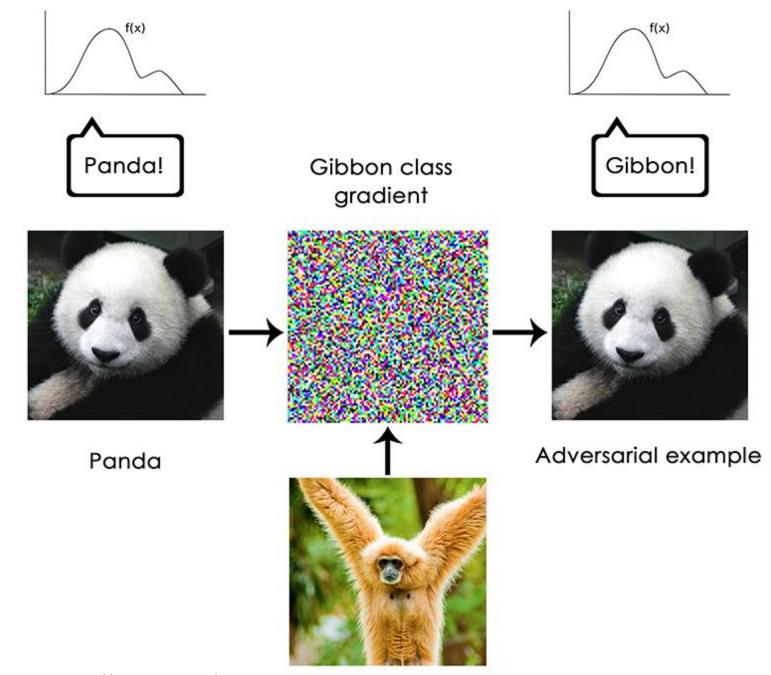


© HarperCollins / Clare Ske



Francois Chollet - https://blog.keras.io/the-limitations-of-deep-learning.html

3rd November 2017



Technology

Single pixel change fools Al programs

Tiny changes can make image recognition systems think a school bus is an ostrich, find scientists.

() 3 hours ago | Technology

Algorithm learns to recognise natural beauty

Artificial intelligence fools security

Al used to detect breast cancer





Technology

Single pixel change fools Al programs

Tiny changes can make image recognition systems think a school bus is an ostrich, find scientists.

() 3 hours ago | Technology

Algorithm learns to recognise natural beauty

Artificial intelligence fools security

Al used to detect breast cancer



Yes, it's a brain image

: (





Automobile(Dog)

10

Automobile

(Airplane)

Frog(Truck)

Horse

(Automobile)



Cat(Dog)

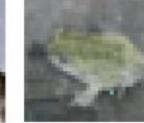
Dog(Ship)



Airplane(Dog)







Deer(Dog)

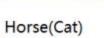
Frog(Dog)

a)

Dog(Cat)

Frog(Truck)





Ship(Truck)



Dog(Horse) Ship(Truck)

Su et al., One pixel attack for fooling deep neural networks <u>https://arxiv.org/abs/1710.08864</u>

SYNTHESIZING ROBUST ADVERSARIAL EXAMPLES

https://arxiv.org/pdf/1707.07397.pdf

Anish Athalye^{*1,2}, Logan Engstrom^{*1,2}, Andrew Ilyas^{*1,2}, Kevin Kwok² ¹Massachusetts Institute of Technology, ²LabSix {aathalye,engstrom,ailyas}@mit.edu, kevin@labsix.org





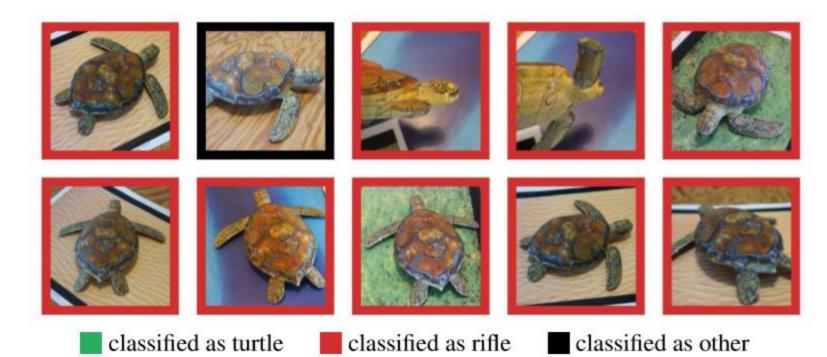




classified as turtle

classified as rifle

classified as other



Fooling Neural Networks in the Real World labsix





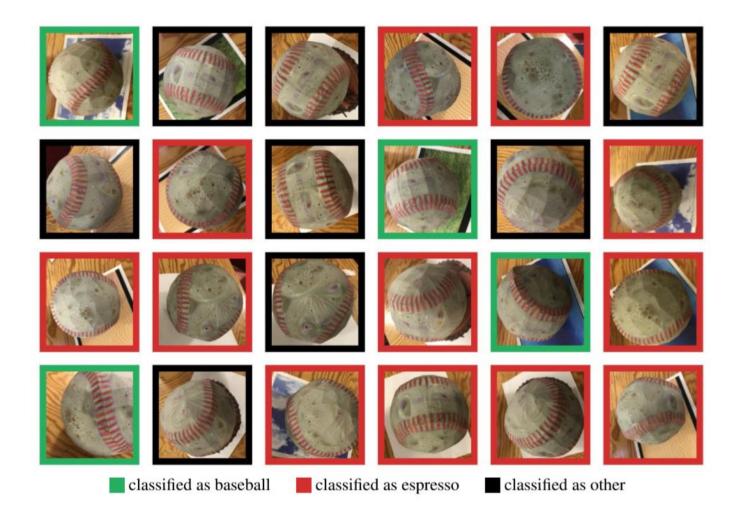


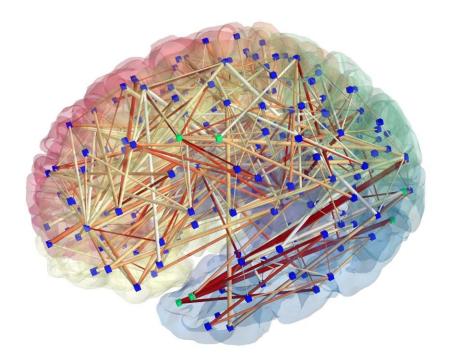


classified as baseball

classified as espresso

classified as other

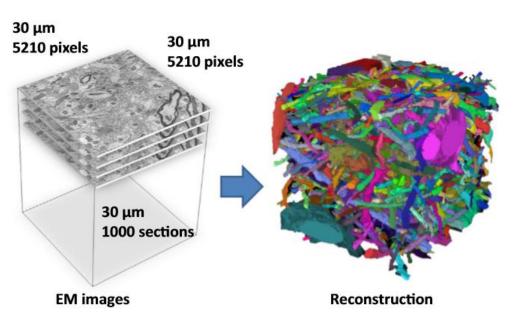




Connectomics: Neural nets for neural nets

[Patric Hagmann]

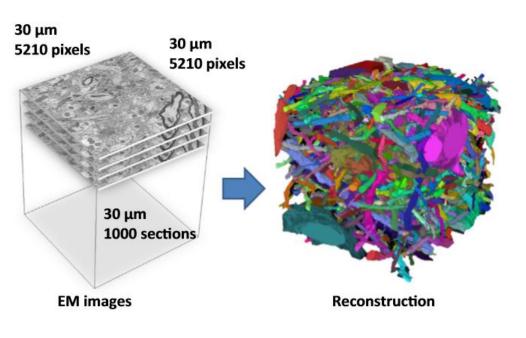
Vision for understanding the brain



1mm cubed of brain Image at 5-30 nanometers

How much data?

Vision for understanding the brain

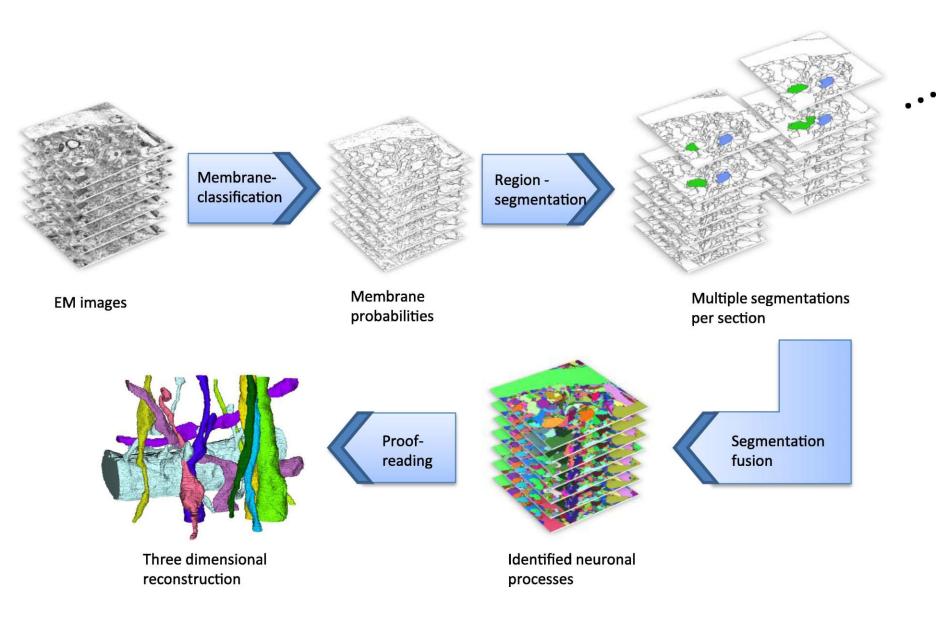


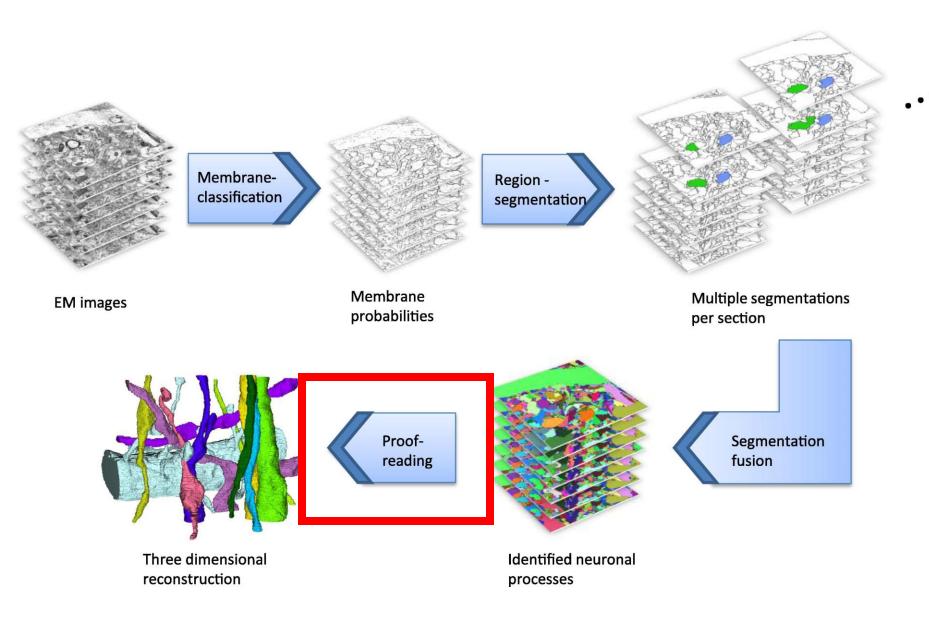
1mm cubed of brain Image at 5-30 nanometers

How much data?

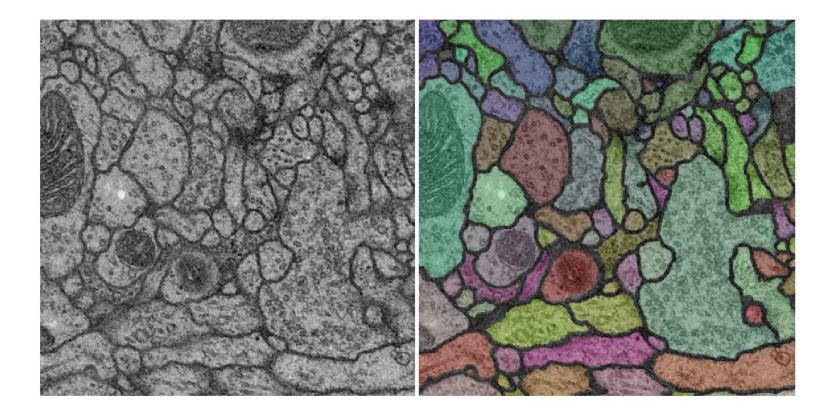
1 Petabyte – 1,000,000,000,000,000

~ All photos uploaded to Facebook per day

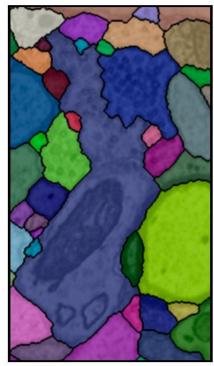


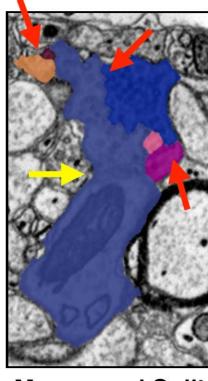


Vision for understanding the brain





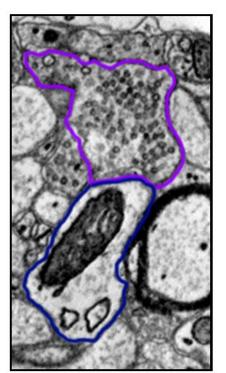




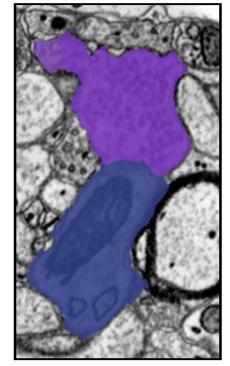
Initial Segmentation

Errors

Merge- and Split

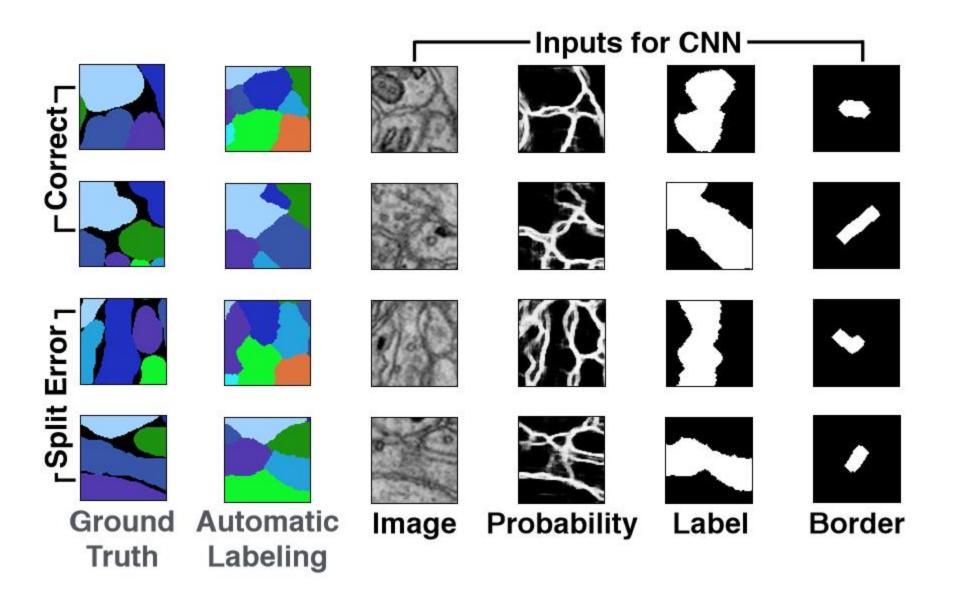


Correct **Borders**



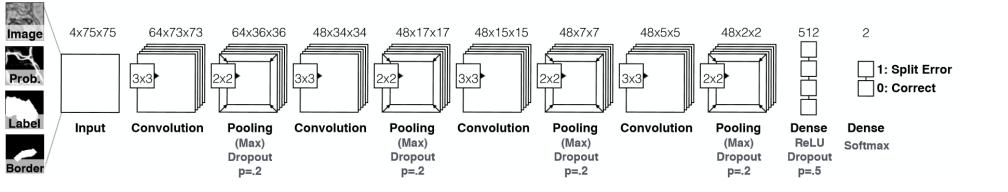
Fixed Segmentation

[Haehn et al.]

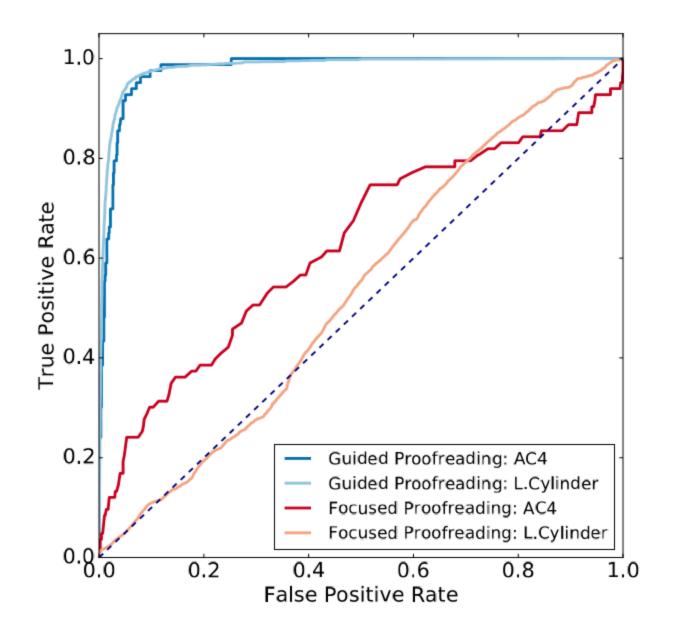


[Haehn et al.]

Network Architecture

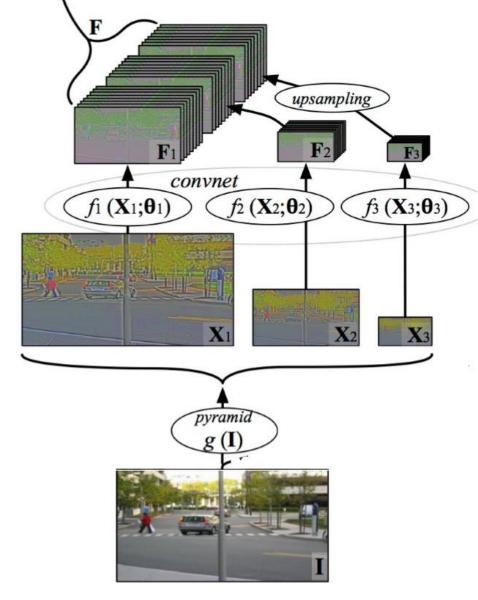


[Haehn et al.]



[Haehn et al.]

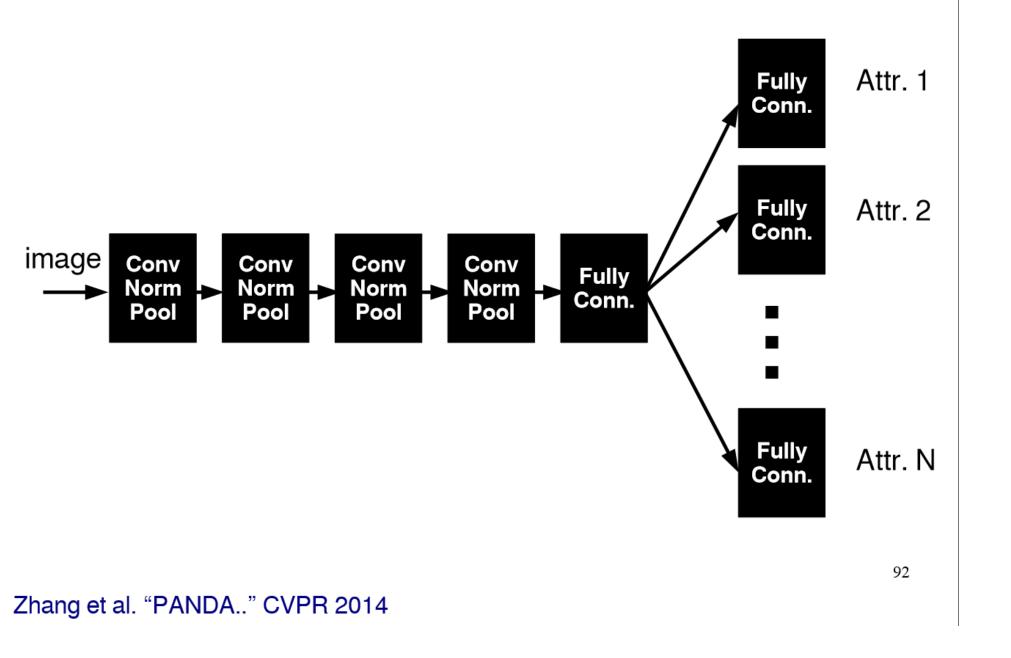
Fancier Architectures: Multi-Scale



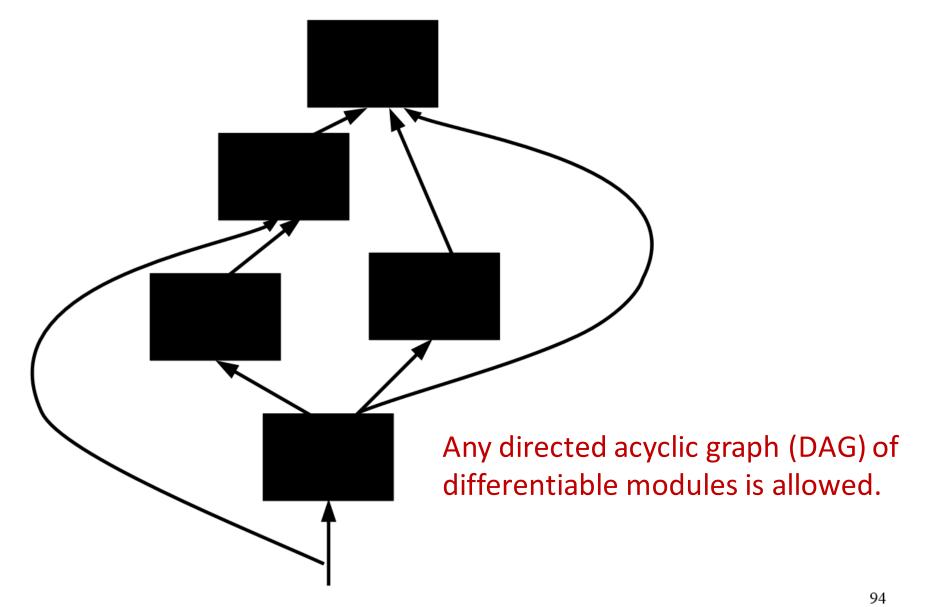
90

Farabet et al. "Learning hierarchical features for scene labeling" PAMI 2013

Fancier Architectures: Multi-Task

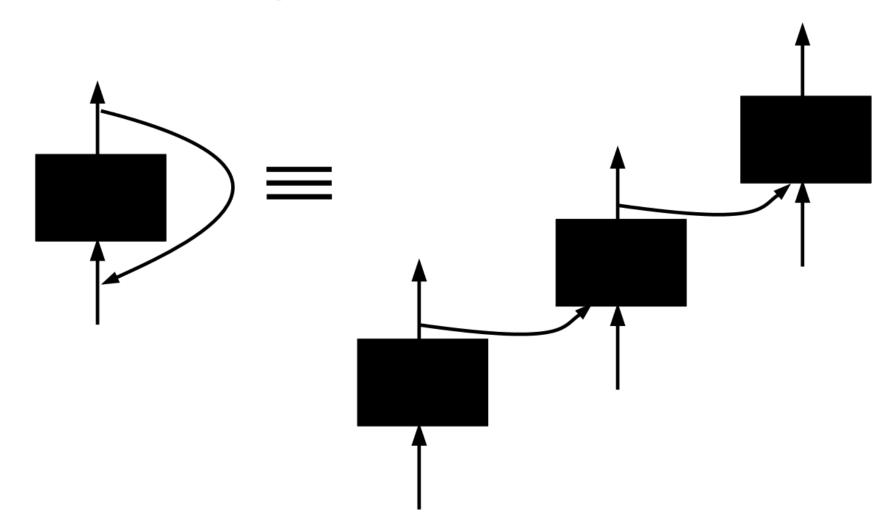


Fancier Architectures: Generic DAG



Fancier Architectures: Generic DAG

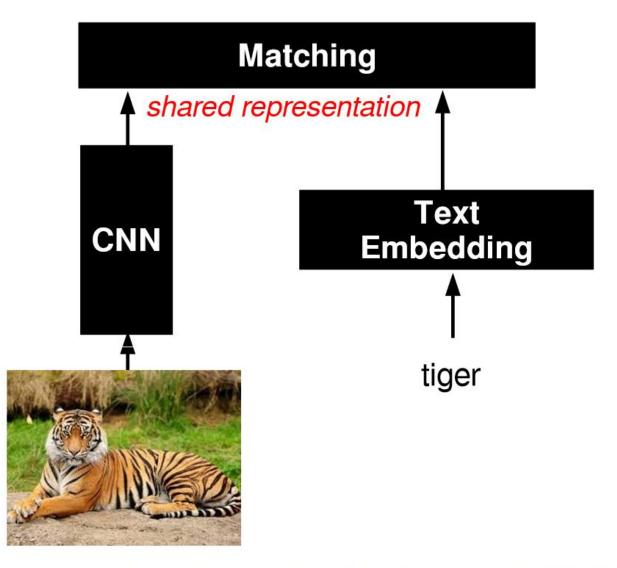
If there are cycles (RNN), one needs to un-roll it.



Pinheiro, Collobert "Recurrent CNN for scene labeling" ICML 2014 Graves "Offline Arabic handwriting recognition.." Springer 2012 95

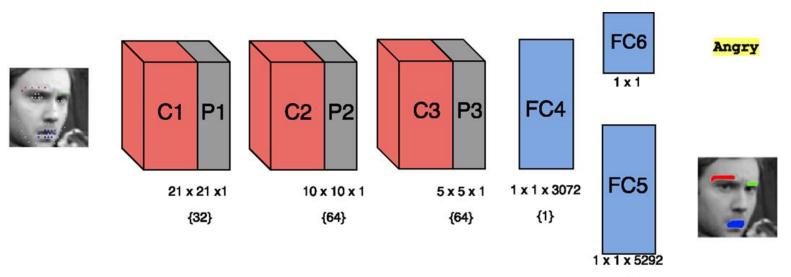
What about learning across 'domains'?

Fancier Architectures: Multi-Modal



91

Frome et al. "Devise: a deep visual semantic embedding model" NIPS 2013

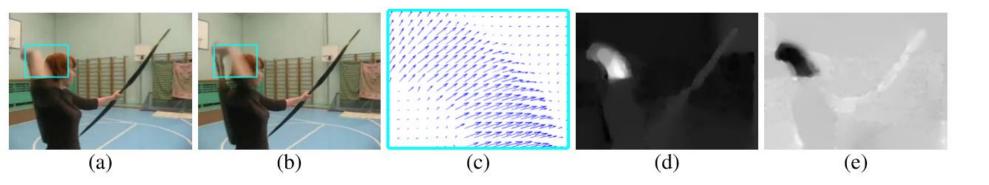


{1}

Two-stream networks – *action recognition*

		Spatial stream ConvNet							
	single frame	conv1 7x7x96 stride 2 norm. pool 2x2	conv2 5x5x256 stride 2 norm. pool 2x2	conv3 3x3x512 stride 1	conv4 3x3x512 stride 1	conv5 3x3x512 stride 1 pool 2x2	full6 4096 dropout	full7 2048 dropout	softmax
	Temporal stream ConvNet								
input video	multi-frame	conv1 7x7x96 stride 2 norm. pool 2x2	conv2 5x5x256 stride 2 pool 2x2	conv3 3x3x512 stride 1	conv4 3x3x512 stride 1	conv5 3x3x512 stride 1 pool 2x2	full6 4096 dropout	full7 2048 dropout	softmax

[Simonyan et al. 2014]



[Simonyan et al. 2014]

Learning Deep Representations For Ground-to-Aerial Geolocalization

Tsung-Yi Lin, Yin Cui, Serge Belongie, James Hays

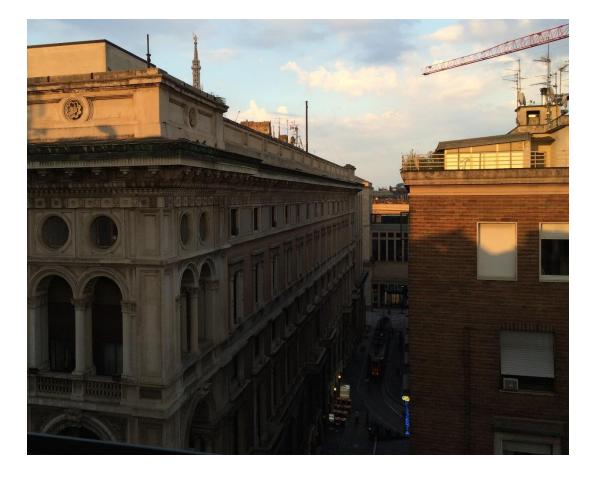




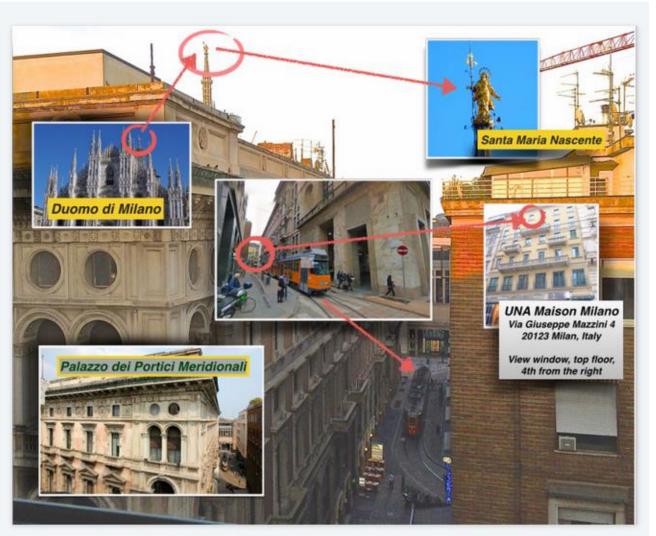
CVPR 2015

View From Your Window Contest

June 9, 2010 – Feb. 4, 2015



Where was the photo taken?



Ans: Milano, Italy

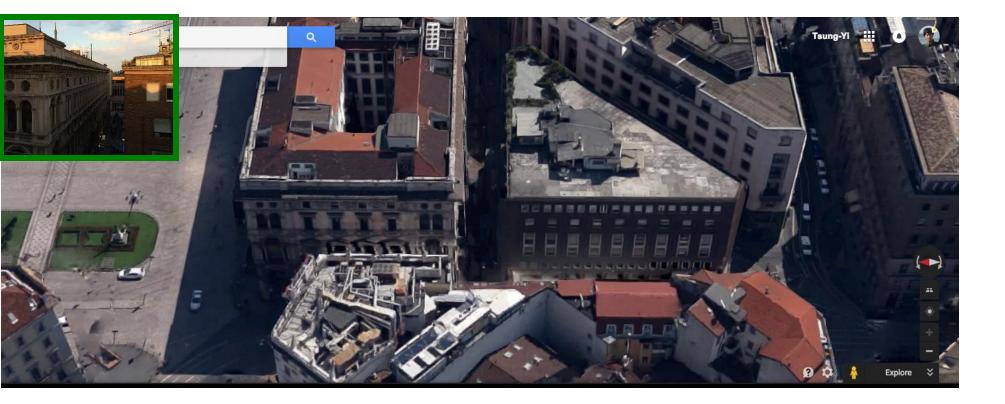
To Geolocalize a Photo

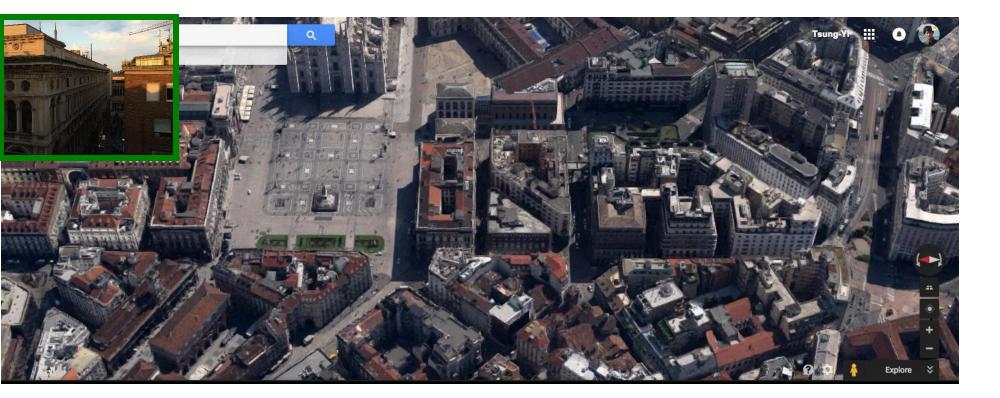


• One can capture every corner on the earth



To Geolocalize a Photo







How To Match Ground-to-Aerial?

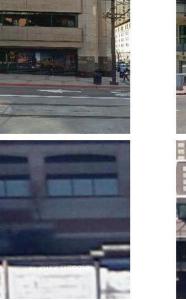


Shan et al., Accurate Geo-registration by Ground-to-Aerial Image Matching, 3DV'14 Bansal et al., Ultra-wide baseline façade matching for geo-localization, ECCV workshop'12

Are these the same location?

Ground

Aerial











Are these the same location?

Ground



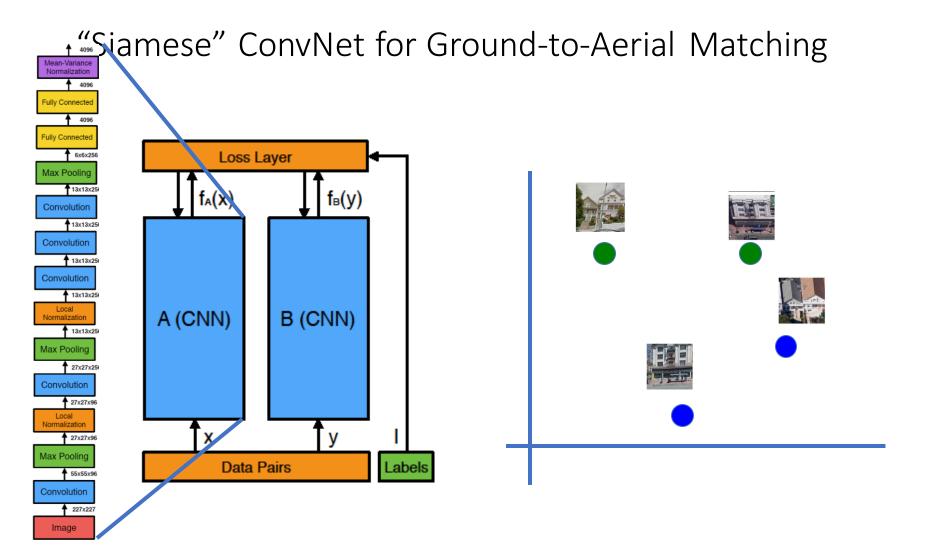


Cross-view Pairs

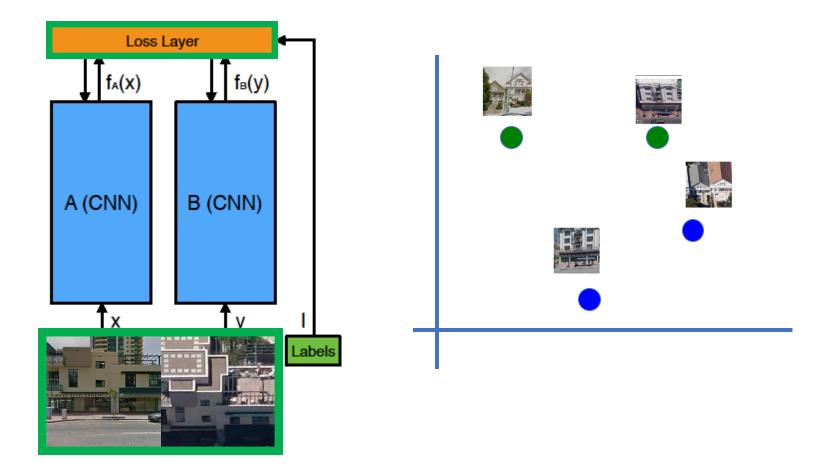




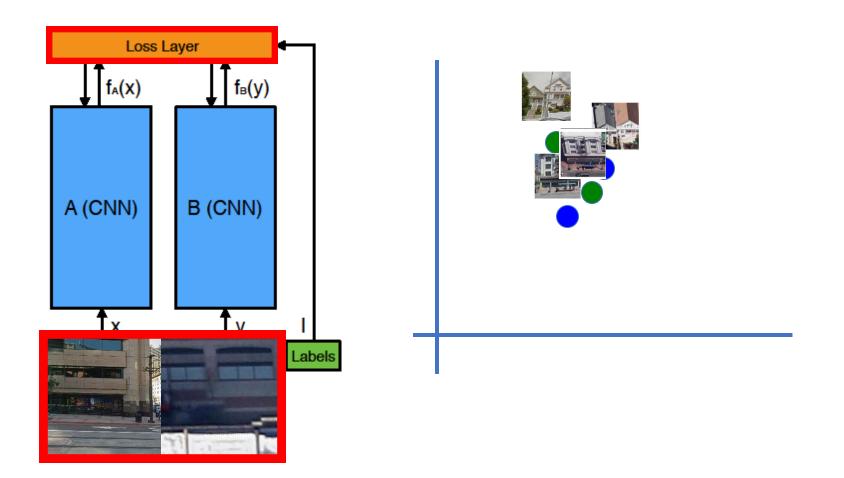
Aerial

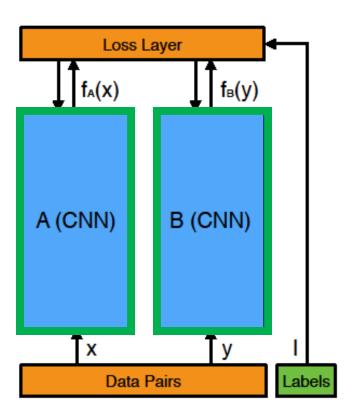


"Siamese" ConvNet for Ground-to-Aerial Matching



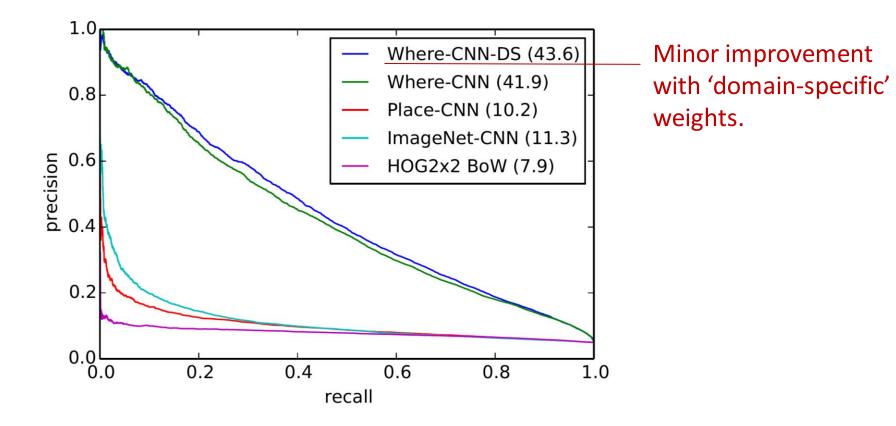
"Siamese" ConvNet for Ground-to-Aerial Matching





For ground-aerial image pairs, should A, B networks share the same weights?

Quantitative Evaluation



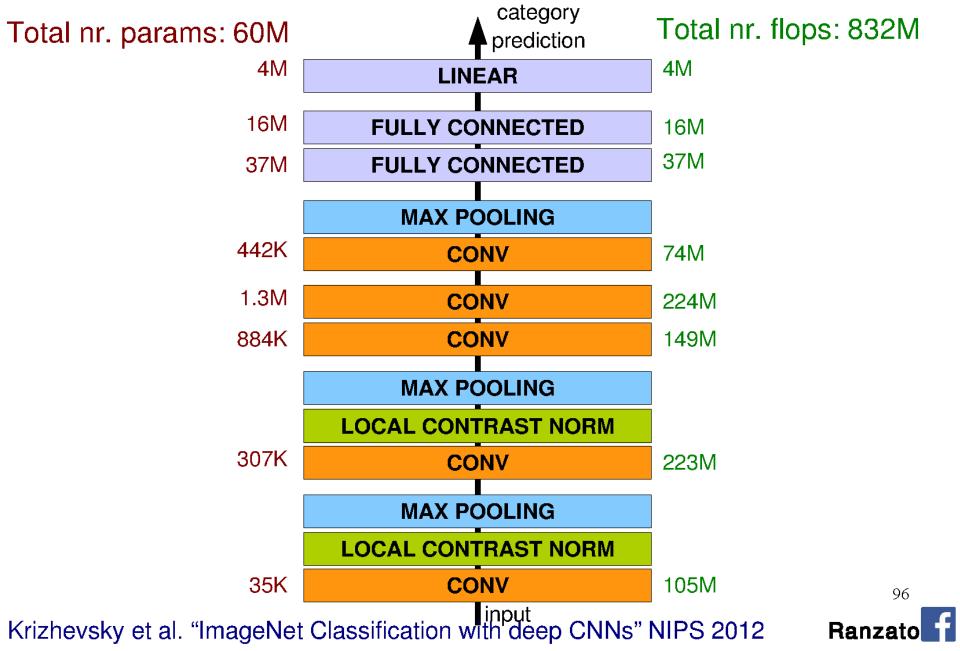
Big space of designs!

But we still don't even know how many layers we need.





Architecture for Classification



Beyond AlexNet

VERY DEEP CONVOLUTIONAL NETWORKS FOR LARGE-SCALE IMAGE RECOGNITION

Karen Simonyan & Andrew Zisserman 2015

These are the pre-trained "VGG" networks that you use in project 5

		ConvNet C	onfiguration		
А	A-LRN	В	С	D	E
11 weight	11 weight	13 weight	16 weight	16 weight	19 weight
layers	layers	layers	layers	layers	layers
	input (224×224 RGB image)				
conv3-64	conv3-64	conv3-64	conv3-64	conv3-64	conv3-64
	LRN	conv3-64	conv3-64	conv3-64	conv3-64
	•		pool	•	•
conv3-128	conv3-128	conv3-128	conv3-128	conv3-128	conv3-128
		conv3-128	conv3-128	conv3-128	conv3-128
	-		pool		
conv3-256	conv3-256	conv3-256	conv3-256	conv3-256	conv3-256
conv3-256	conv3-256	conv3-256	conv3-256	conv3-256	conv3-256
			conv1-256	conv3-256	conv3-256
					conv3-256
			pool		
conv3-512	conv3-512	conv3-512	conv3-512	conv3-512	conv3-512
conv3-512	conv3-512	conv3-512	conv3-512	conv3-512	conv3-512
			conv1-512	conv3-512	conv3-512
					conv3-512
			pool		
conv3-512	conv3-512	conv3-512	conv3-512	conv3-512	conv3-512
conv3-512	conv3-512	conv3-512	conv3-512	conv3-512	conv3-512
			conv1-512	conv3-512	conv3-512
					conv3-512
			pool		
			4096		
			4096		
			1000		
		soft	-max		

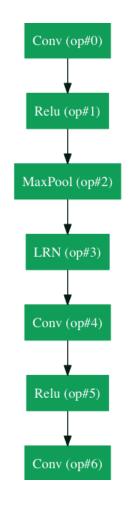
Table 2.	Number of	parameters	(in millions)
10010 2.	TIMMOUT OF	parameters	(III IIIIIIOIIS).

		1				
Network		A,A-LRN	В	С	D	E
Number o	f parameters	133	133	134	138	144

ConvNet config. (Table 1)	smallest image side		top-1 val. error (%)	top-5 val. error (%)
	train (S)	test (Q)		
В	256	224,256,288	28.2	9.6
	256	224,256,288	27.7	9.2
C	384	352,384,416	27.8	9.2
	[256; 512]	256,384,512	26.3	8.2
	256	224,256,288	26.6	8.6
D	384	352,384,416	26.5	8.6
	[256; 512]	256,384,512	24.8	7.5
	256	224,256,288	26.9	8.7
E	384	352,384,416	26.7	8.6
	[256; 512]	256,384,512	24.8	7.5

Table 4: ConvNet performance at multiple test scales.

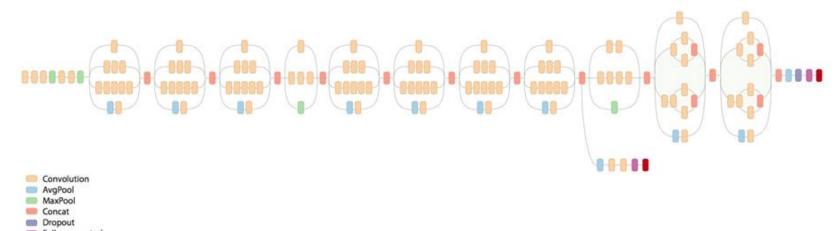
Google LeNet (2014)



22 layers

6.67% error ImageNet top 5

Inception!

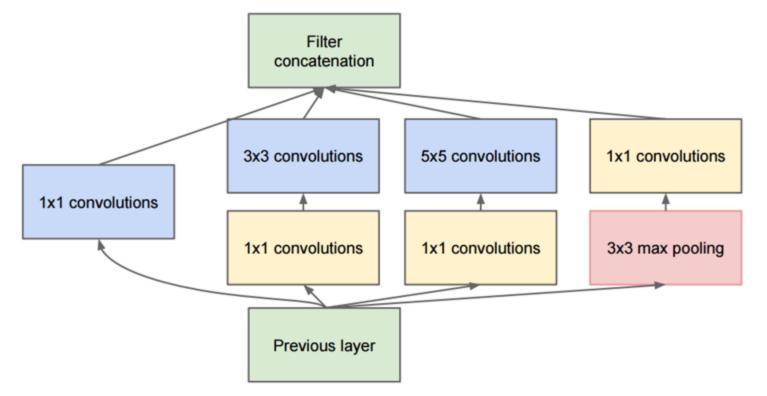


E Fully connected

Softmax

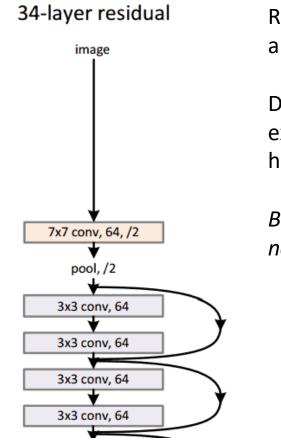
Another view of GoogLeNet's architecture.

Parallel layers



Full Inception module

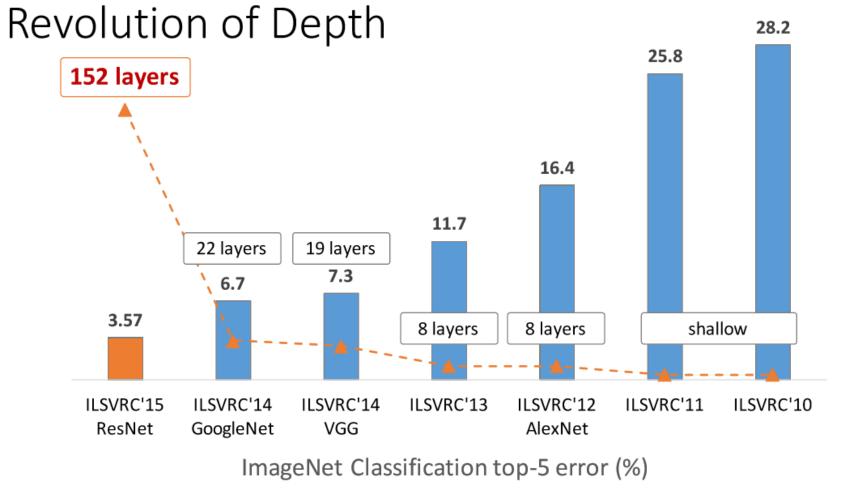
ResNet (He et al., 2015)



ResNet won ILSVRC 2015 with a top-5 error rate of 3.6%

Depending on their skill and expertise, humans generally hover around a 5-10% error.

But the task is arguably not well defined.



Revolution of Depth AlexNet, 8 layers VGG, 19 layers ResNet, 152 layers (ILSVRC 2015) (ILSVRC 2012) (ILSVRC 2014)

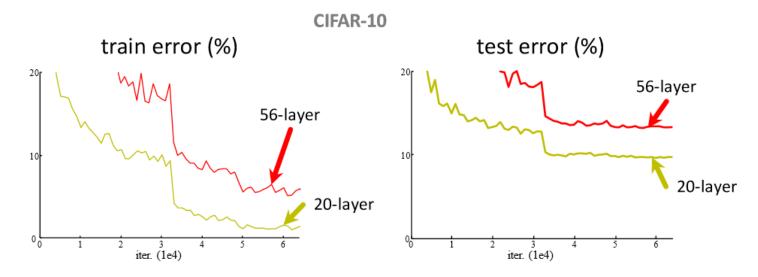
CIFAR-10

• 60,000 32x32 color images, 10 classes

Here are the classes in the dataset, as well as 10 random images from each:

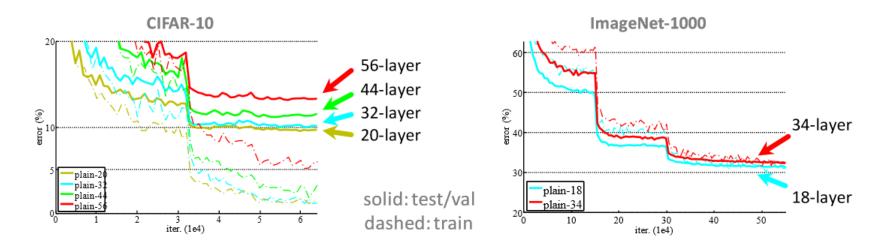
airplane	🛁 🔊 💒 📈 🍝 🐂 🛃 🔐 🛶
automobile	ar 😻 🚵 🔜 🕍 😂 📾 🐝
bird	in the second
cat	li 🖉 📚 🔛 🎇 🐜 🕰 🥪 🐋
deer	NG 🐄 😭 🥽 🦃 🎇 🐄 👔
dog	🛞 🔬 🤝 🥂 🎘 🎒 🦉 👘 🎊
frog	NA 100
horse	🚽 🐼 💥 🤭 📷 🖙 🏹 🕷
ship	🥶 🌌 🖛 🚢 🛥 💋 🖉 👛
truck	🚅 🍇 💒 🌉 🚞 🚞 🏹 🔤 🚮

Simply stacking layers?

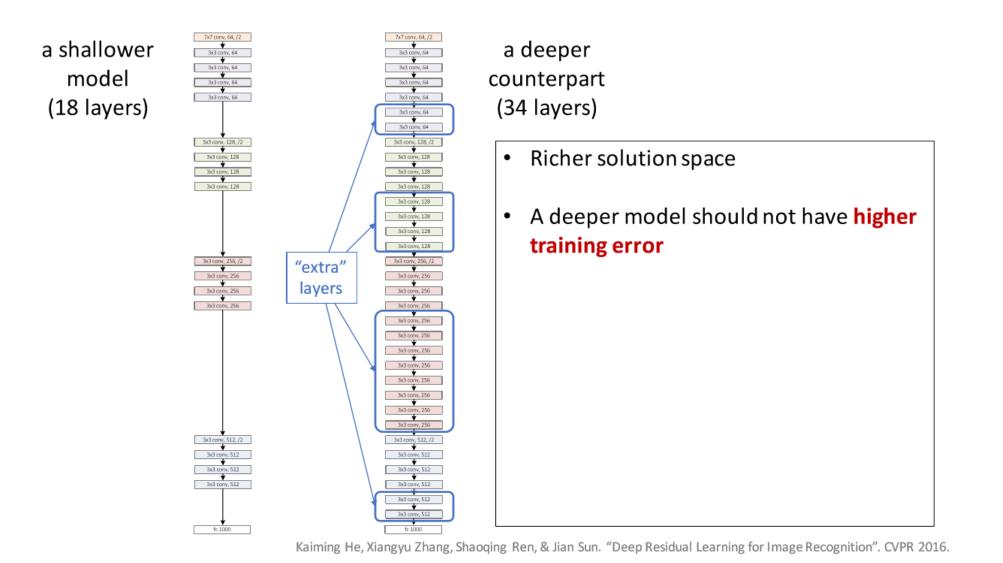


- *Plain* nets: stacking 3x3 conv layers...
- 56-layer net has higher training error and test error than 20-layer net

Simply stacking layers?



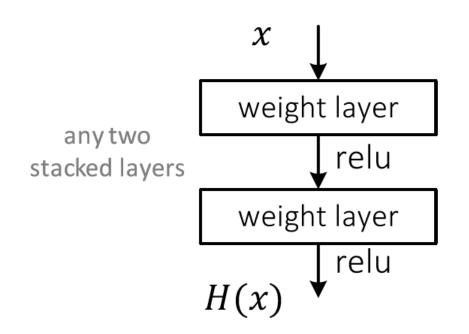
- "Overly deep" plain nets have higher training error
- A general phenomenon, observed in many datasets



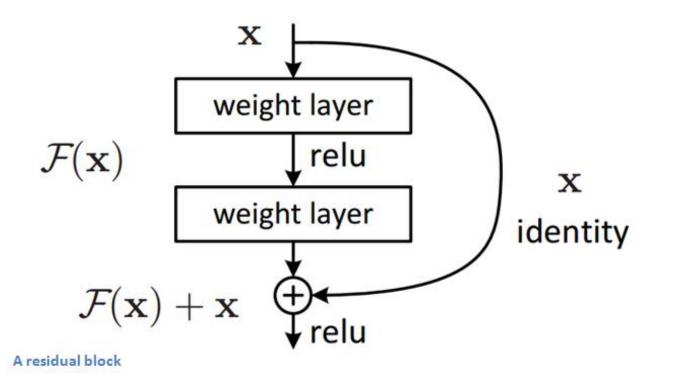
Regular net

H(x) is any desired mapping,

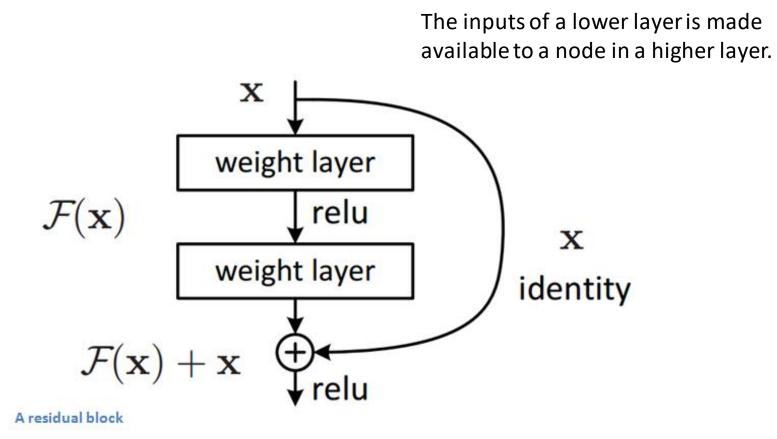
hope the 2 weight layers fit H(x)

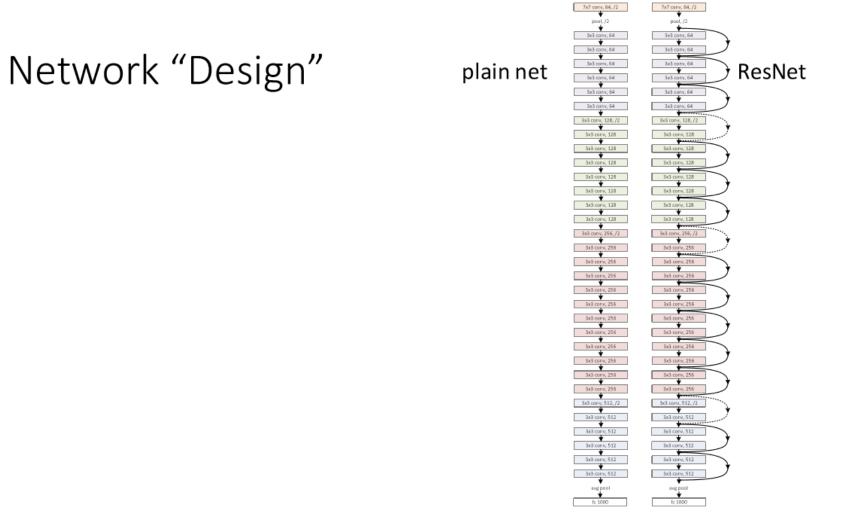


Residual Unit



Residual Unit

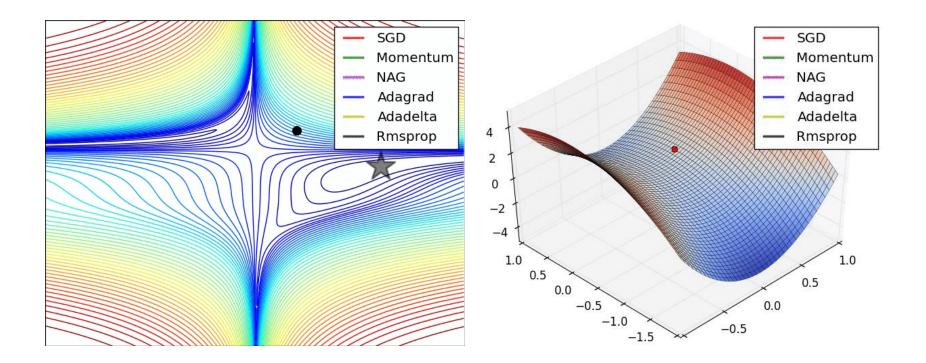




Why so steep? CIFAR-10 experiments **CIFAR-10** plain nets **CIFAR-10 ResNets** ResNet-20 ResNet-32 56-layer ResNet-44 ResNet-56 44-layer ResNet-110 20-layer error (%) 10 (%) 10 32-layer 32-layer 20-layer 44-layer MAX 56-layer plain-20 plain-32 plain-44 110-layer solid: test plain-5 dashed: train 3 iter.(1e4) 6 3 iter. (1e4)

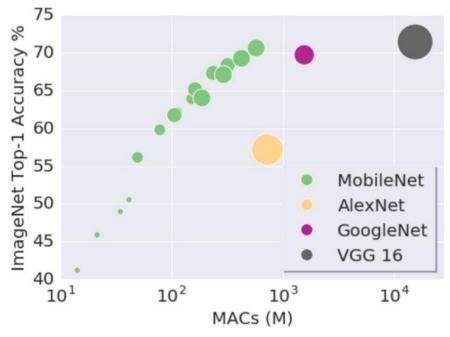
- Deep ResNets can be trained without difficulties
- Deeper ResNets have lower training error, and also lower test error

Flat regions in energy landscape



James, do we *have* to go deeper?

Compute vs. parameters / multiply-adds



Hmm...efficient nets... might be useful for final project ???

https://www.infoq.com/news/2017/06/google-mobilenets-tensorflow https://arxiv.org/abs/1704.04861