28th Vienna Deep Learning Meetup

24th June 2019

#VDLM

Vienna Deep Learning Meetup

The Organizers:

René Donner
contextflow

Thomas Lidy
Musimap

Alex Schindler
AIT & TU Wien

Jan Schlüter
OFAI & UTLN

Topics for Today

Vienna Deep Learning Meetup

Introduction

Adversarial Machine Learning - An Introduction to Backdoor, Evasion and Inversion Attacks
Rudolf Mayer, Senior Researcher, SBA Research & Lector, TU Wien

Machine Learning Survey Results: The importance of reproducible ML pipeline elements
Camillo Pachmann, CEO - MLreef

<Break>

Using EEG and GAN to train robotic movements - *Emanuel Gollob, Designer & Media Artist*

Deep Learning for Electrical Biosignals and their Application in Medical Products
Franz Fürbass, Scientist in Biosignal Processing Group at Austrian Institute of Technology (AIT)

Hot Topics
EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks *Michael Pieler*
Adversial Learning for Fairness, Domain Adaptation and Unsupervised Learning *René Donner, contextflow*

Vienna Deep Learning Meetup


MLReef
The ideal nurturing ground
for creating the best
machine learning projects.

Survey Results

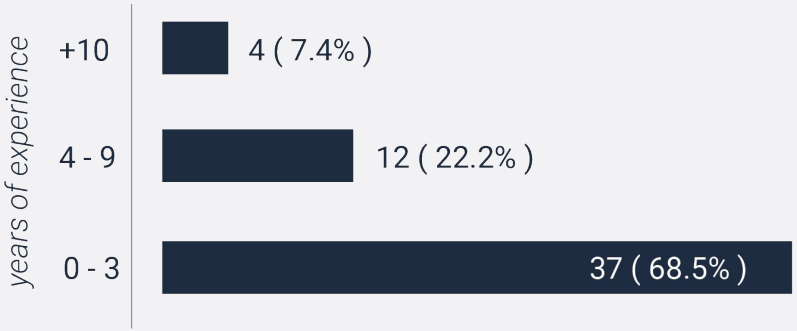
Version: 1.0

N=54

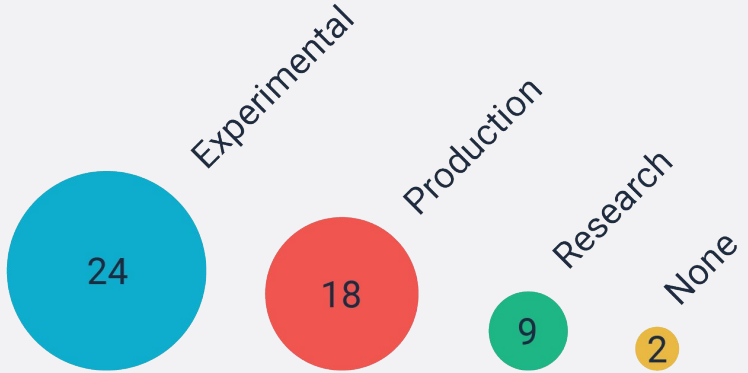
participate at

www.mlreef.com

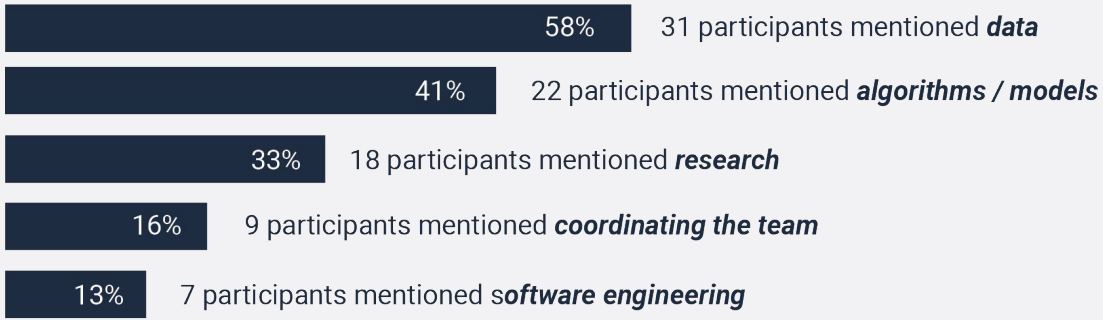
Years of experience



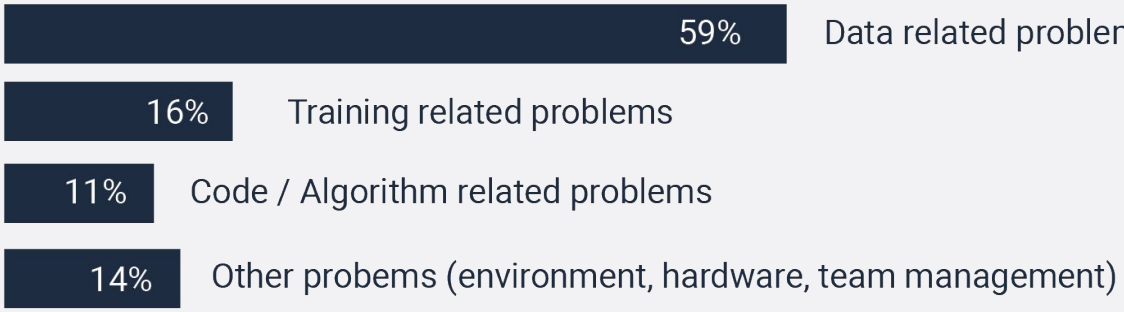
Use case level



Most time spent



Pains & problems



Importance of version control for data

0 as the lowest, 10 as the highest

Avg.: 6.4 Med.: 6 Mode: 9

Noticeable correlation:

the more the use case is for “production”, the higher the importance for version control on data

Importance of version control for models

0 as the lowest, 10 as the highest

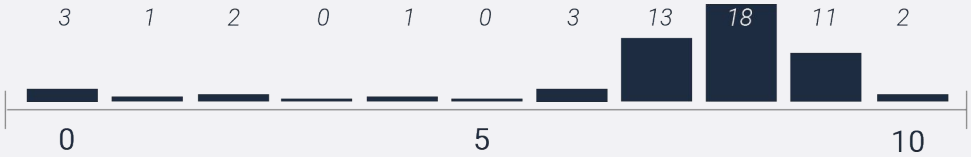
Avg.: 7.1 Med.: 8 Mode: 8

Noticeable correlation:

it seems that only for “experimental” use cases or for inexperienced data scientist version control on models is not so important.

Importance of “community content”

0 as the lowest, 10 as the highest



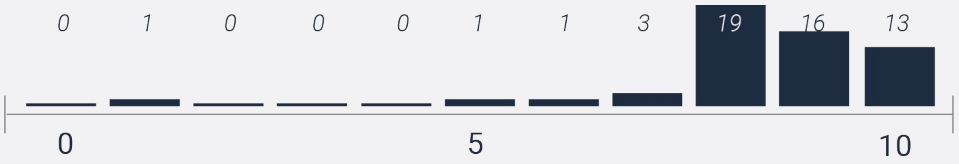
Avg.: 7.0 Med.: 7 Mode: 8

Noticeable correlation:

it seems that only for experienced data scientists (+10 years) the importance of open source content diminishes. For less experienced data scientists it is very important.

Importance of replicability of results

0 as the lowest, 10 as the highest



Avg.: 8.5 Med.: 8 Mode: 8

Noticeable correlation:

no matter on what use cases or how experienced, replicability is always very important for the majority of participants.

ML tools

Keras Pytorch Fast AI Google Cloud

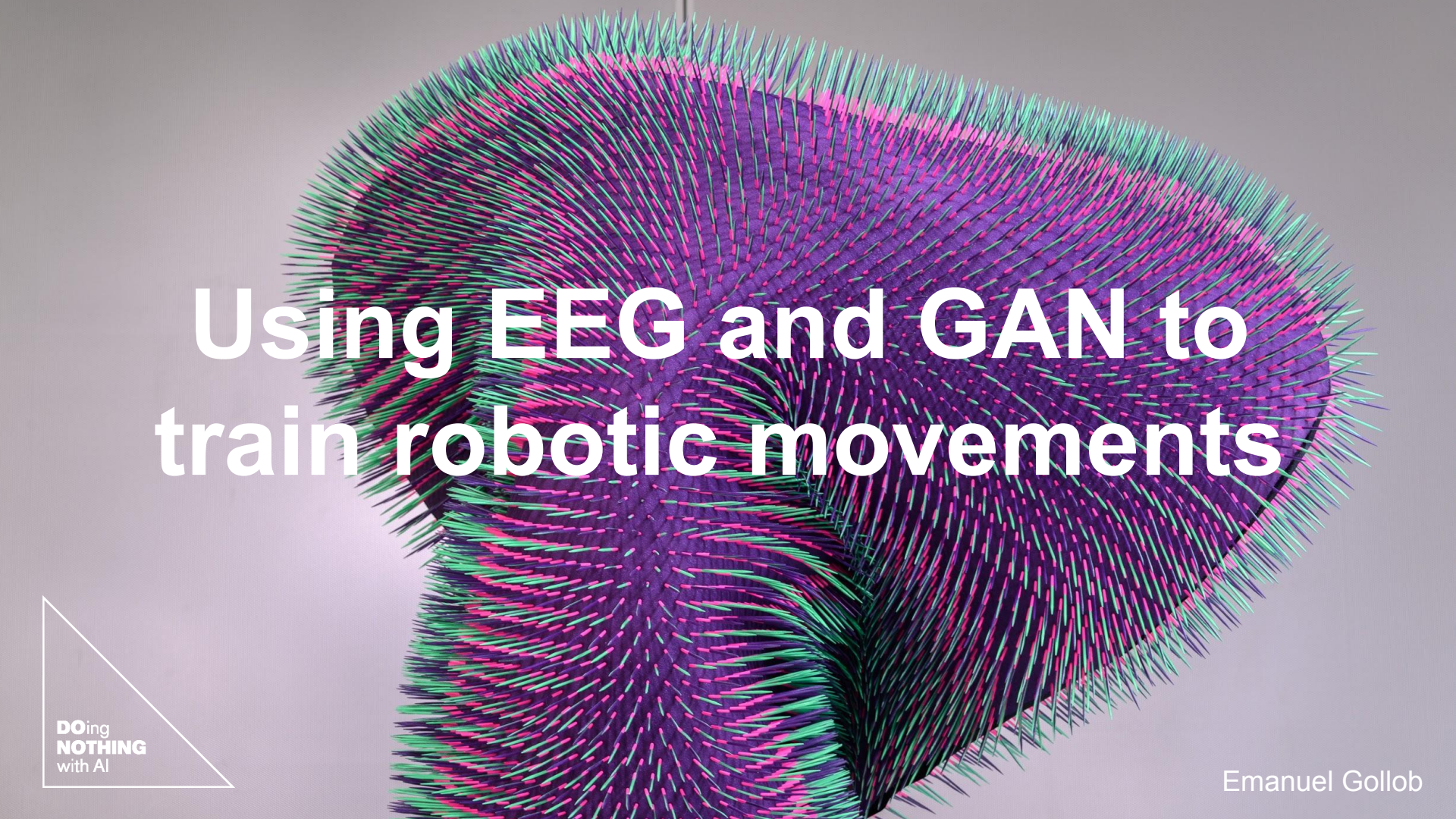
Python Tensorflow Pandas Pycharm Pachy derm

R Scikit-learn Apache Julia / Knet

www.mlreef.com

Camillo Pachmann
ceo

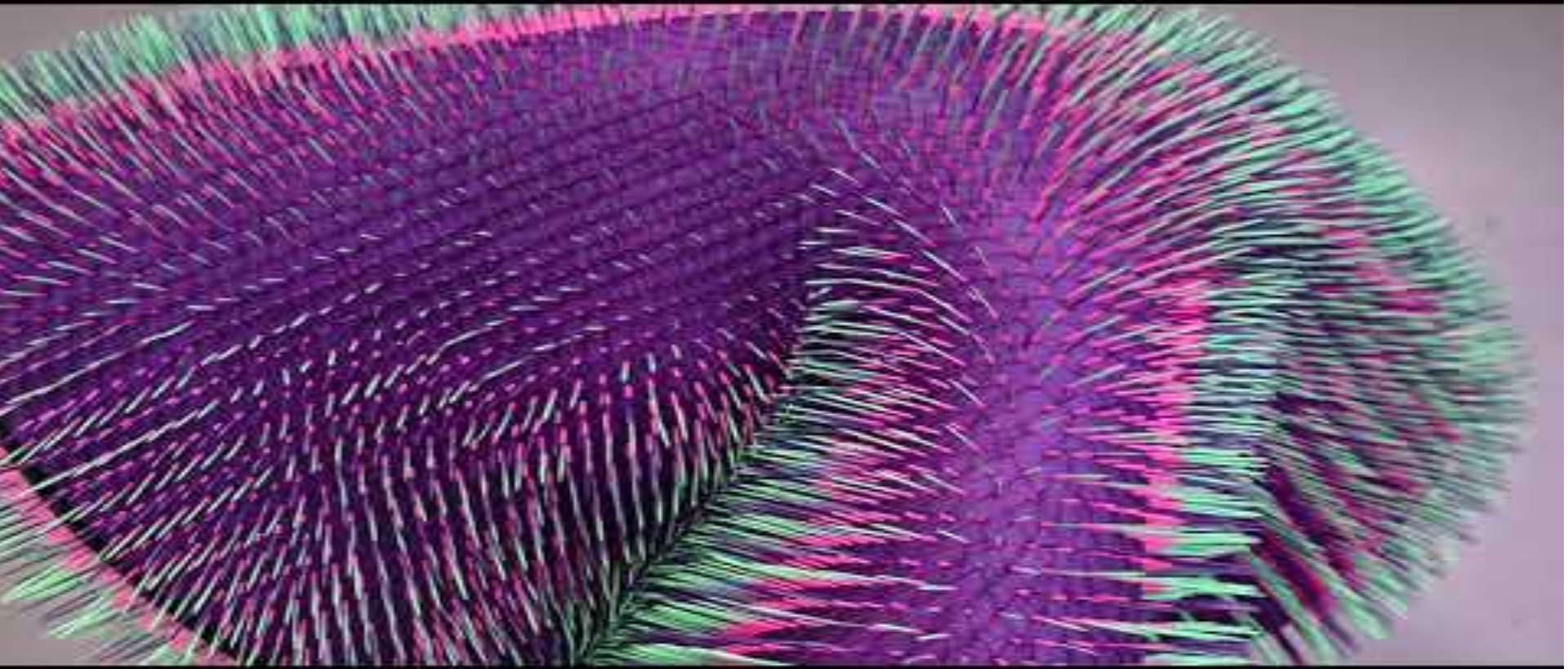
cp@mlreef.com
+43 650 3711055

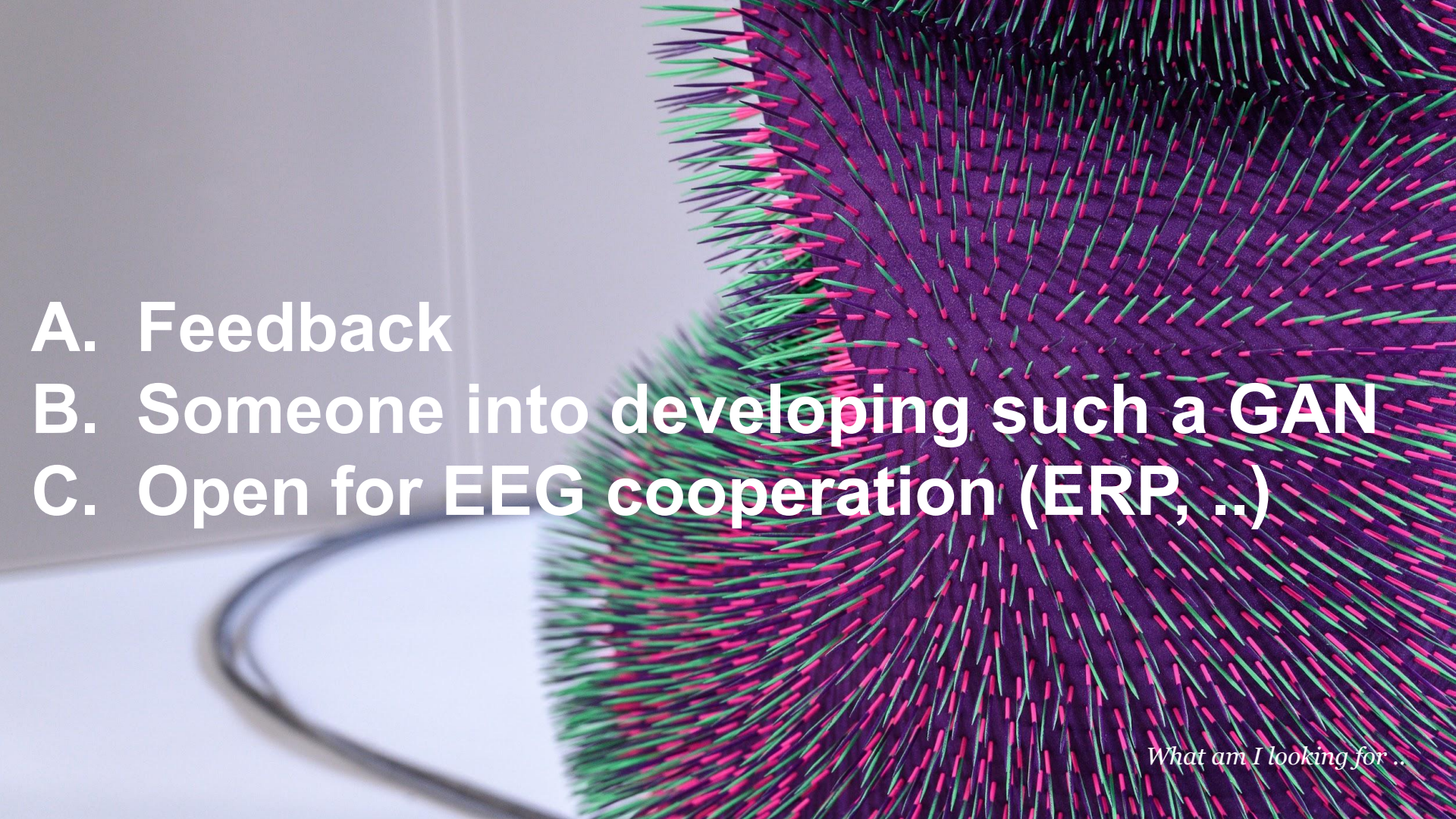


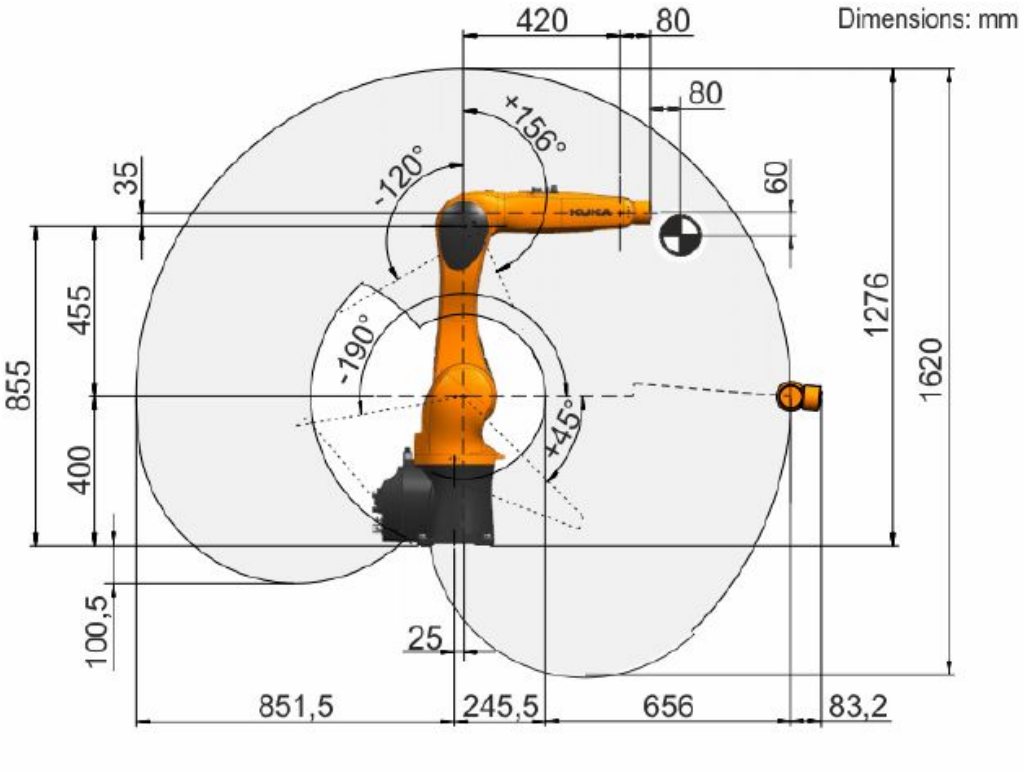
Using EEG and GAN to train robotic movements

DOing
NOTHING
with AI

Emanuel Gollob



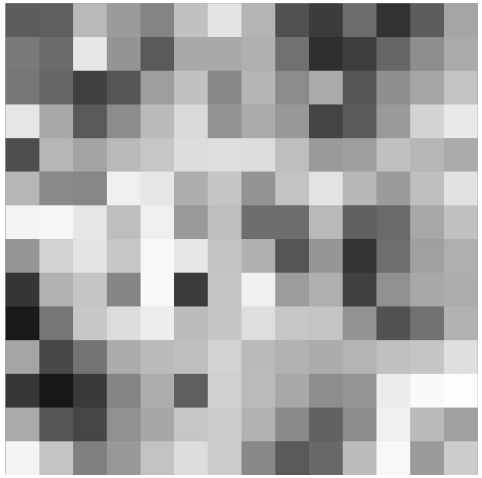

A. Feedback
B. Someone into developing such a GAN
C. Open for EEG cooperation (ERP, ..)
What am I looking for ..



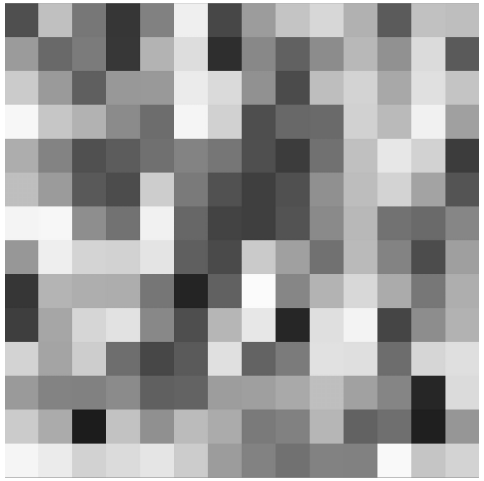
Axis Limitations Kuka KR6 R900

Movement Control & Analysis - Rhinoceros, Grasshopper, Kuka PRC, Mx Automation

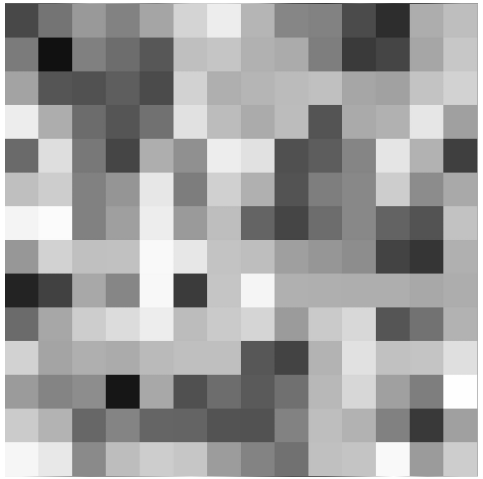
196 parameters between 0 and 255



*choreo 5012902



*choreo 897908890



*choreo 378906323

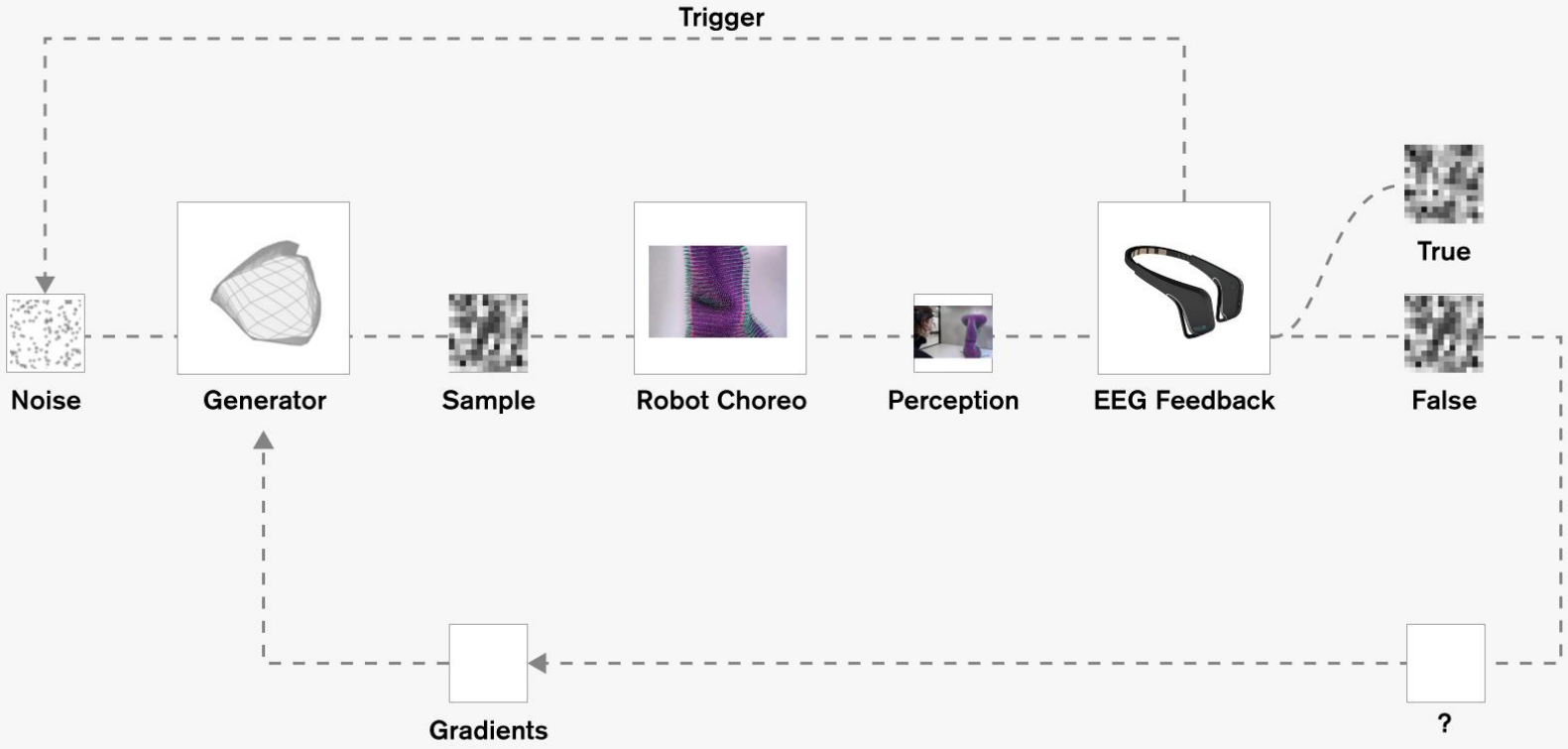
Choreography Parameter Examples

Realtime EEG Feedback - Muse 2016 EEG headband

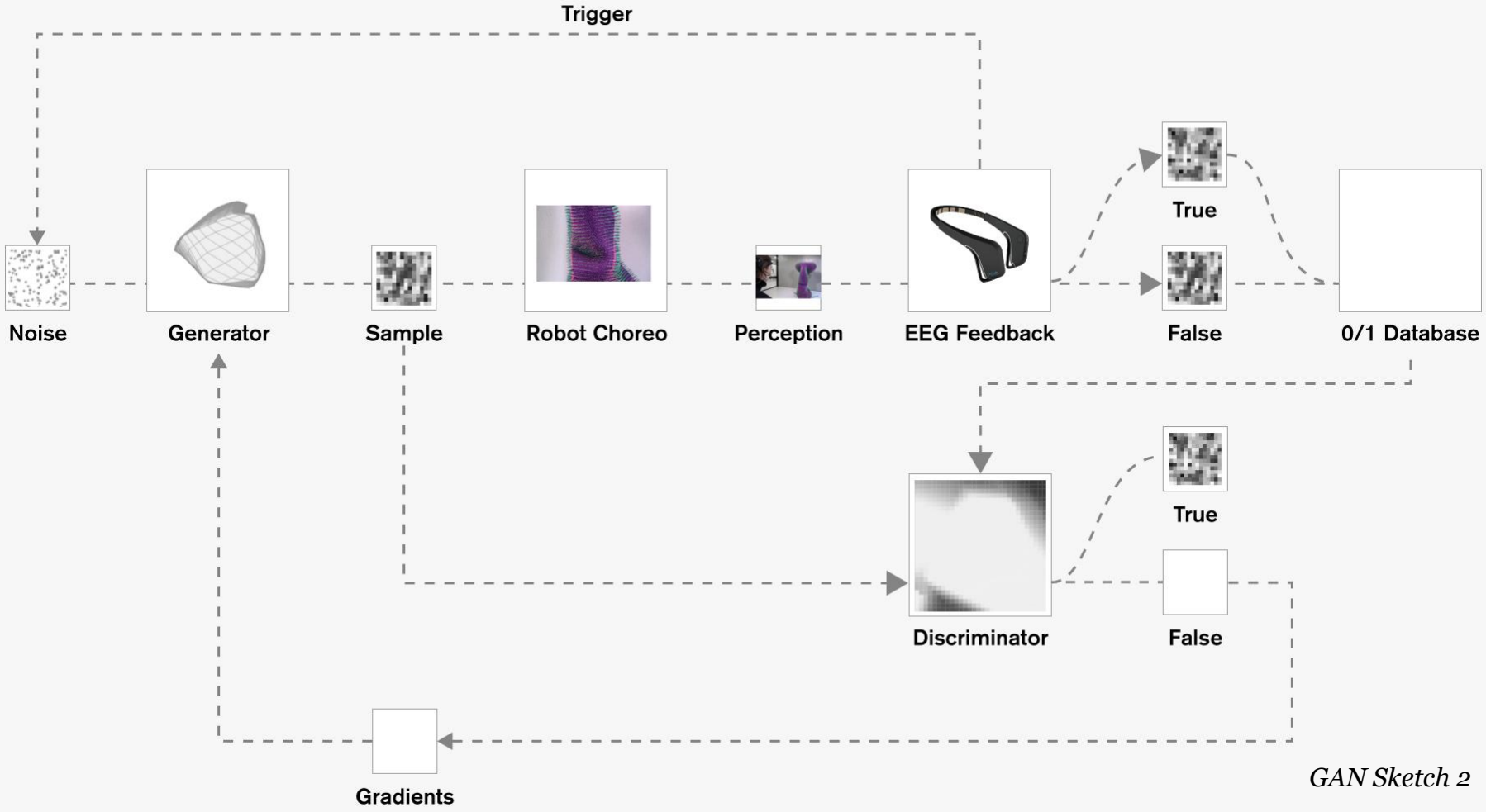
Muse 2016 EEG headband with relative Alpha and Theta interpretation in the frontal cortex

Enobio EEG Cap from Neuroelectrics with "Braindecode" from Schirrmeister & team

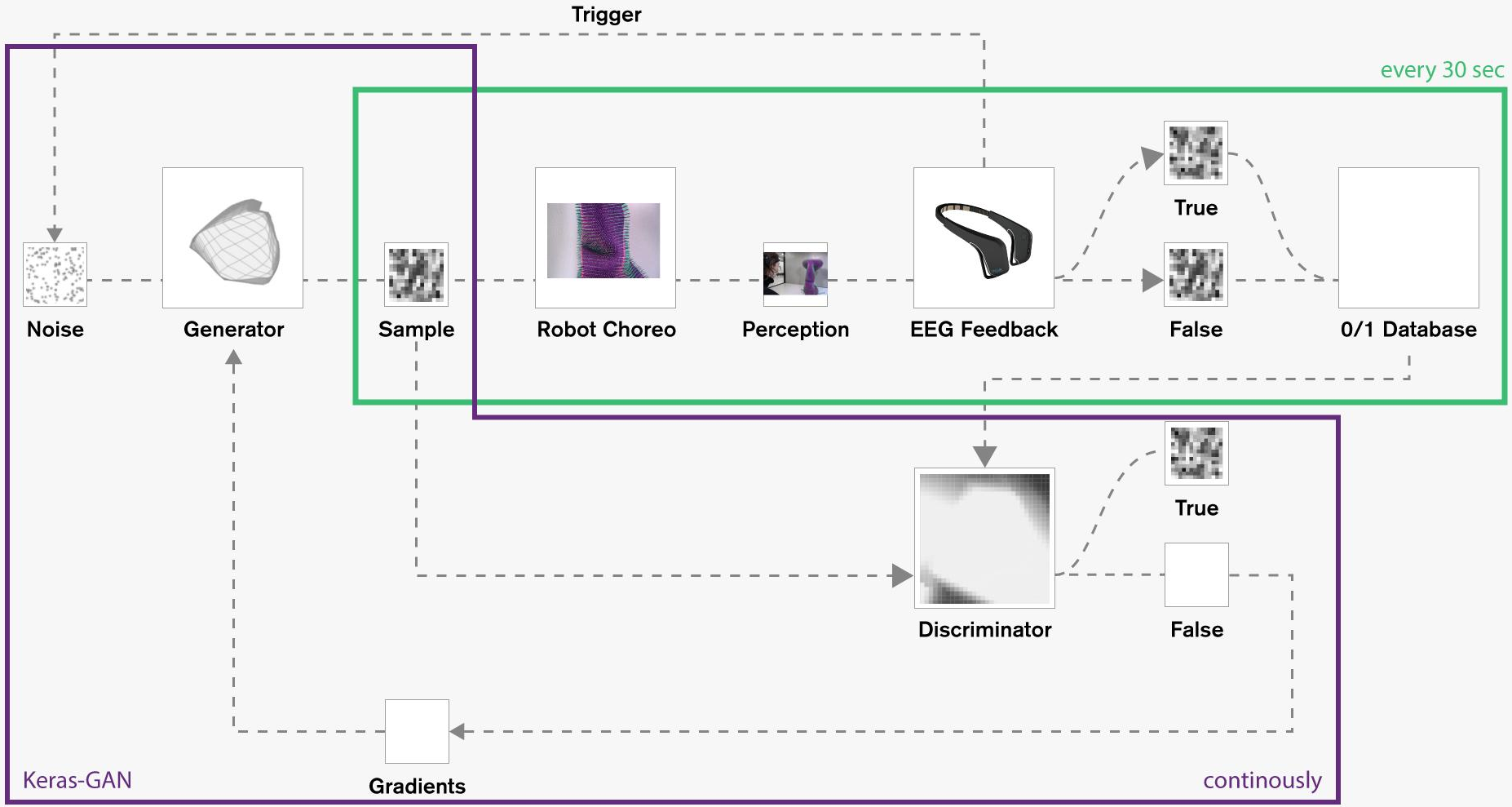
A. DMN - default mode network activation (Loretta)
B. Relative Alpha & Theta change in the frontal cortex
C. ERP - error related potential
D. ...


Trigger
Noise
Generator
Sample
Robot Choreo
Perception
EEG Feedback
True
False
Gradients
?

GAN Sketch 1


Trigger
Noise
Generator
Sample
Robot Choreo
Perception
EEG Feedback
True
False
0/1 Database
Discriminator
True
False
Gradients

GAN Sketch 2


Trigger
every 30 sec
Noise
Generator
Sample
Robot Choreo
Perception
EEG Feedback
True
False
0/1 Database
True
Discriminator
False
Gradients
Keras-GAN
continously


Thank you!
DOing
NOTHING
with AI
emanuel@emanuelgollob.com

DOing
NOTHING
with AI

Doing Nothing with AI **is a robotic installation which uses EEG measurements to optimize its choreography with the aim to make me *Do Nothing* in 2019.**

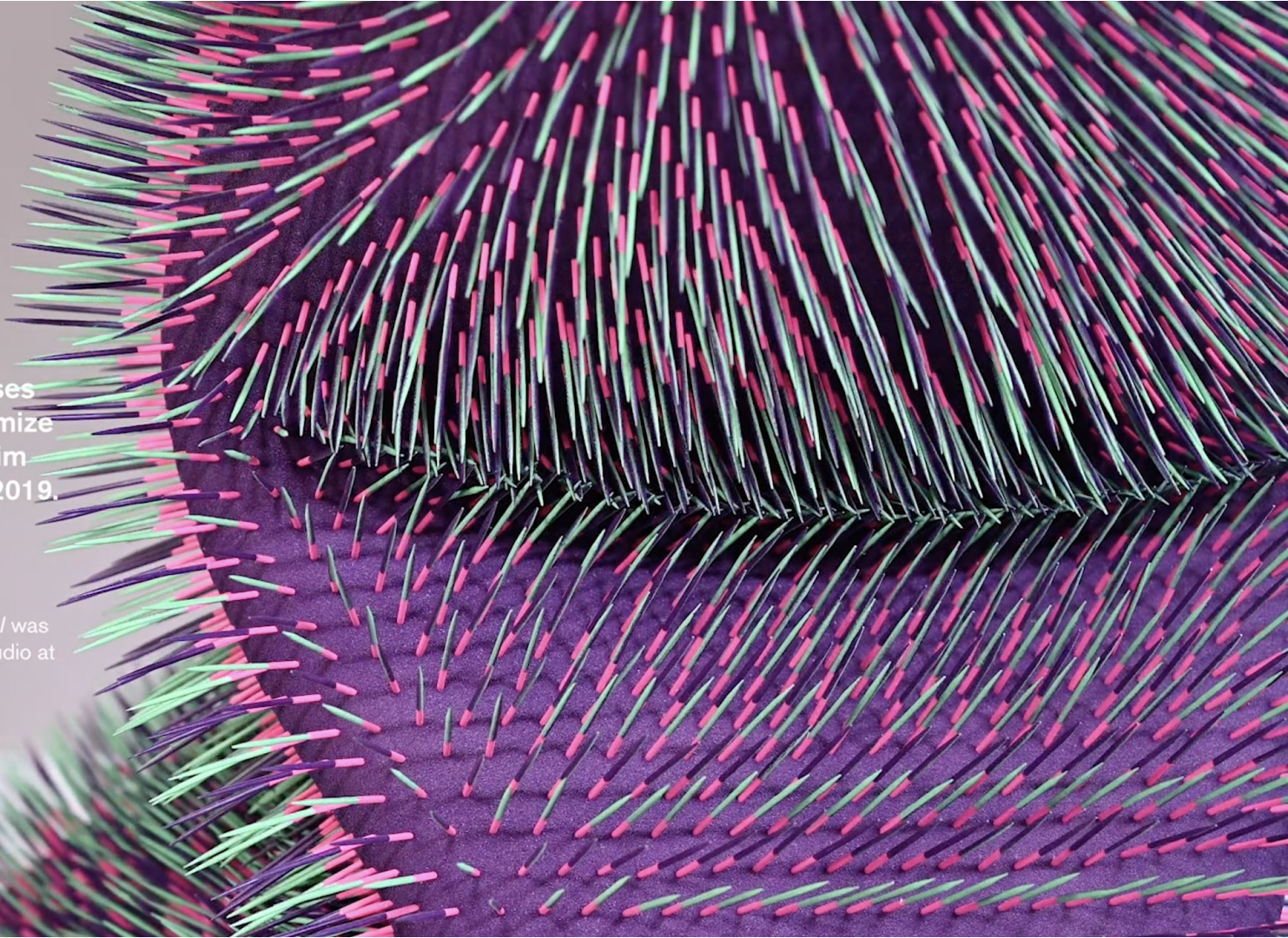
www.emanuelgollob.com

This iteration of *Doing Nothing with AI* was produced at *Design Investigations* studio at the *University of Applied Arts Vienna*.

supported by

vienna business agency

A service offered by the City of Vienna



Announcements

VDLM on Github

https://github.com/vdlm/meetups

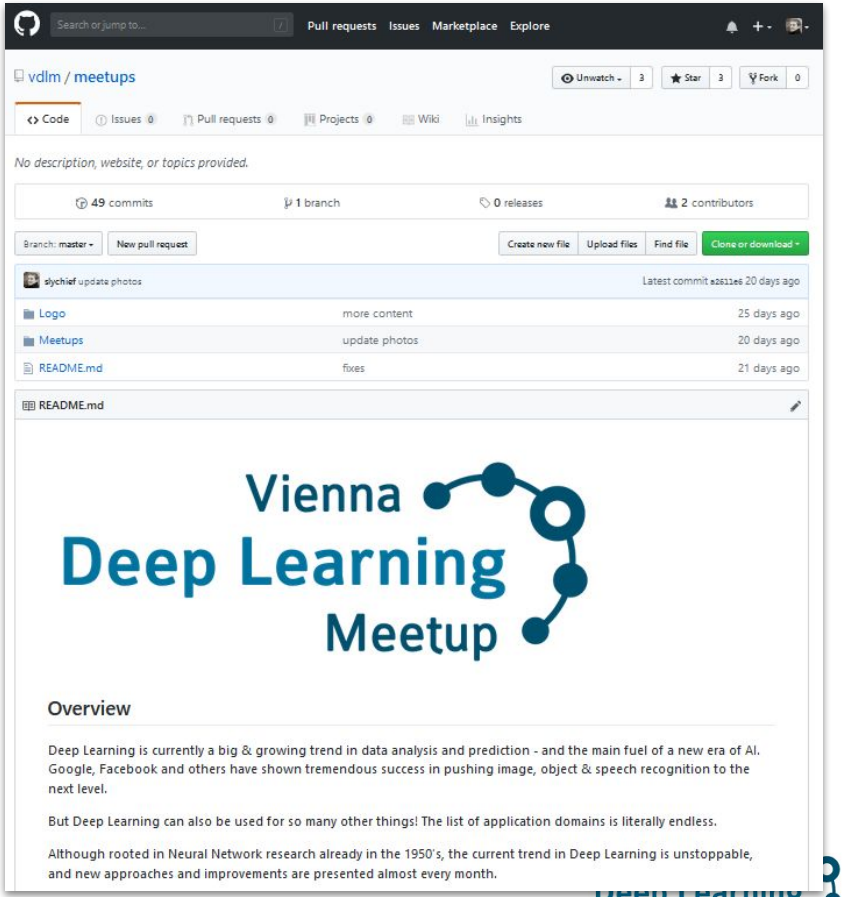
- all talks
- slides
- photos
- videos
- Wiki

Meetups

#	Date	Place	Topic	Link	Video	Meetup.com
1	2016-04-07	Sector 5	intro	more		link
2	2016-05-09	Sector 5		more		link
3	2016-06-06	Sector 5		more		link
4	2016-07-07	TU Wien		more		link
5	2016-09-22	Automic Software GmbH		more		link
6	2016-10-12	Sector 5		more		link
7	2016-12-01	Agentur Virtual Identity		more		link
8	2017-01-17	TU Wien Informatik		more		link
9	2017-02-21	bwin.party services (Austria) GmbH		more		link

Talks

Date	MU#	Speaker	Topic	Slides
2016-04-07	1	Thomas Lidy	An overview presentation of Deep Learning	pdf
2016-04-07	1	Jan Schlüter	History, Approaches, Applications	pdf
2016-05-09	2	Alex Champandard	Neural Networks for Image Synthesis	
2016-05-09	2	Gregor Mitscha-Baude	Recurrent Neural Networks	pdf
2016-06-06	3	Jan Schlüter	Open-source Deep Learning with Theano and Lasagne	pdf
2016-09-22	5	Josef Puchinger	Deep Learning & The Future of Automation	
2016-09-22	5	Christoph Körner	Going Deeper with GoogLeNet and CaffeJS	pdf



Deep Learning
Meetup

fastai learning group in Vienna

How to setup a deep learning library from matrix multiplication to SOTA!

For people with coding and deep learning experience (fast.ai v3 part 1).

Start in Oct. 2019. Course material will be soon online (fast.ai v3 **part 2**).

More information soon here:
https://github.com/MicPie/fastai-pytorch-course-vienna-v2

Topics for Today

Vienna Deep Learning Meetup

Introduction

Adversarial Machine Learning - An Introduction to Backdoor, Evasion and Inversion Attacks
Rudolf Mayer, Senior Researcher, SBA Research & Lector, TU Wien

Machine Learning Survey Results: The importance of reproducible ML pipeline elements
Camillo Pachmann, CEO - MLreef

<Break>

Using EEG and GAN to train robotic movements - *Emanuel Gollob, Designer & Media Artist*

Deep Learning for Electrical Biosignals and their Application in Medical Products
Franz Fürbass, Scientist in Biosignal Processing Group at Austrian Institute of Technology (AIT)

Hot Topics
EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks *Michael Pieler*
Adversial Learning for Fairness, Domain Adaptation and Unsupervised Learning *René Donner, contextflow*

Vienna Deep Learning Meetup

viesure Innovation Center

founded:

- January 1st 2019
- Vienna Insurance Group

focus on:

- cooperation with Wiener Städtische
- customer experience

We want you!

Build a team of:

- AI / ML Engineers all levels
- Data Scientists all levels

Contact:

- Dalibor Mitrovic:

dalibor.mitrovic@viesure.io

Work on:

- Computer Vision
- Natural Language Understanding
- next generation services for our customers

Hot Topics & Latest News

a short block at every meetup
to briefly present recent papers and news in Deep Learning

Send us contributions (tom.lidy@gmail.com)
or come with slides to do a short block yourself!

Vienna
Deep Learning
Meetup

EfficientNet

Adversarial Learning

EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks

Mingxing Tan [1] **Quoc V. Le** [1]

Abstract

Convolutional Neural Networks (ConvNets) are commonly developed at a fixed resource budget, and then scaled up for better accuracy if more resources are available. In this paper, we systematically study model scaling and identify that carefully balancing network depth, width, and resolution can lead to better performance. Based on this observation, we propose a new scaling method that uniformly scales all dimensions of depth/width/resolution using a simple yet highly effective *compound coefficient*. We demonstrate the effectiveness of this method on scaling up MobileNets and ResNet.

To go even further, we use neural architecture search to design a new baseline network and scale it up to obtain a family of models, called *EfficientNets*, which achieve much better accu-

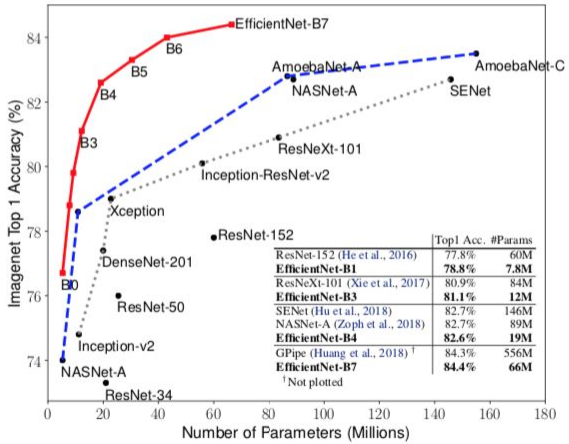
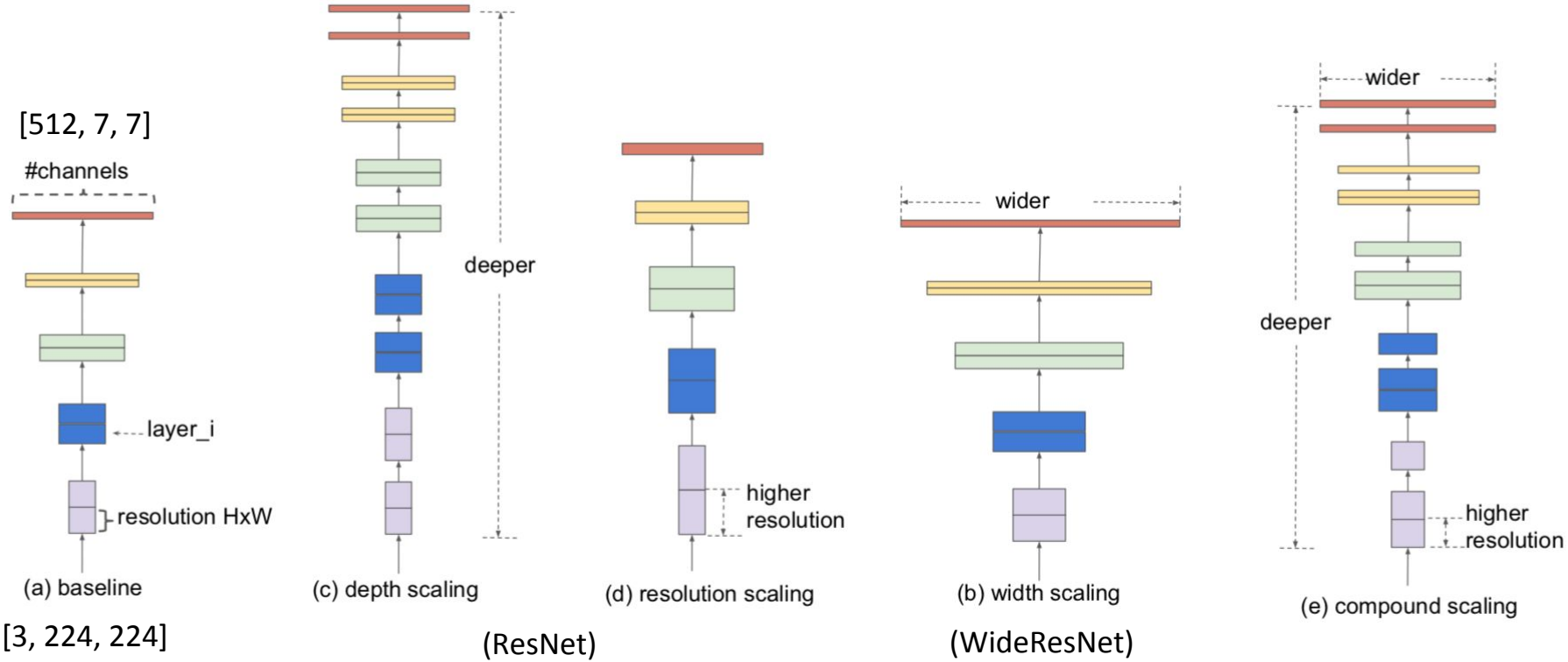
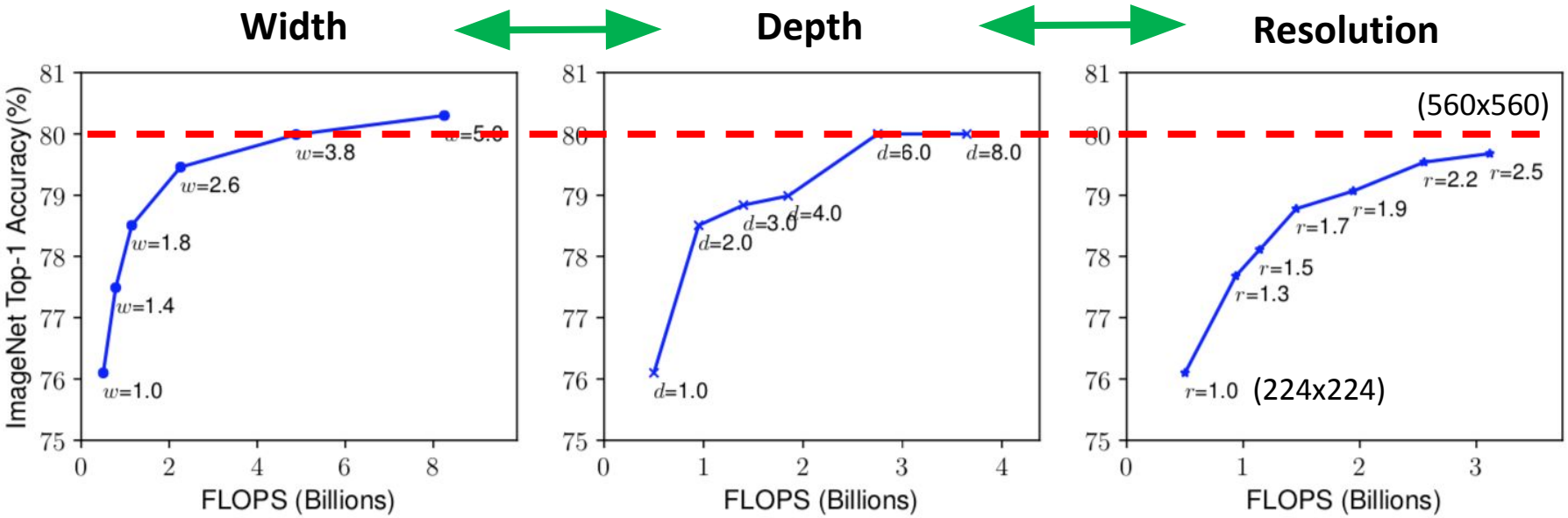


Figure 1. **Model Size vs. ImageNet Accuracy.** All numbers are for single-crop, single-model. Our EfficientNets significantly outperform other ConvNets. In particular, EfficientNet-B7 achieves

How to scale your baseline with more computational resources?

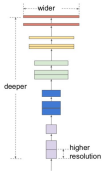


Scaling width, depth, and resolution?



Compound scaling and FLOP allocation

FLOPS in a CNN proportional to



depth

width^2

resolution^2

depth = α^{φ}

width = β^{φ}

resolution = γ^{φ}

Scale with ~~compound~~ coefficient φ

$$\alpha \cdot \beta^2 \cdot \gamma^2 \approx 2 \text{ (constraint)}$$

Scaling will approx. increase FLOPS by

$$(\alpha \cdot \beta^2 \cdot \gamma^2)^{\varphi} = 2^{\varphi}$$

Scaling of architectures

Works on ResNets & Co. but was optimized for new architecture:

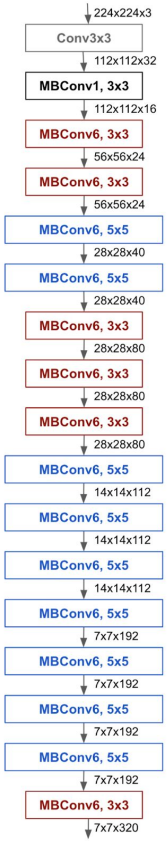
1. Neural architecture search optimizing accuracy and FLOPS to get EfficientNet-B0

2. Small grid search of α, β, γ

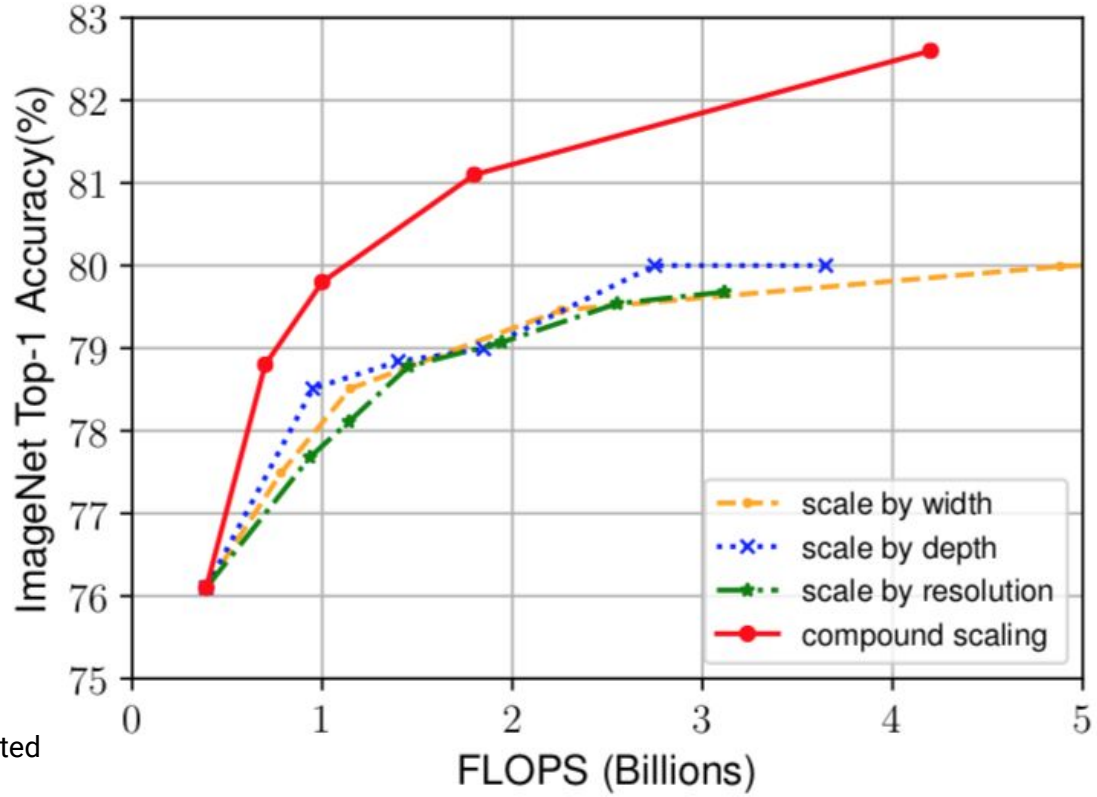
3. Fix α, β, γ and scale up baseline network with φ to obtain EfficientNet-B1 to B7

(Search for α, β, γ could be carried out directly on large networks but becomes very expensive.)

EfficientNet-B0 scaling

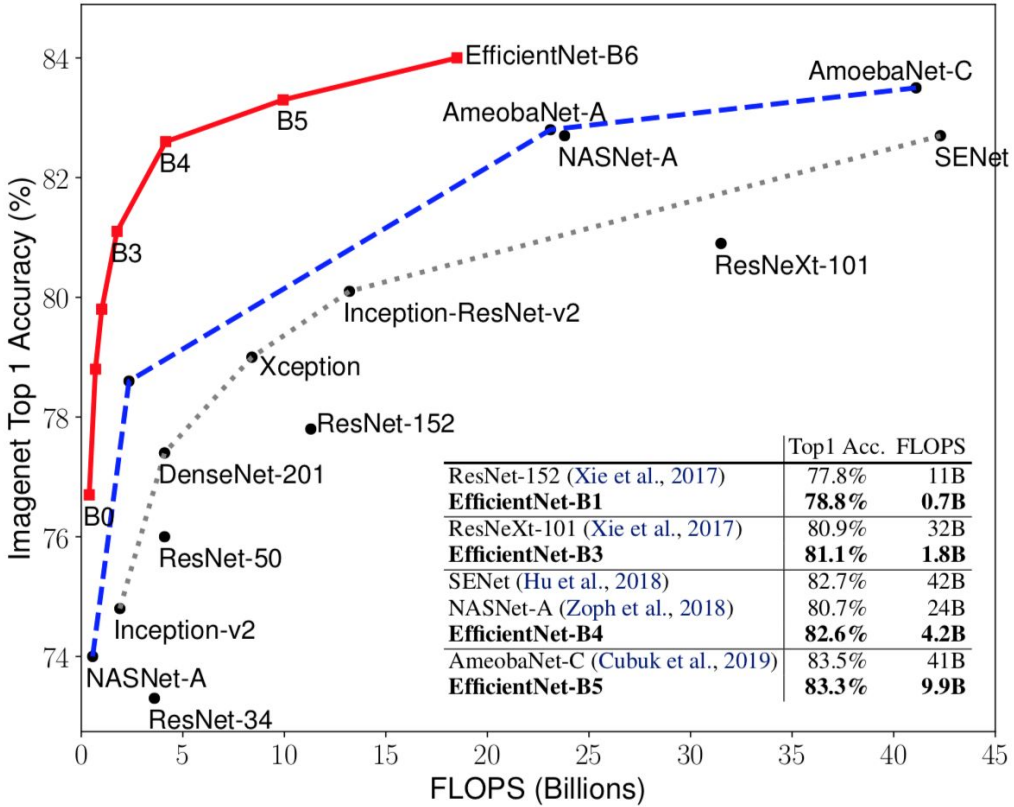


(MBConv = mobile inverted bottleneck convolution)

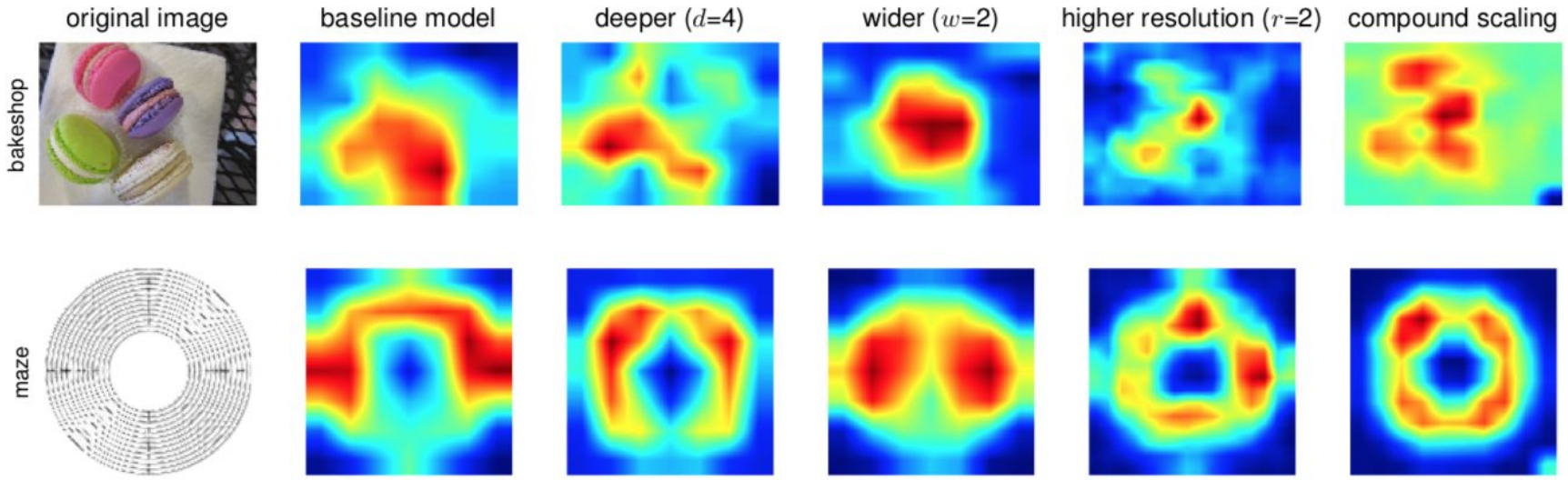


Results - EfficientNet-B7

- ImageNet SOTA
  84.4% top-1 / 97.1% top-5
- 8.4x smaller
- 6.1x faster on inference
- transfers well to other datasets



Results – Class activation maps (CAM)



Sources

(1) “EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks”, https://arxiv.org/abs/1905.11946

(2) EfficientNet Google AI blog post, https://ai.googleblog.com/2019/05/efficientnet-improving-accuracy-and.html

(3) “Searching for MobileNetV3”, https://arxiv.org/abs/1905.02244

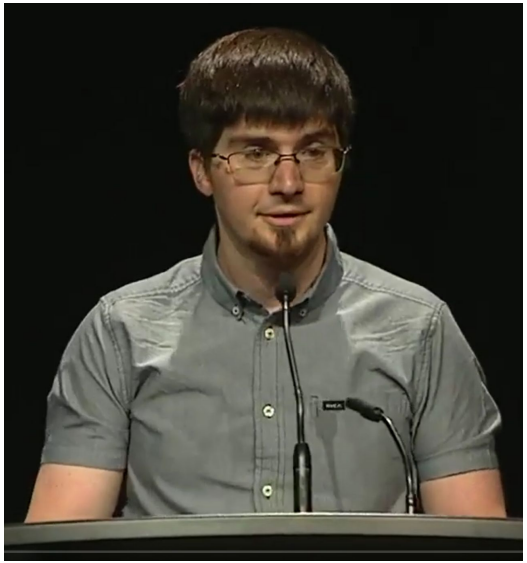
(4) “Squeeze-and-Excitation Networks”, https://arxiv.org/abs/1709.01507

(5) fast.ai forum thread, https://forums.fast.ai/t/efficientnet/46978

(6) Implementations, https://paperswithcode.com/paper/efficientnet-rethinking-model-scaling-for

Adversarial Learning

ICLR 2019 Invited Talks



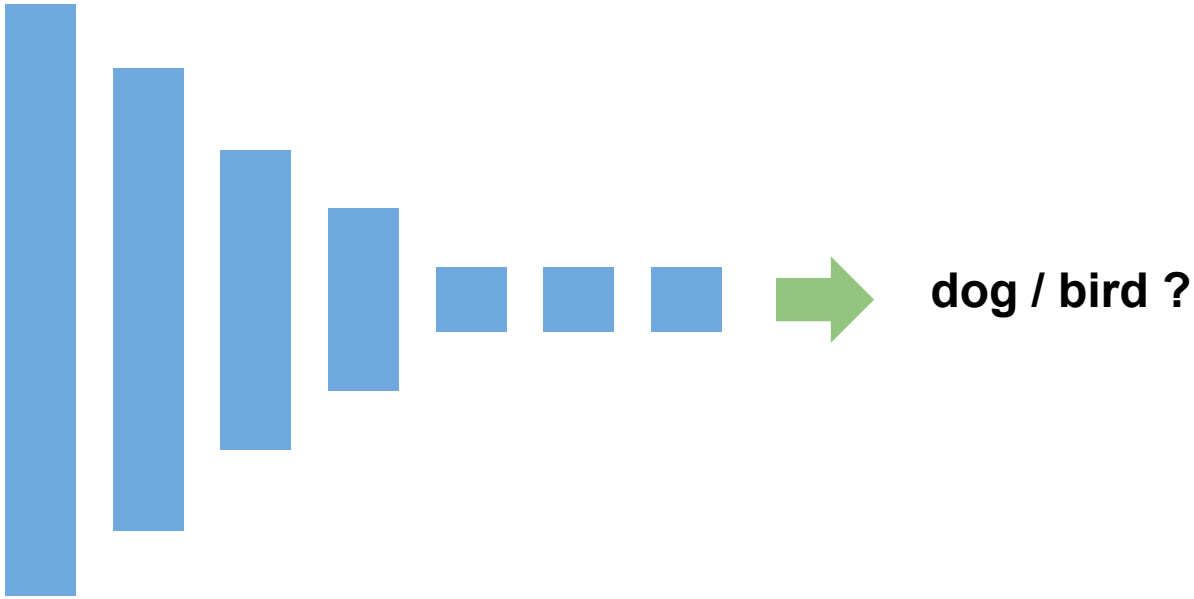
Ian Goodfellow
Adversarial Learning

https://www.youtube.com/watch?v=sucqskXRkss&t=1147s

Cynthia Dwark
Algorithmic Fairness

https://www.facebook.com/iclr.cc/videos/2261061694154984/

Simple Classification Problem



Adversarial Learning

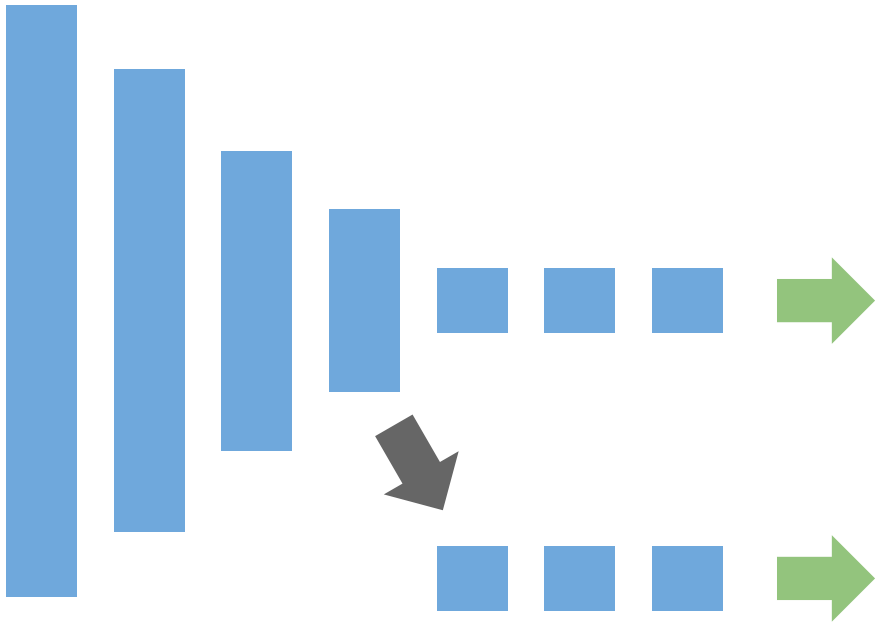
Adversarial Learning

Deep networks are lazy / clever!

dog / bird ?

Expensive camera / cheap camera ?

Adversarial Learning



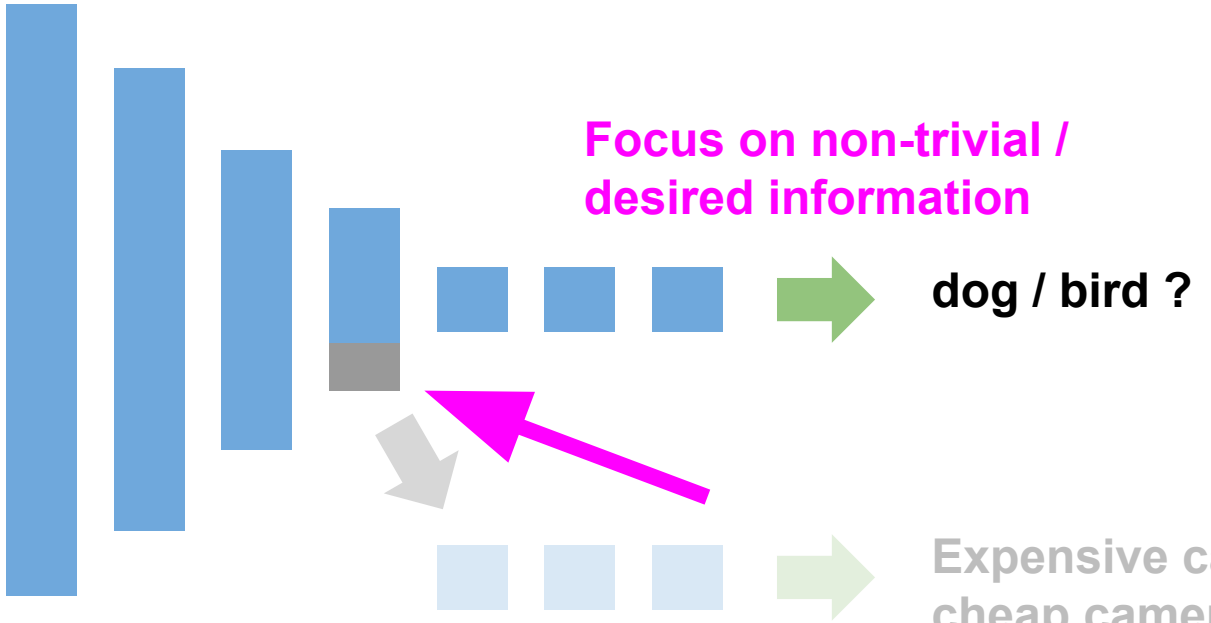
dog / bird ?

Try to be good at this task!

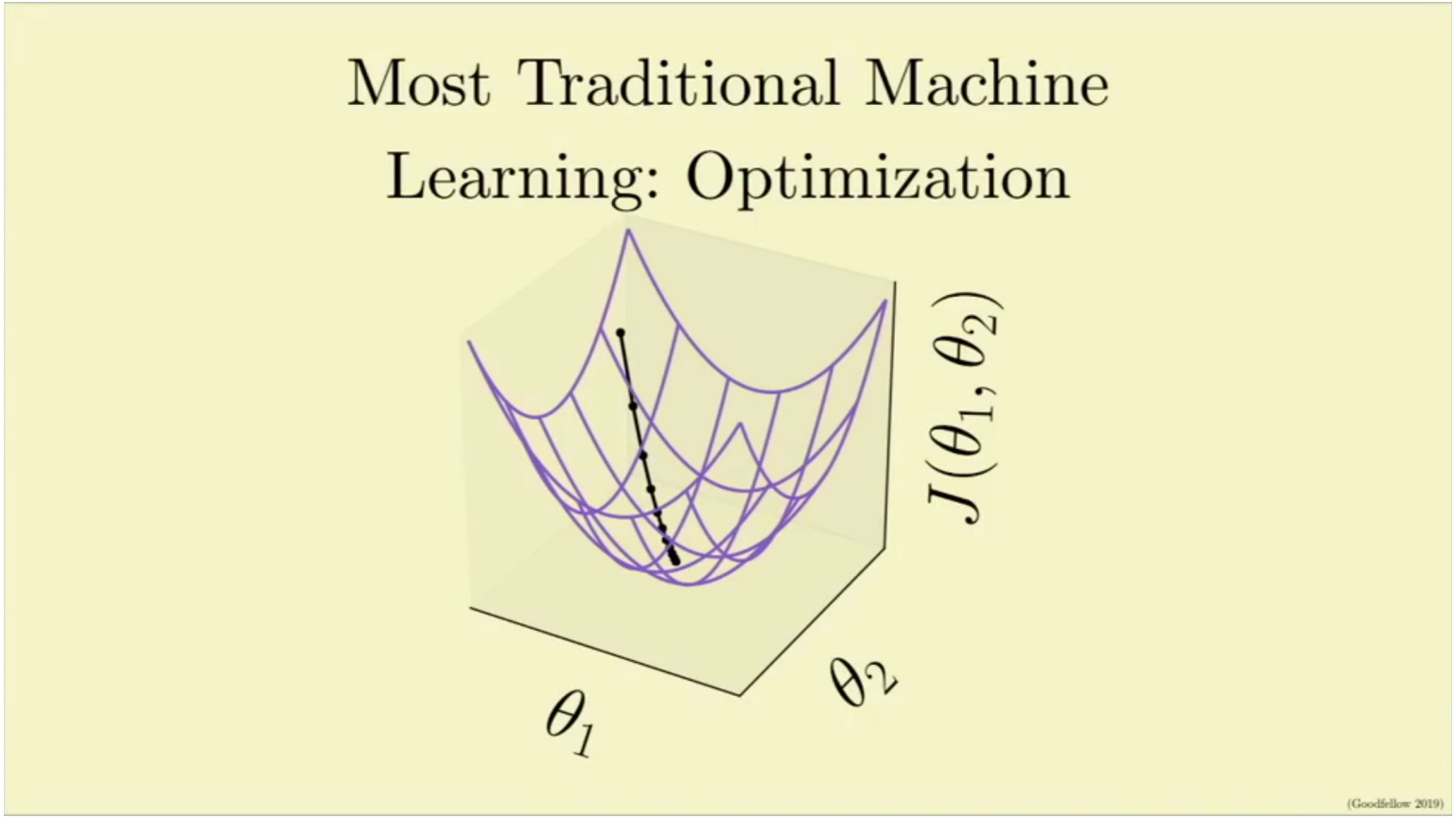
Expensive camera / cheap camera ?

Try to be bad at this task!

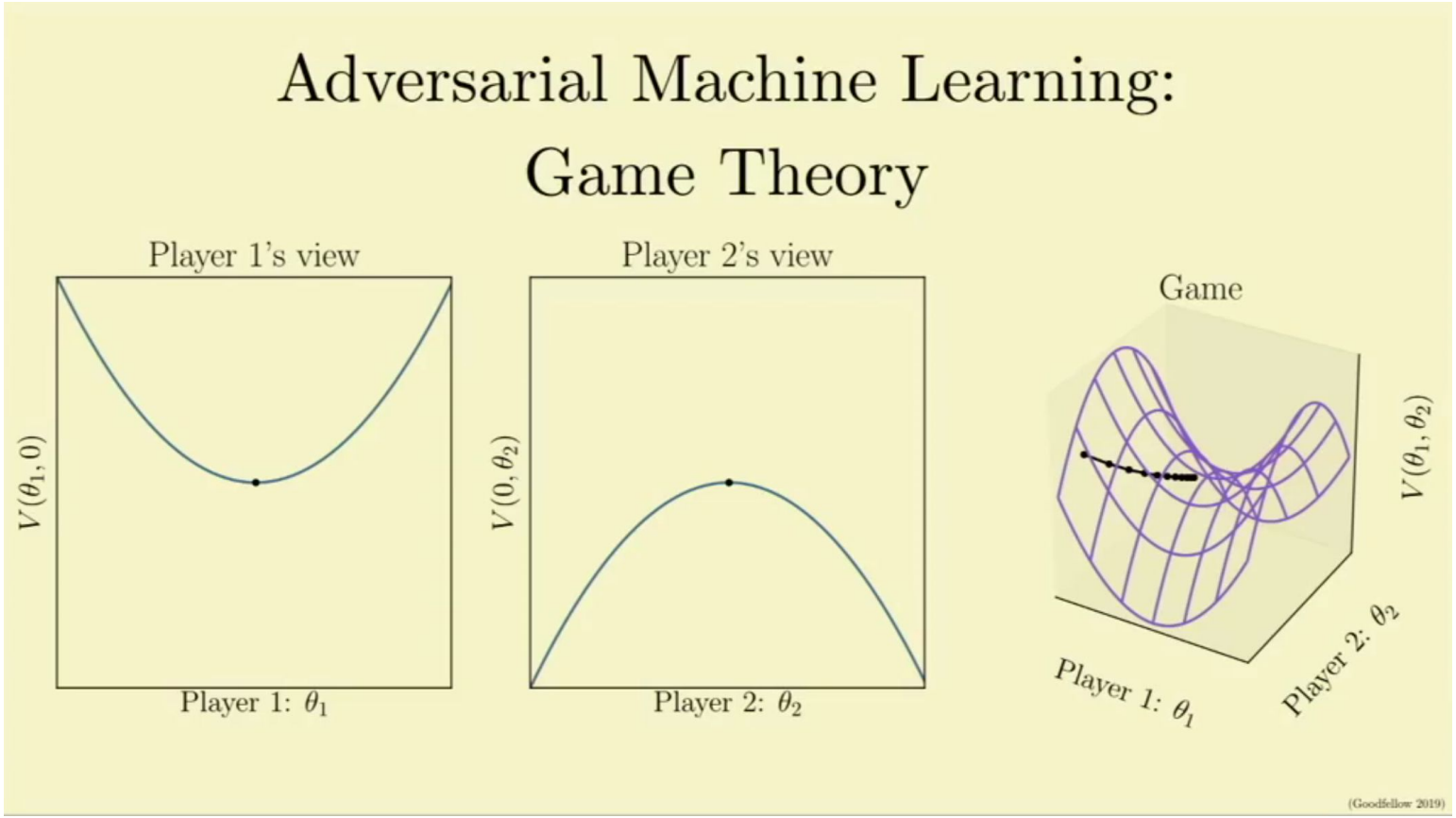
Adversarial Learning



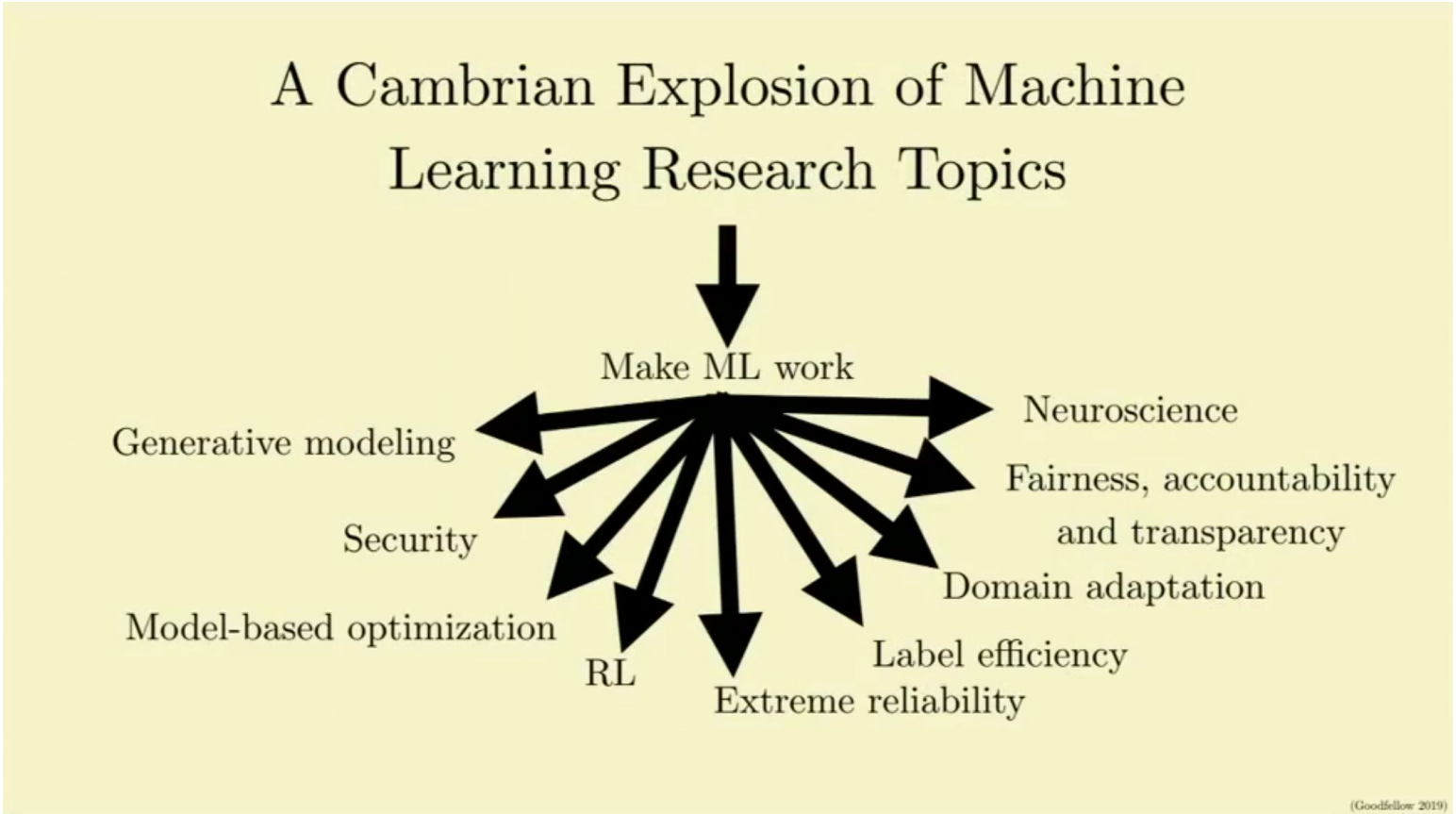
Goodfellow Talk



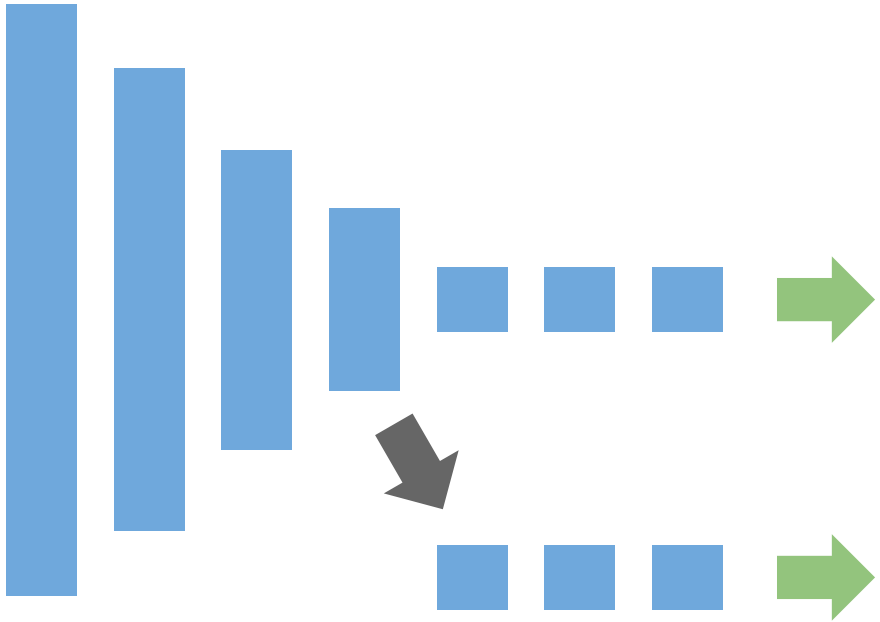
Goodfellow Talk



Goodfellow Talk



Fairness: Hiring interview



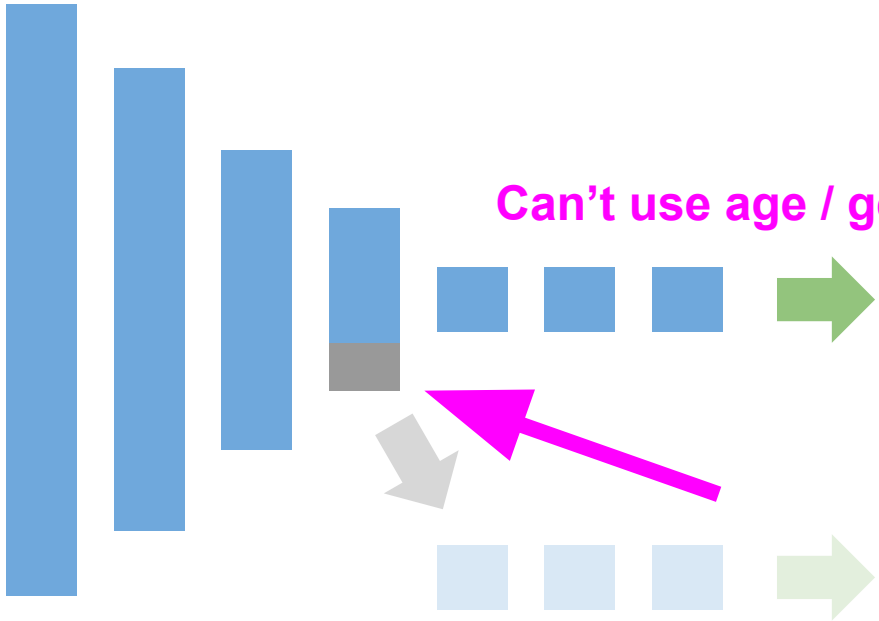
Try to be good at this task!

Will be a good new hire?

Predict age / gender / ethnicity

Try to be bad at this task!

Adversarial Learning



Can't use age / gender / ethnicity !

Will be a good new hire?

Predict age / gender / ethnicity

Try to be bad at this task!

Adversarial Learning

Adversarial Discriminative Domain Adaptation

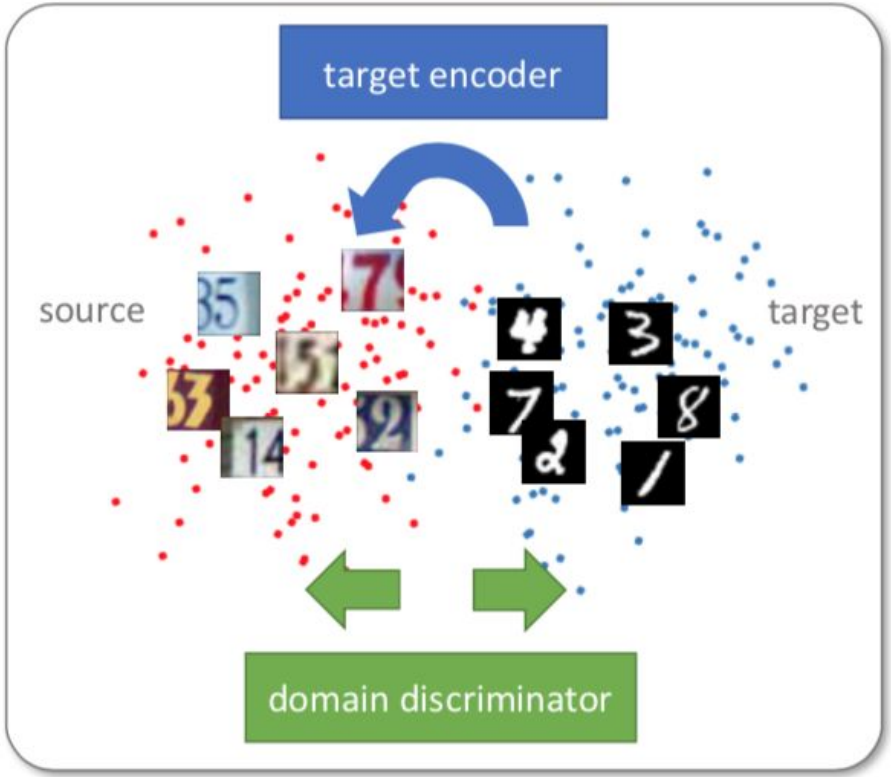
Eric Tzeng
University of California, Berkeley
etzeng@eecs.berkeley.edu

Judy Hoffman
Stanford University
jhoffman@cs.stanford.edu

Kate Saenko
Boston University
saenko@bu.edu

Trevor Darrell
University of California, Berkeley
trevor@eecs.berkeley.edu

Adversarial Learning



Adversarial Learning

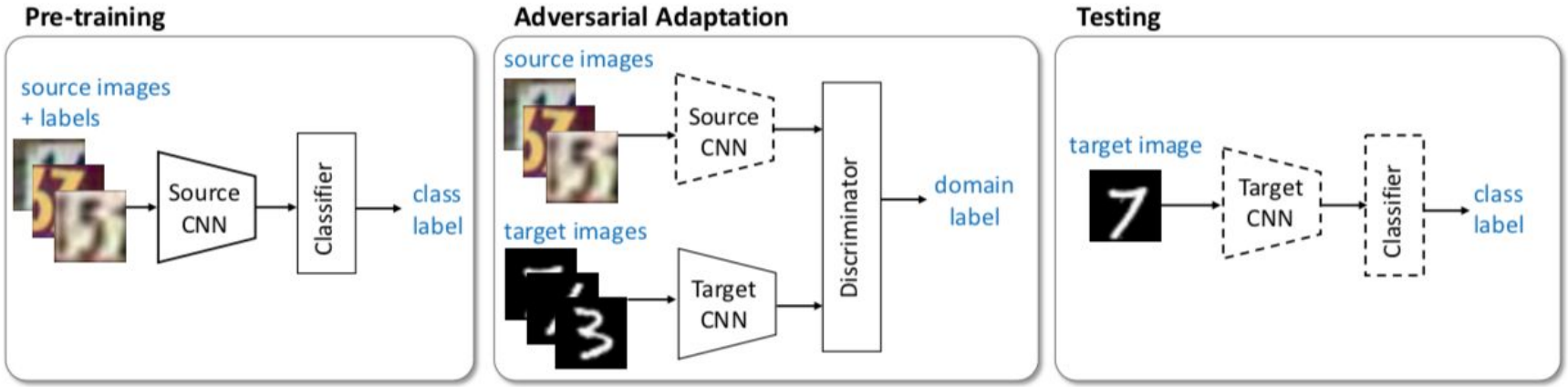


Figure 3: An overview of our proposed Adversarial Discriminative Domain Adaptation (ADDA) approach. We first pre-train a source encoder CNN using labeled source image examples. Next, we perform adversarial adaptation by learning a target encoder CNN such that a discriminator that sees encoded source and target examples cannot reliably predict their domain label. During testing, target images are mapped with the target encoder to the shared feature space and classified by the source classifier. Dashed lines indicate fixed network parameters.

Deep networks are lazy / clever and learn shortcuts!

Position in the image?

Expensive camera / cheap camera ?

Dataset characteristics?

Dataset imbalance ?

Adversarial learning allows to:
introduce expert knowledge / design decisions on which information to delete!

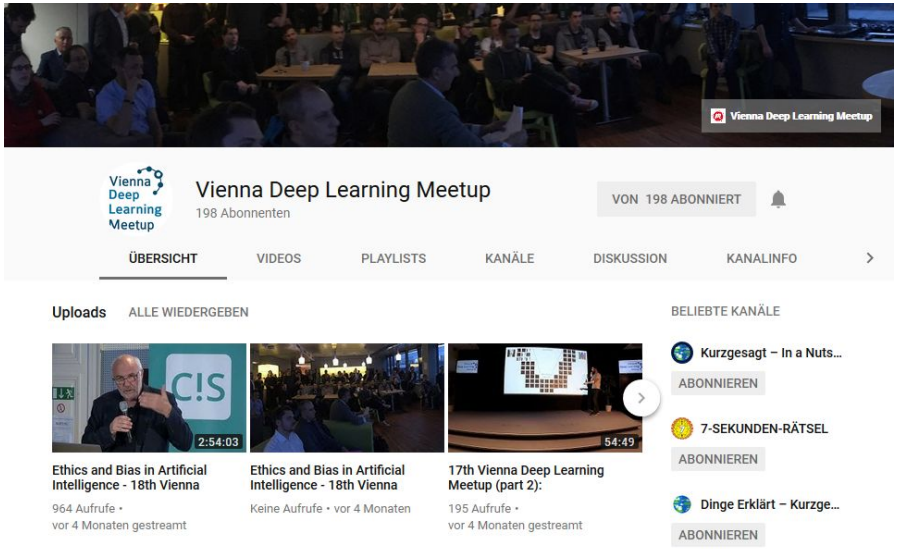
Adversarial Learning

Next Meetup:
September

www.meetup.com/Vienna-Deep-Learning-Meetup

Vienna
Deep Learning
Meetup

VDLM Youtube Channel



https://www.youtube.com/ViennaDeepLearningMeetup

Vienna Deep Learning Meetup