Adversarial examples in Machine Learning.

Rafael Carvalhaes Possas

(rcar7834@uni.sydney.edu.au)

Master of Information Technology

*10 Articles or Books relevant to my research topics/area*

1 – Adversarial examples in the Physical World – Alexey Kurakin, Ian Goodfellow, Samy Bengio, 2016

2 – Adversarial classification – Dalvi, Nilesh, Domingos, Pedro, Sanghai, Sumit, Verma, Deepak et al. 2004

3 – Explaining and harnessing adversarial examples – Goodfellow, Ian J, Shlens, Jonathon, 2014

4 – ImageNet classification with deep convolutional neural networks – Krizhevsky, Alex, Sutskever, Ilya and Hinton, Geoffrey, 2012

5 – Neural machine translation by jointly learning to align and translate – Bahdanu, Dzmitry, Cho, Kyunghyun and Bengio, Yoshua, 2015

6 – Face recognition on consumer devices: Reflection on replay attacks – Smith, Daniel F, Wiliem, Arnold and Lovell, Brian C, 2015

7 – Intriguing properties of neural networks – Szegedy, Christian Zaremba, Wojciech, Sutskever, Ilya, Bruna, Joan, Erhan, Dumitru, Goodfellow, Ian J and Fergus, Rob, 2014

8 – Imagenet large scale visual recognition challenge – Russakovsky, Olga, Deng, Jia, Su, Hao, Krause, Jonathan, Satheesh, Sanjeev, Ma, Sean, Huang, Zhiheng, Karpathy, Andrej, Khosla, Aditya, Bernstein, Michael, et al. 2014

9 – Neural Networks and Deep Learning (http://neuralnetworksanddeeplearning.com/) – Nielsen Michael, 2016

10 – Deep Learning (<http://www.deeplearningbook.org/>) – Ian Goodfellow, Yoshua Bengio and Aaron Courville, MIT Press Book, 2014

11 – Deep Learning: A Practitioner’s Approach – Adam Gibson & Josh Patterson, O’Reilly, 2016

12 – Towards Deep Neural Network Architectures Robust to Adversarial Examples – Shixiang Gu, Luca Rigazio, 2014

*30 Top A\*, A and B conference events and journals in Deep Learning / Machine Learning*

**CORE CONFERENCES RANKING**

**Rank: A\***

1 – Advances in Neural Information Processing Systems – NIPS – A\*

2 – International Conference on Machine Learning – ICML – A\*

3 – IEEE International Conference on Computer Vision – ICCV – A\*

4 – National Conference of the American Association for Artificial Intelligence – AAAI – A\*

5 – International Joint Conference on Artificial Intelligence – IJCAI – A\*

**Rank: A**

1 – IEEE International Joint Conference on Neural Networks – IJCNN – A

2 – European Conference on Machine Learning – ECML – A

3 – European Conference on Computer Vision – ECCV – A

4 – IEEE Conference on Computer Vision and Pattern Recognition – CVPR – A

5 – IEEE Workshop on Applications of Computer Vision – WACV - A

**Rank: B**

1 – French Conference on Knowledge Acquisition and Machine Learning – FCKAML – B

2 – Joint Workshop on Multimodal Interaction and Related Machine Learning Algorithms – MLMI – B

3 – Asian Conference on Computer Vision – ACCV – B

4 – Artificial Neural Networks in Engineering Conference – ANNIE – B

5 – European Symposium on Artificial Neural Networks – ESANN – B

**CORE JOURNALS RANKING**

**Rank: A\***

1 – IEEE Transaction on Neural Networks – ERA2010 - A\*

2 – Machine Learning – ERA2010 – A\*

3 – Artificial Intelligence – ERA2010 – A\*

4 – IEEE Transactions on Neural Networks – ERA2010 – A\*

5 – IEEE Transactions on Pattern Analysis and Machine Intelligence – ERA2010 – A\*

**Rank: A**

1 – Neural Networks - ERA2010 – A

2 – Journal of Machine Learning Research – ERA2010 – A

3 – Computer Vision and Image Understanding – ERA2010 – A

4 – International Journal of Computer Vision – ERA2010 – A

5 – Computer Vision and Image Understanding – ERA2010 - A

**Rank: B**

1 – IET Computer Vision – ERA2010 – B

2 – ACM Transactions on Knowledge Discovery From Data – ERA2010 – B

3 – Connection Science: Journal of Neural Computing, AI and Cognitive Research – ERA2010 – B

4 – Image and Vision Computing – ERA2010 – B

5 – International Journal of Pattern Recognition and Artificial Intelligence – ERA2010 – B

**Deep Learning Research Groups**

1 – Stanford University – Andrew Ng, Christopher Manning, Fei-fei Li

2 – Google Research – Jeff Dean, Geoffrey Hinton, Samy Bengio, Ilya Sutskever, Ian Goodfellow, Oriol Vinyals, Dumitru Erhan, Quoc Le

3 – Google DeepMind – Alex Graves, Karol Gregor, Koray Kavukcuoglu, Andriy Mnih, Guillaume Desjardins, Xavier Glorot, Razvan Pascanu, Volodymyr Mnih

4 – Microsoft Research – Li Deng et al.

5 – Twitter’s Deep Learning Group – Hugo Larochelle, Ryan Adams, Clement Farabet et al.

6 – Facebook AI Research (FAIR) – Yann Lecun, Rob Fergus, Jason Weston, Antoine Bordes, Soumit Chintala, Leon Bouttou, Ronan Collobert, Yann Dauphin et al.