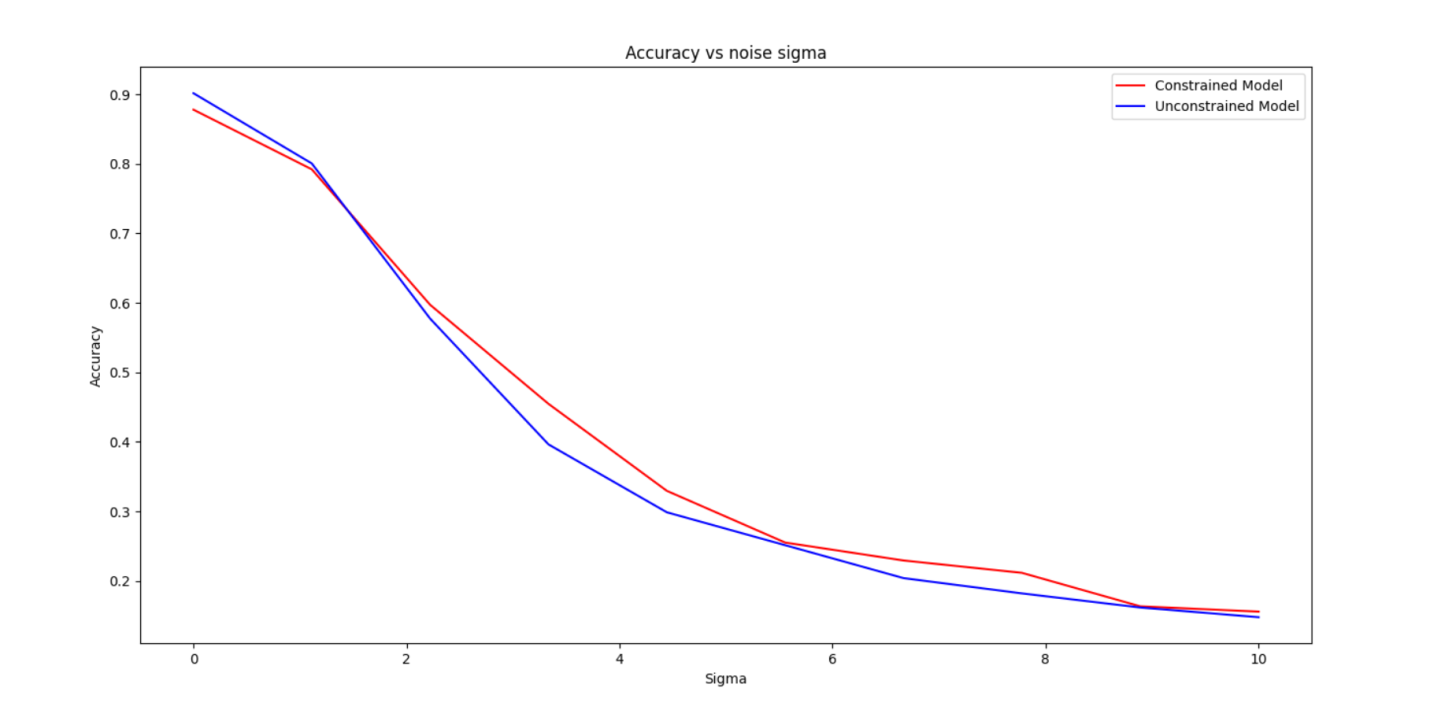
* **model\_constrained\_rho2\_dropout02**

****

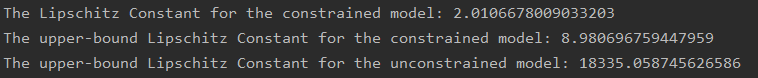
****

****

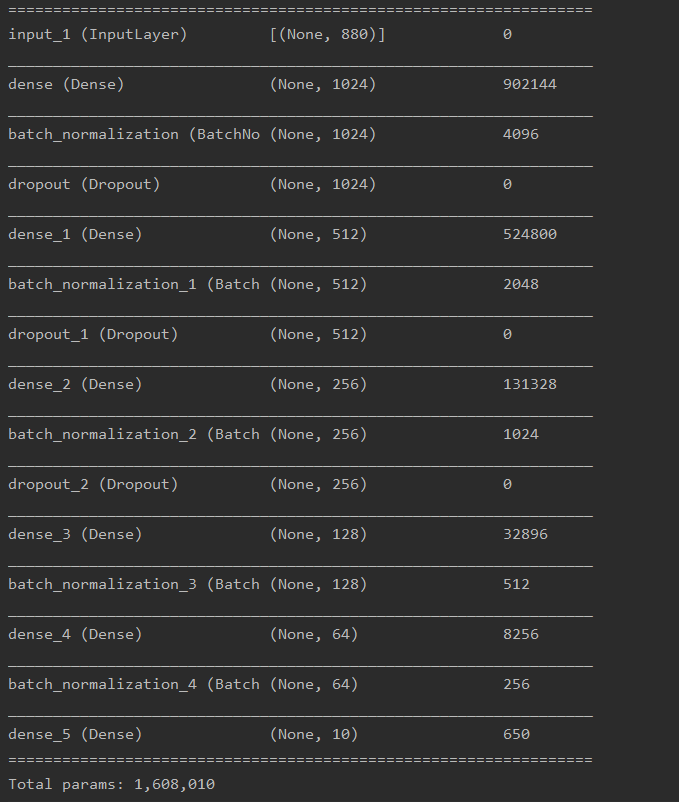
****

****

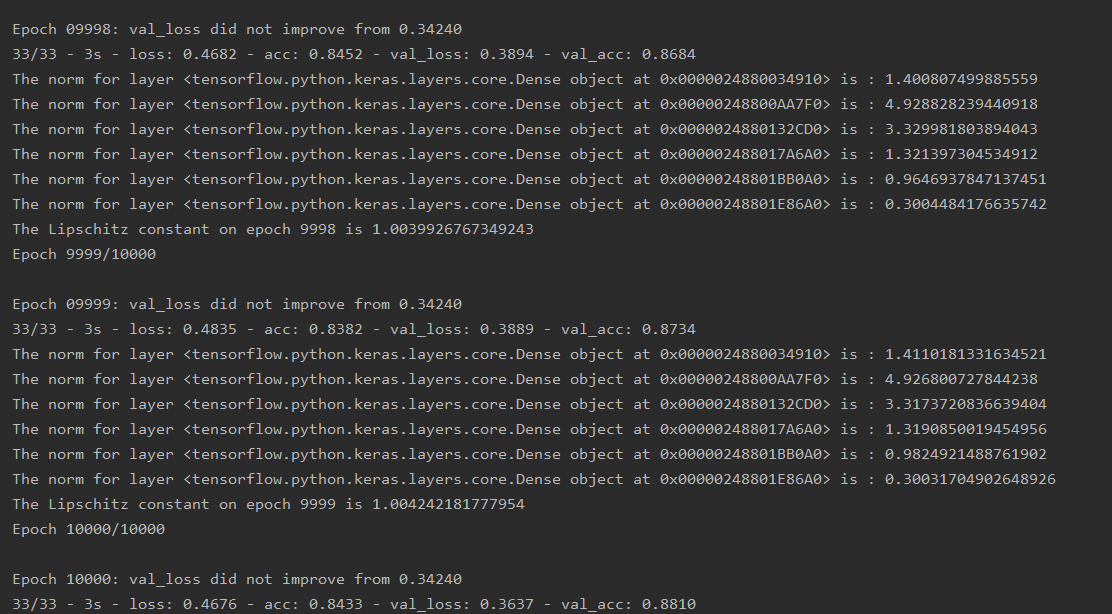
****

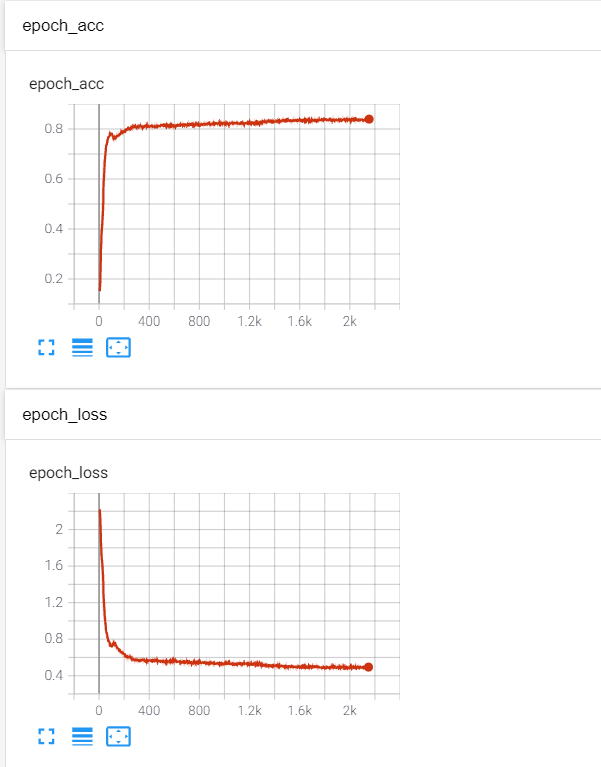
****

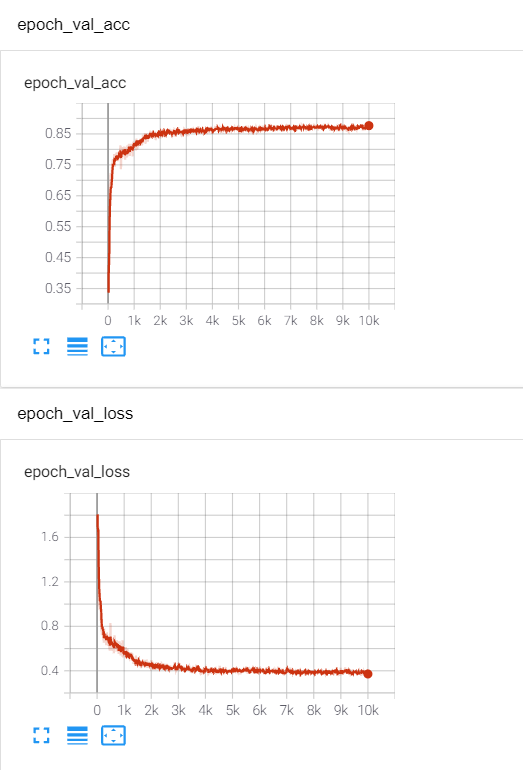
* **model\_constrained\_Rho1\_dropout02**

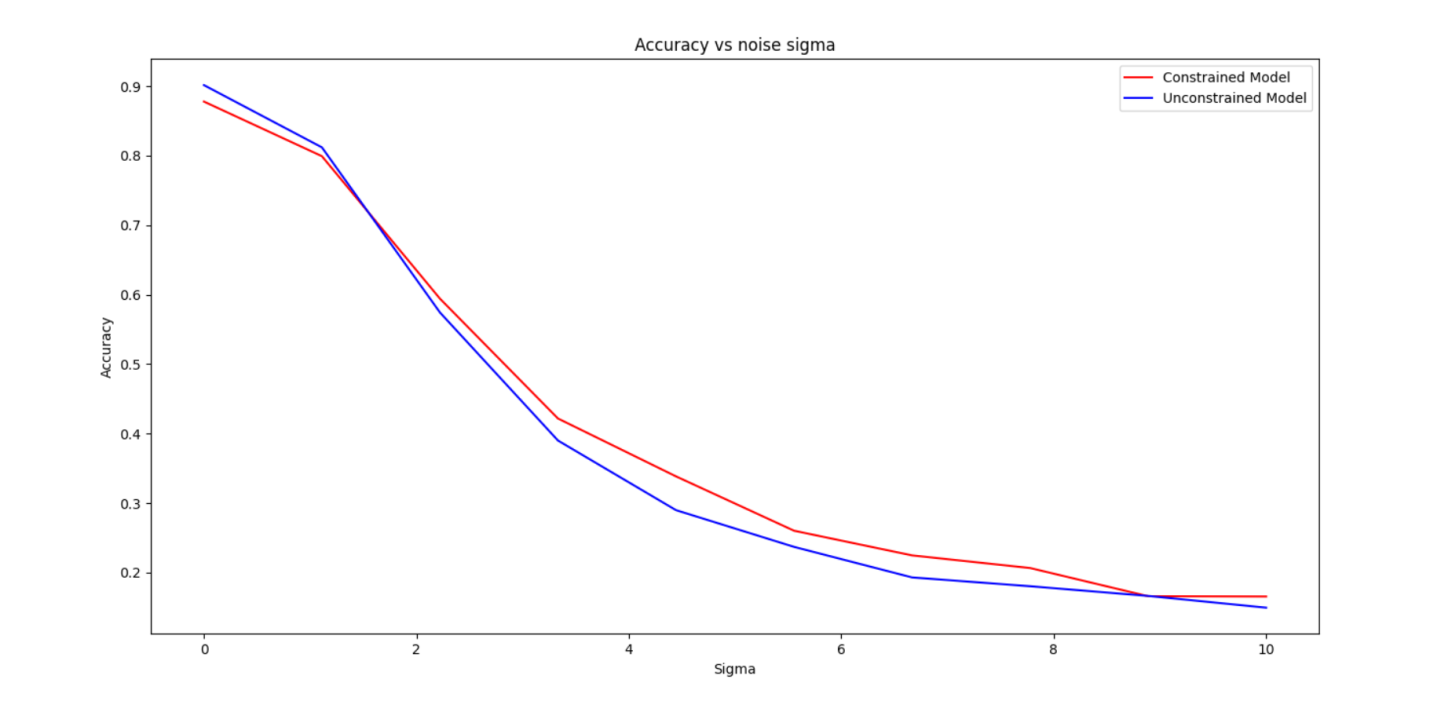
****

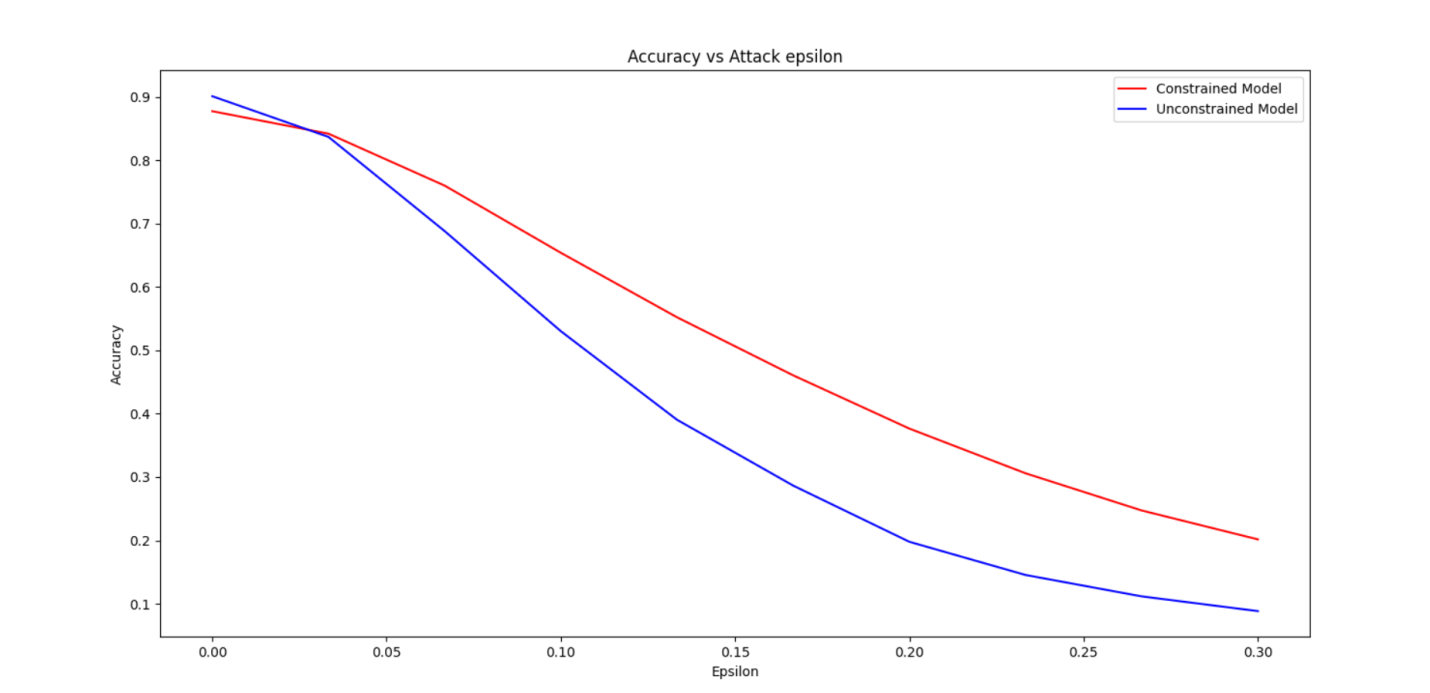
****

****

****

****

****

****

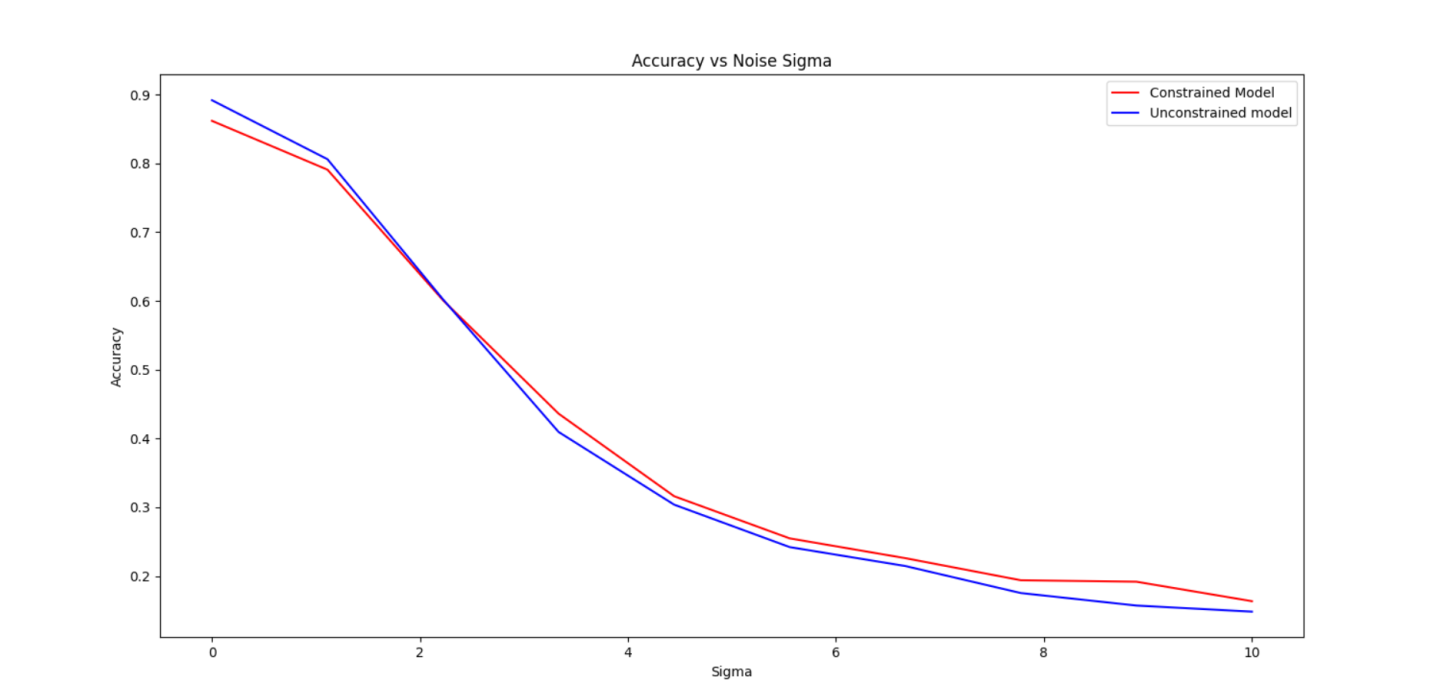
****

* **model\_constrained\_Rho01\_dropout02.h5**

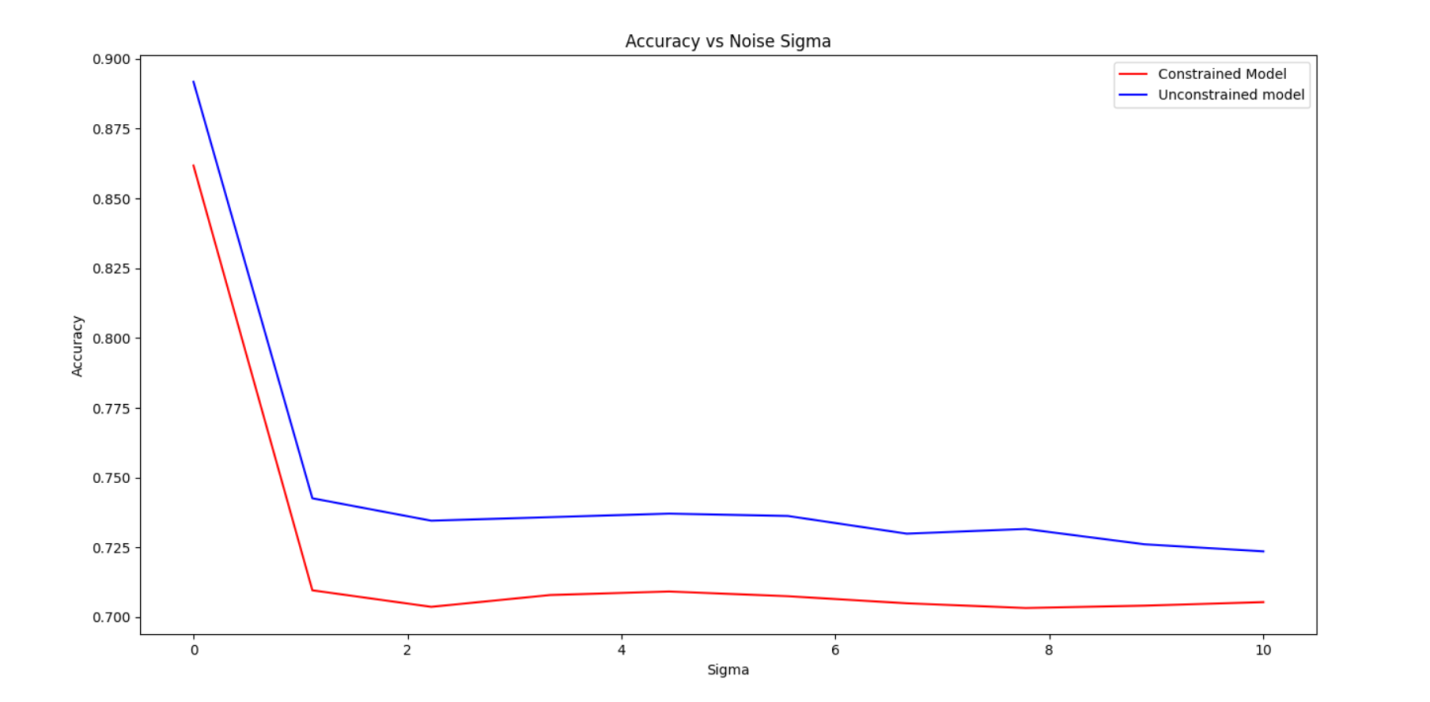
****

****

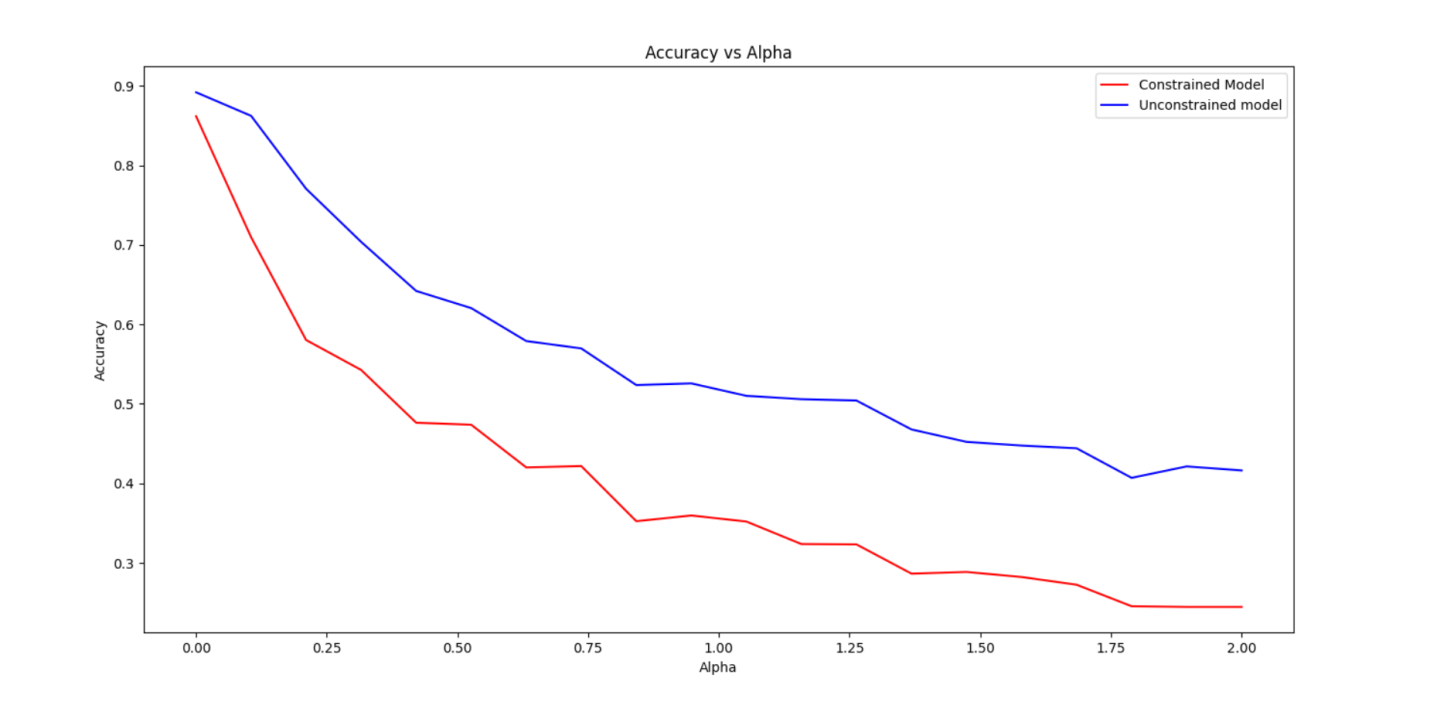
The white noise was added after the MFCCs were standardized.

****

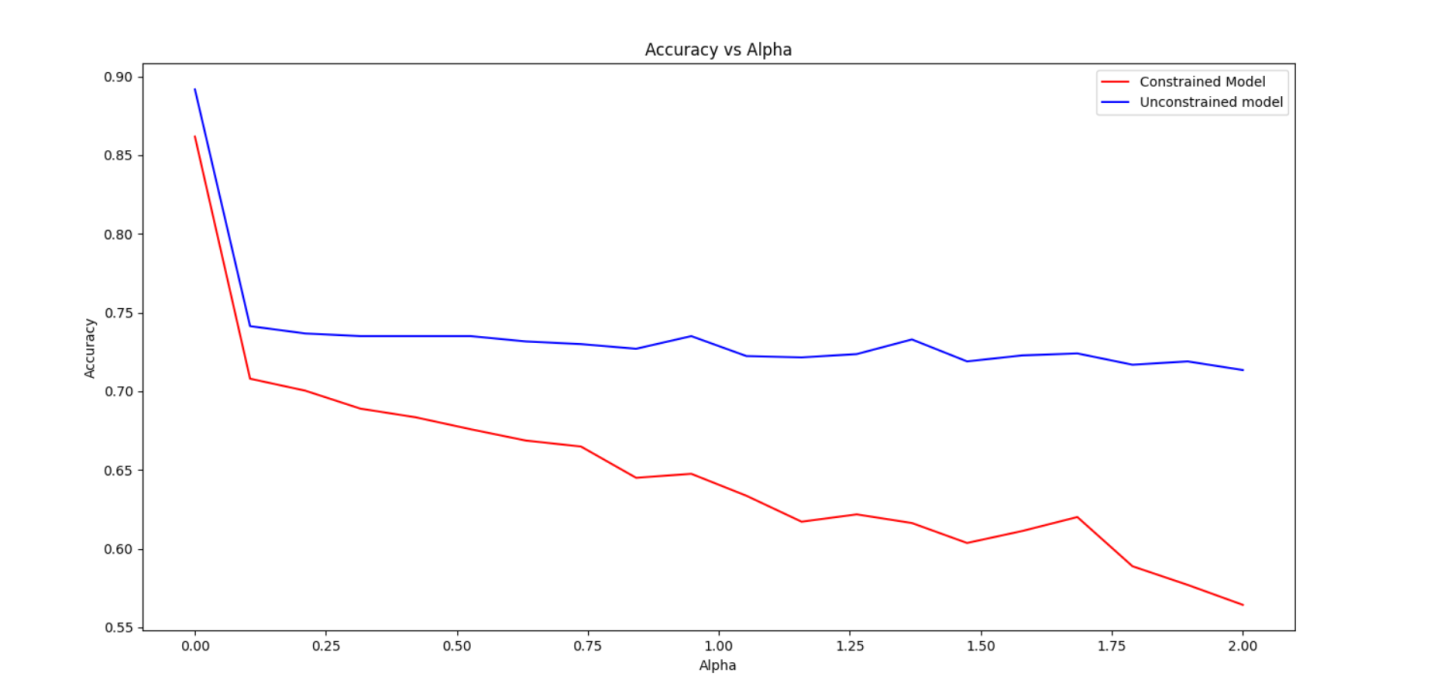
**The white noise was before the MFCCs were standardized.**

****

**The white noise mixture was added after the MFCCs were standardized. P=0.1**

****

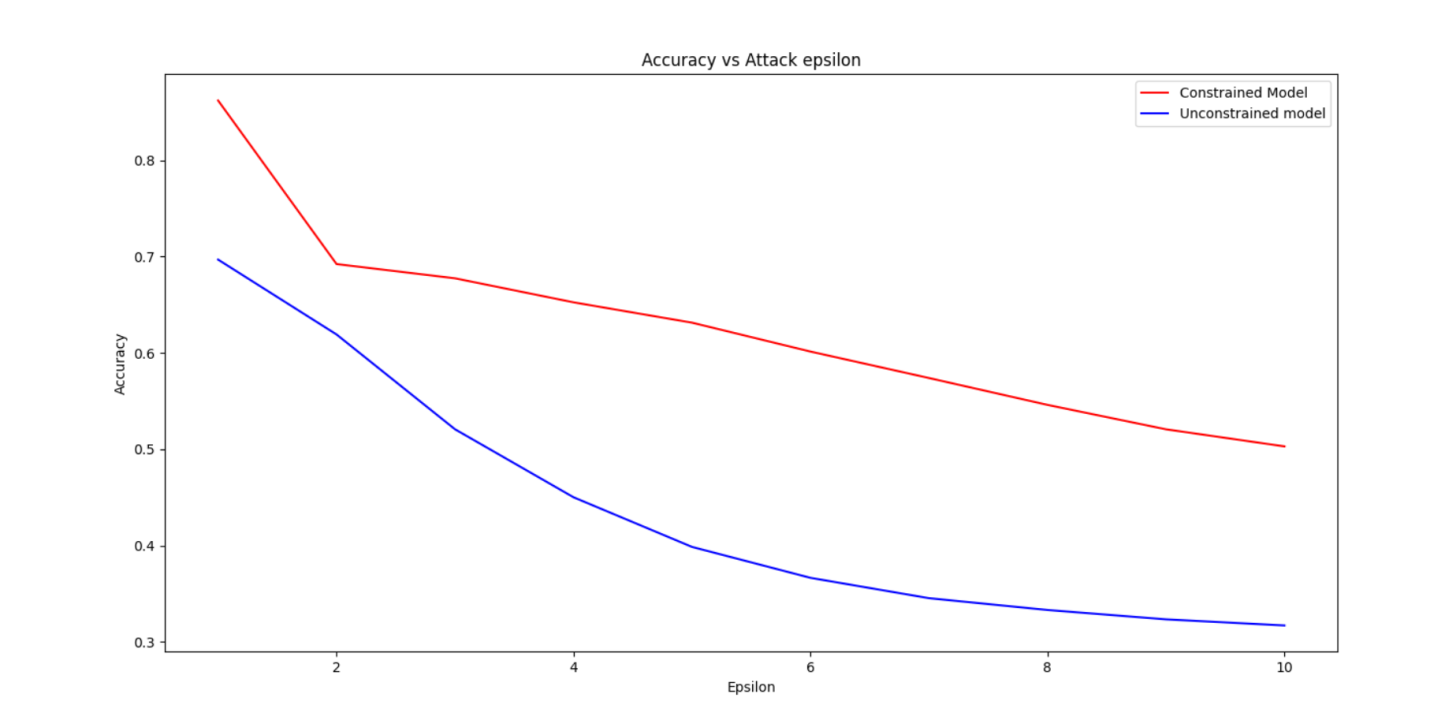
**The white noise mixture was added before the MFCCs were standardized. P=0.1**

****

**The attack was done after the MFCCs were standardized.**

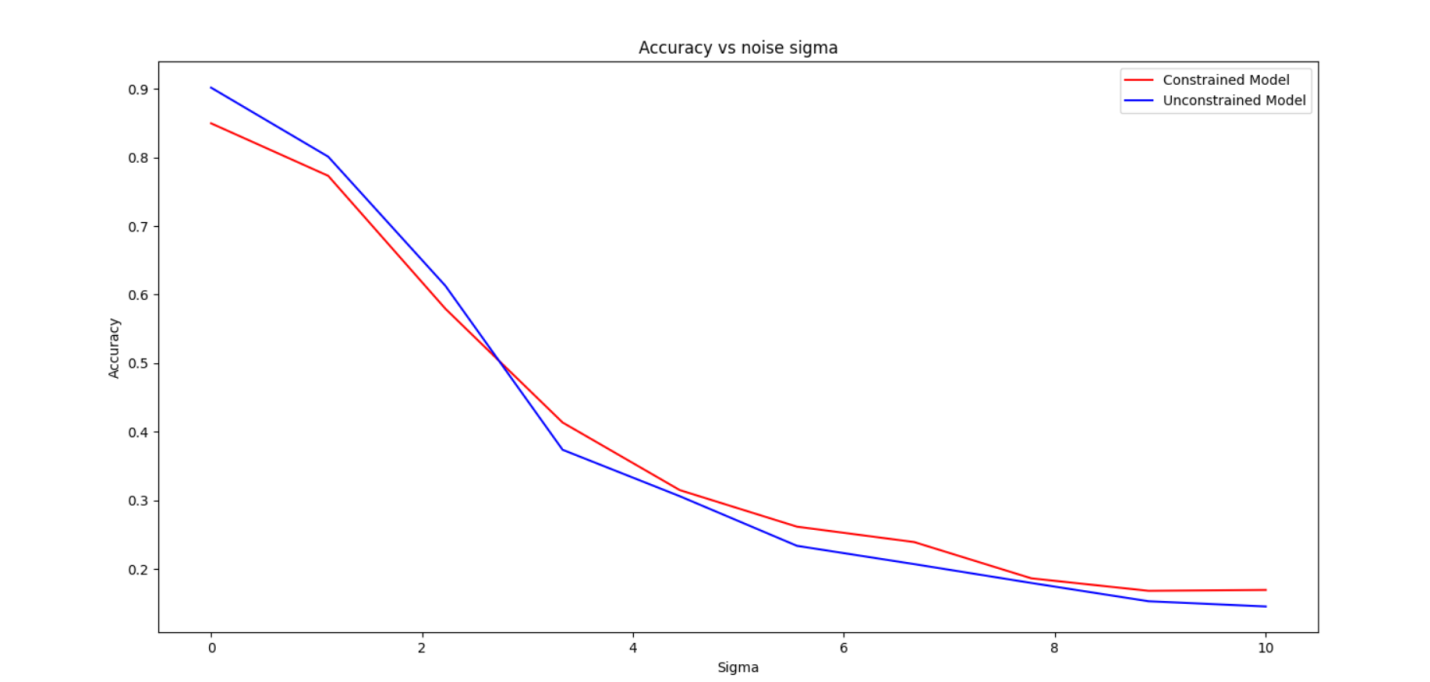
****

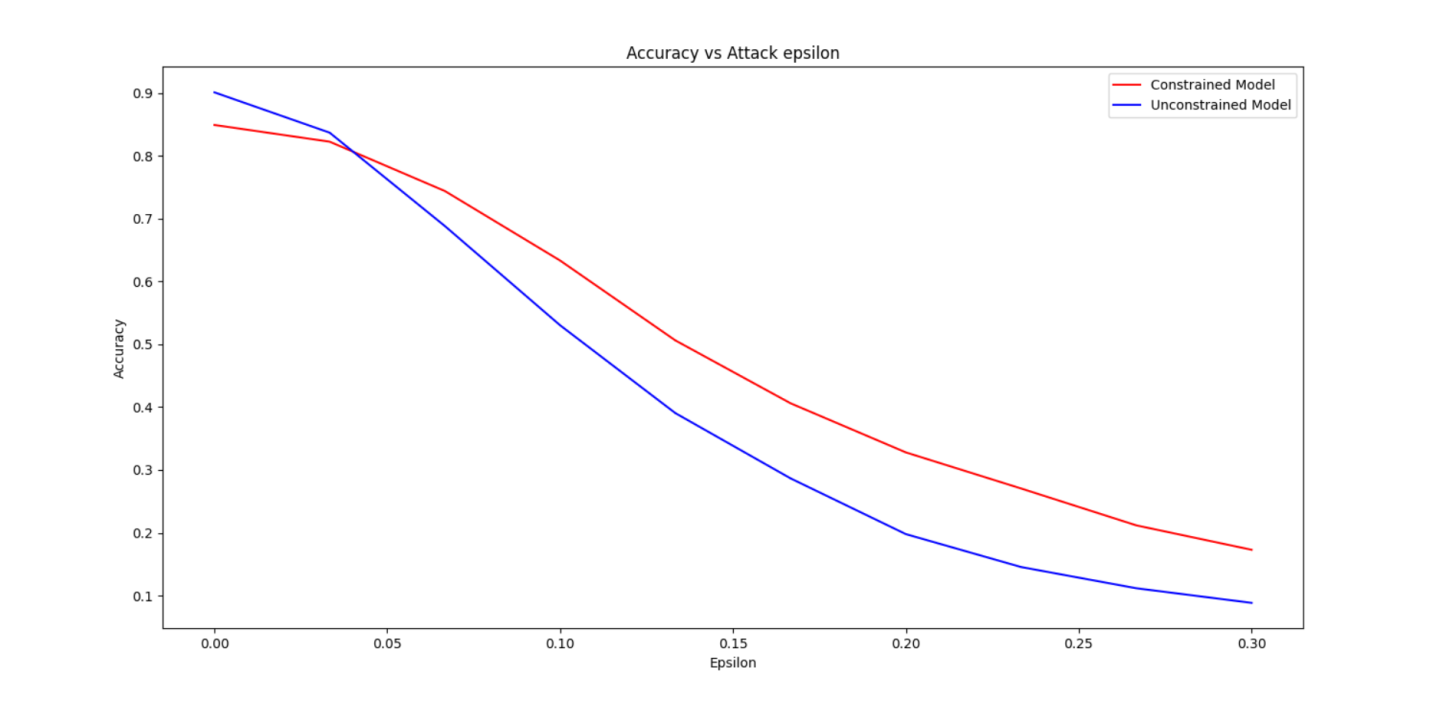
**The attack was done before the MFCCs were standardized.**

****

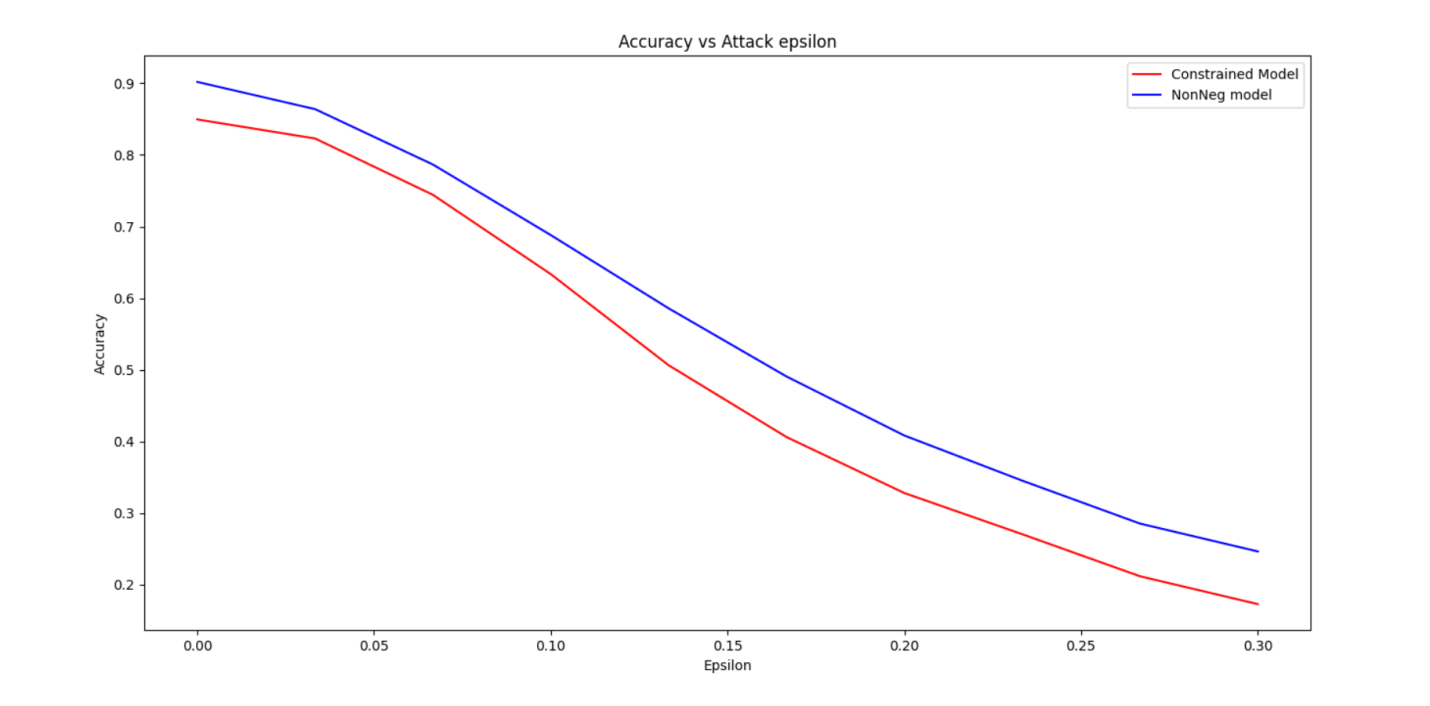
* **model\_constrained\_Rho001\_dropout02.h5**

****

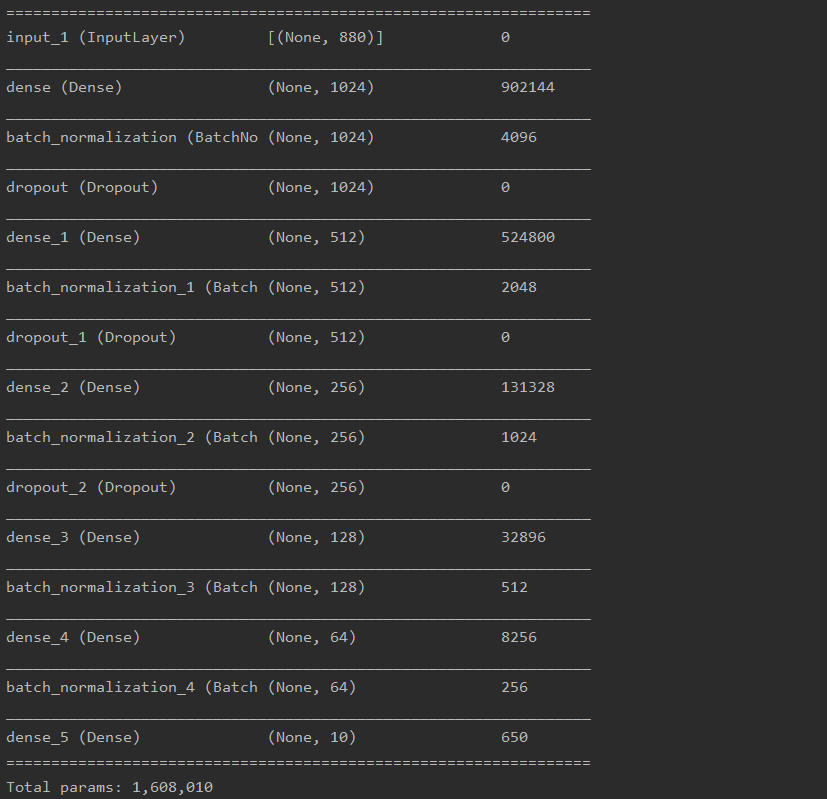
****

****

model\_constrained\_Rho001\_dropout02 vs baseline\_NonNeg

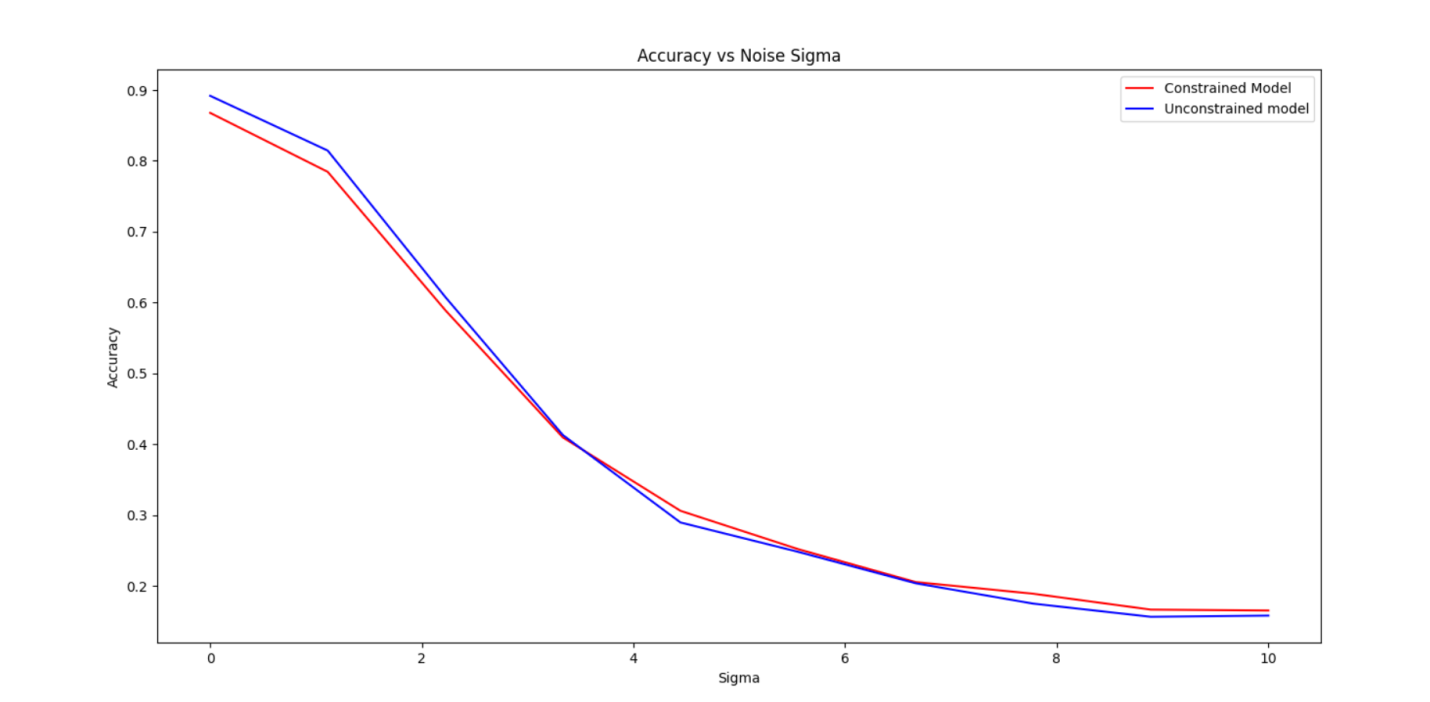


* **model\_constrained\_Rho01\_dropout01.h5**

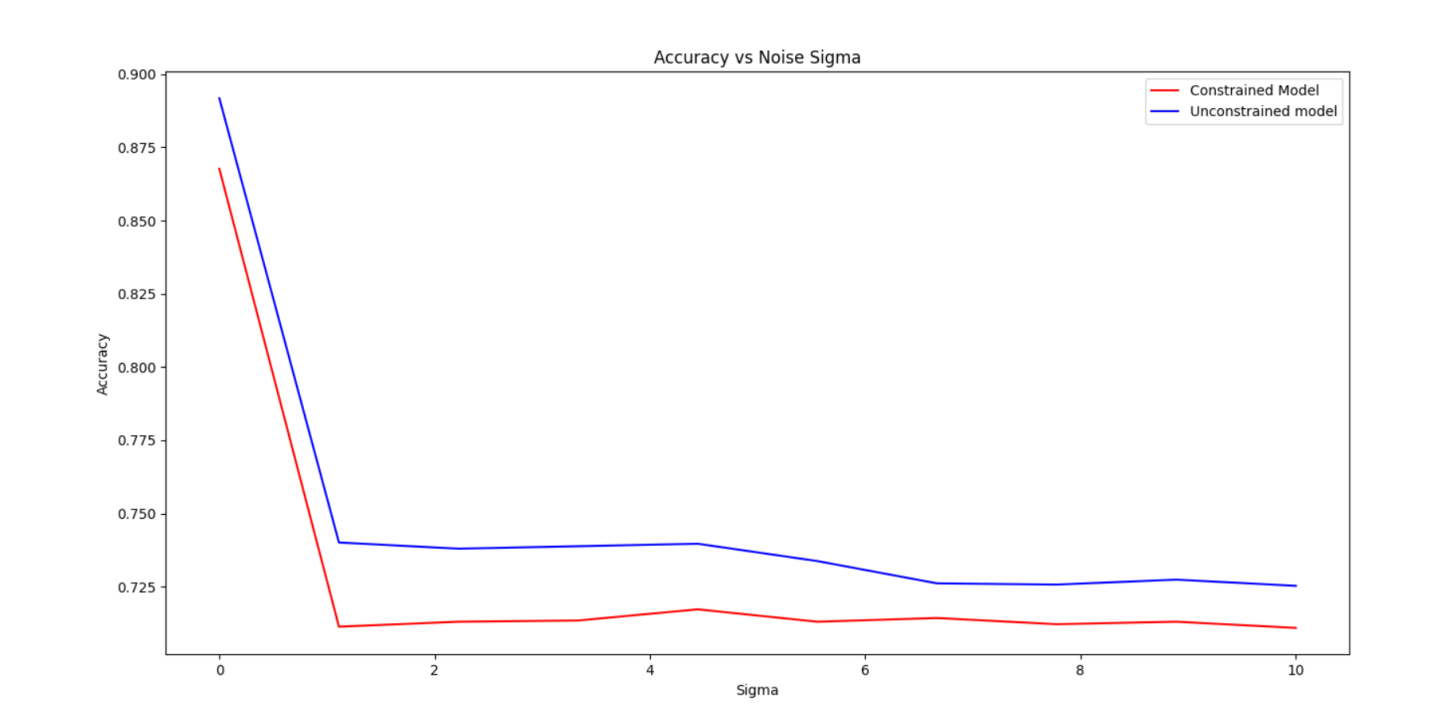




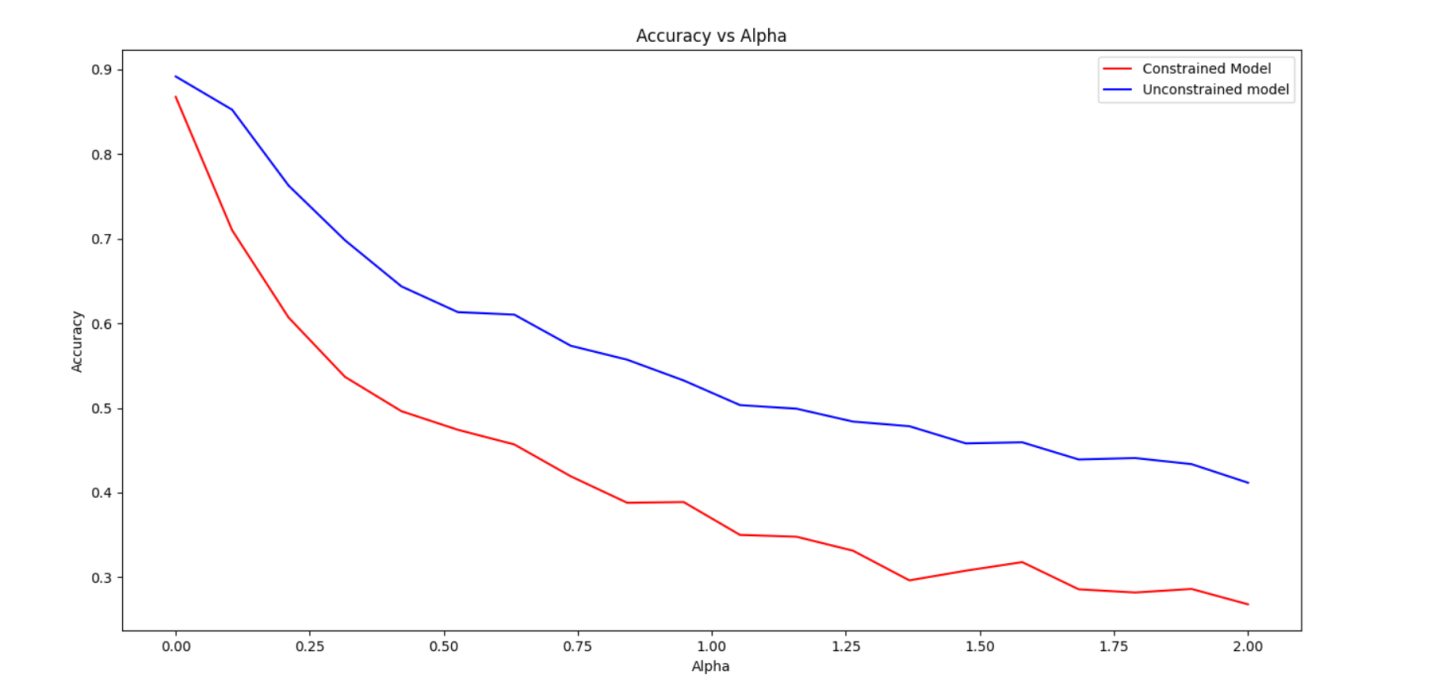
The white noise was added after the MFCCs were standardized.



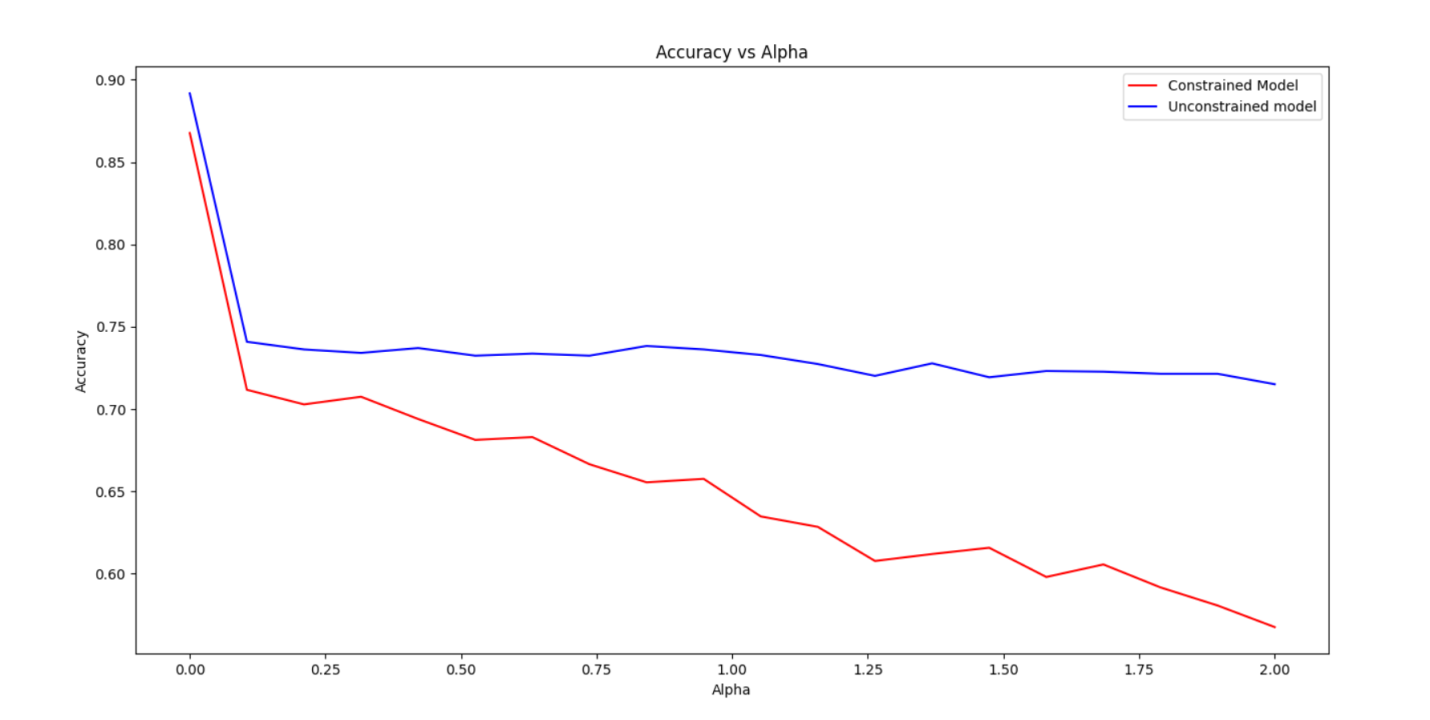
The white noise was added before the MFCCs were standardized.



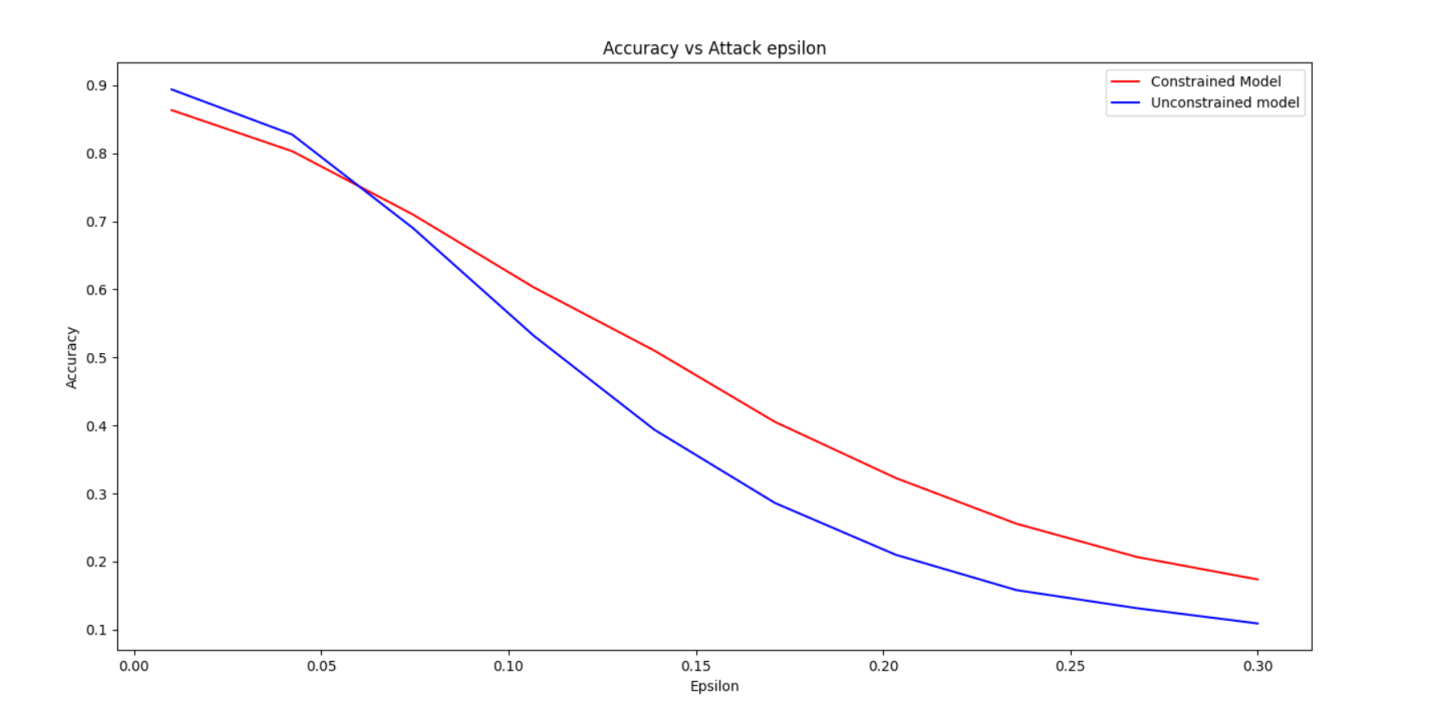
**The white noise mixture was added after the MFCCs were standardized. P=0.1**



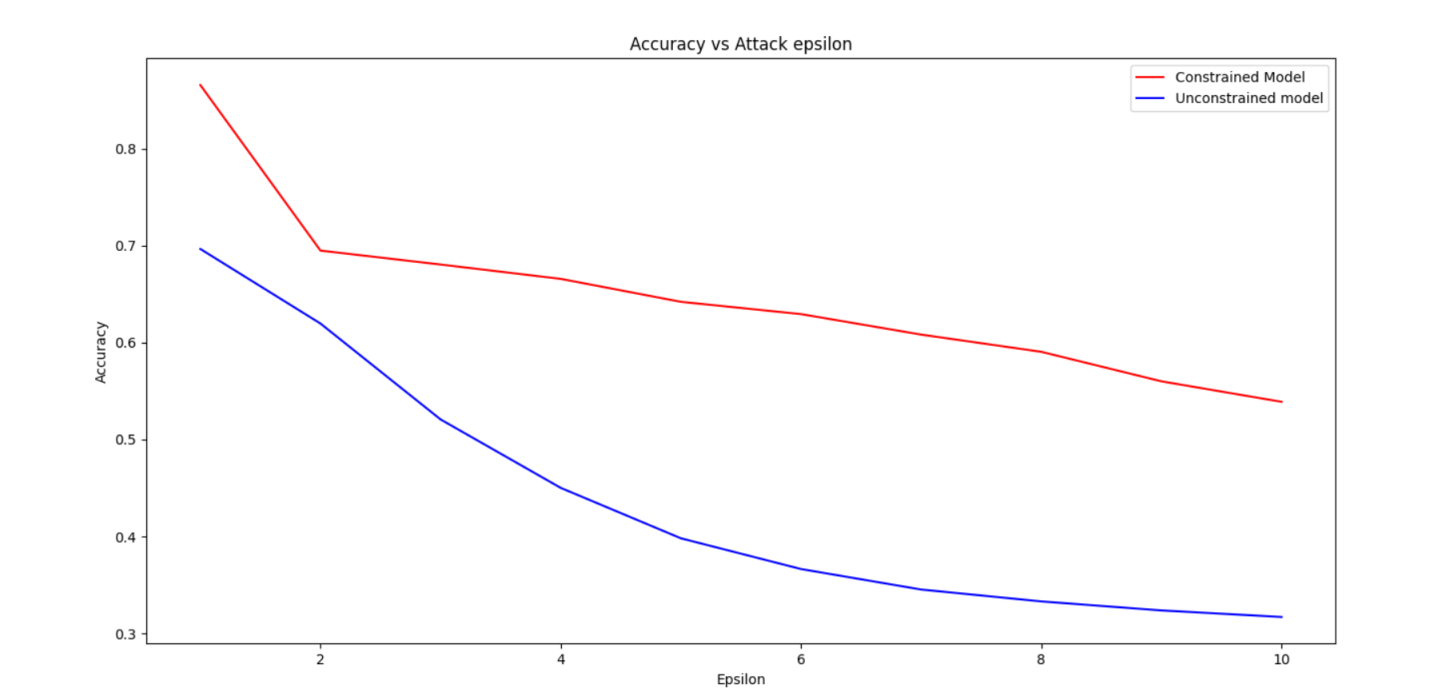
**The white noise mixture was added before the MFCCs were standardized. P=0.1**

****

**The attack was done after the MFCCs were standardized.**



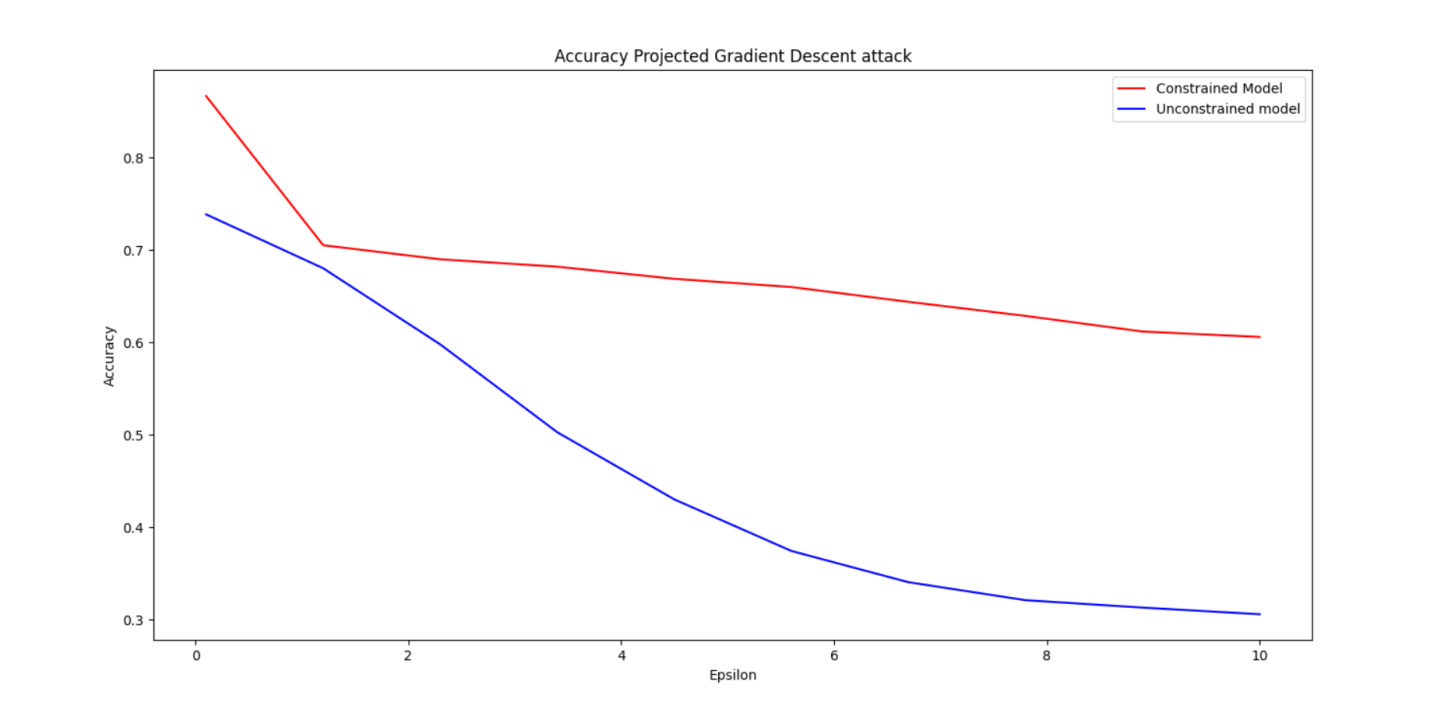
**The attack was done before the MFCCs were standardized.**



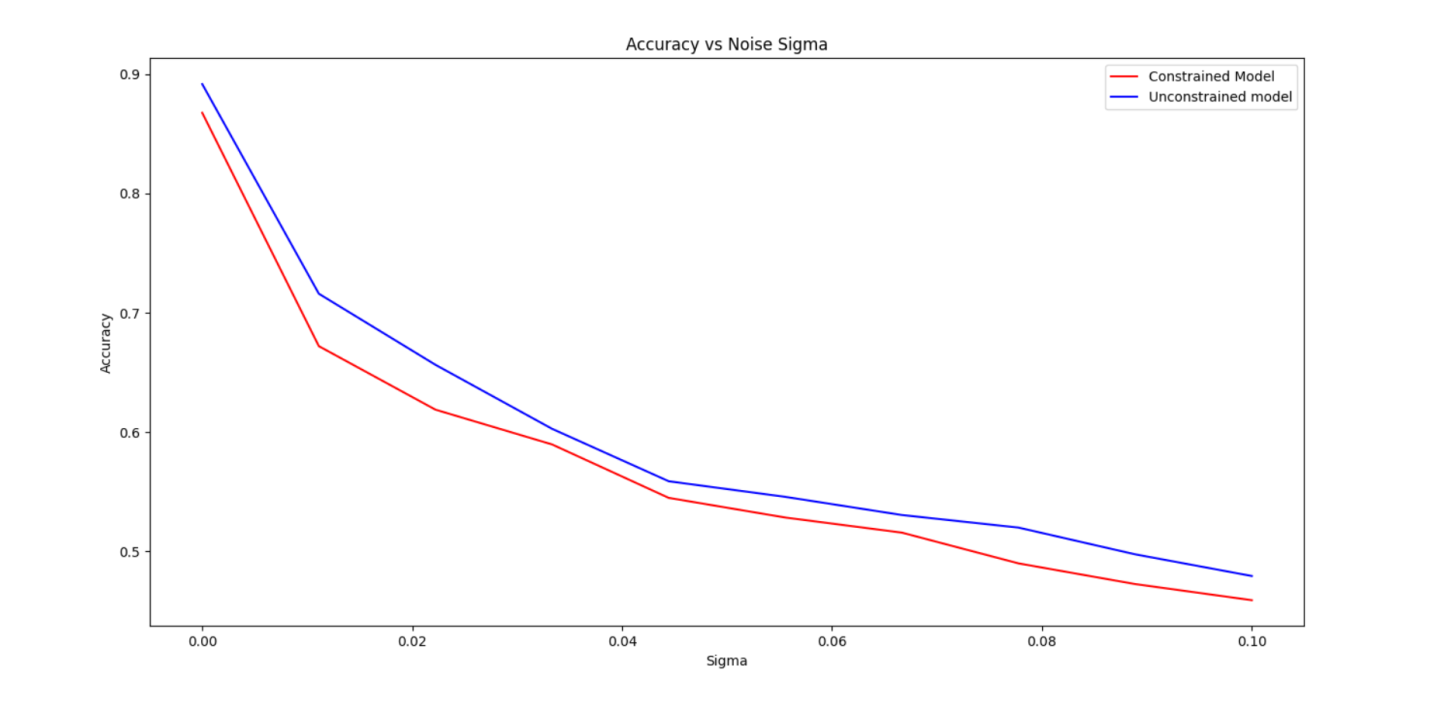
Carlini & Wagner L2 attack: confidence = 0.1



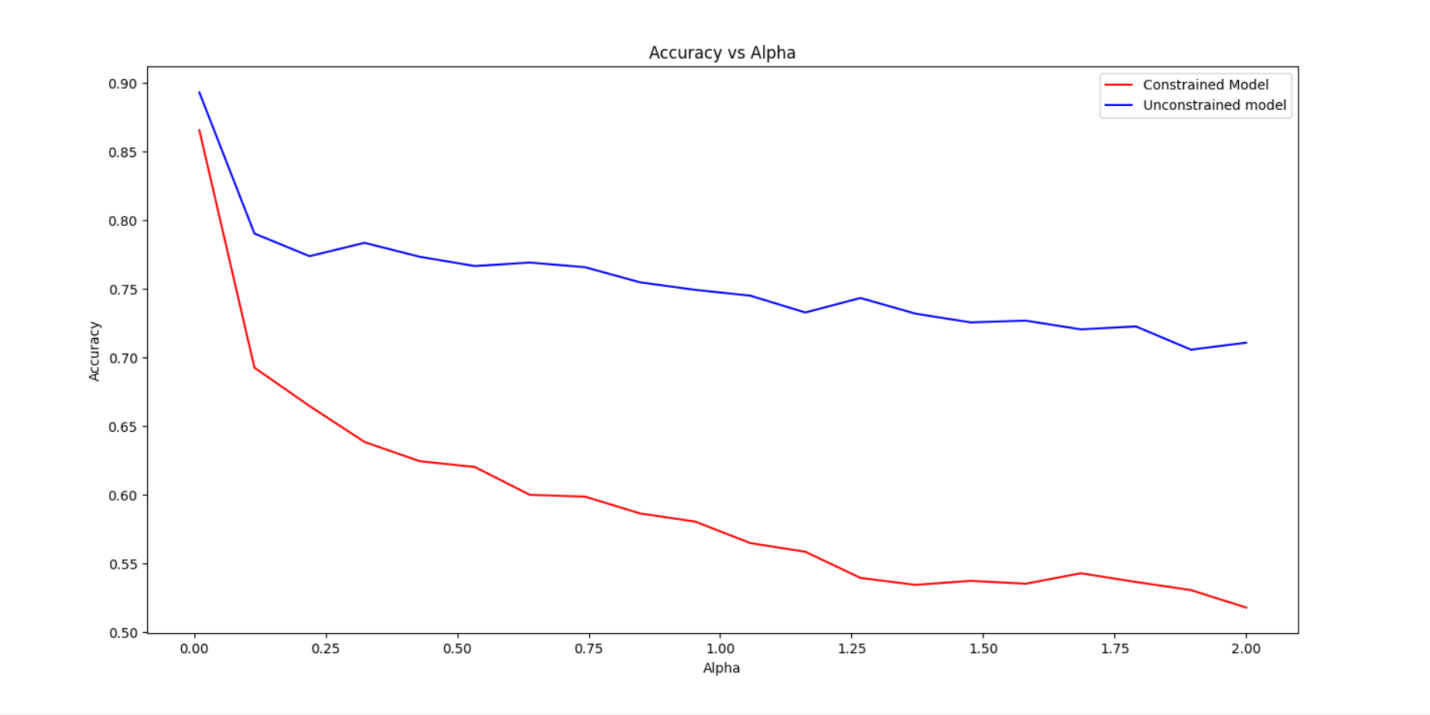
Projected Gradient Descent



White noise on audio.



Noise mixture on audio. P=0.1



White noise over audio with respect to SNR.

