International Conference on Machine Learning (ICML) 2018 Overview

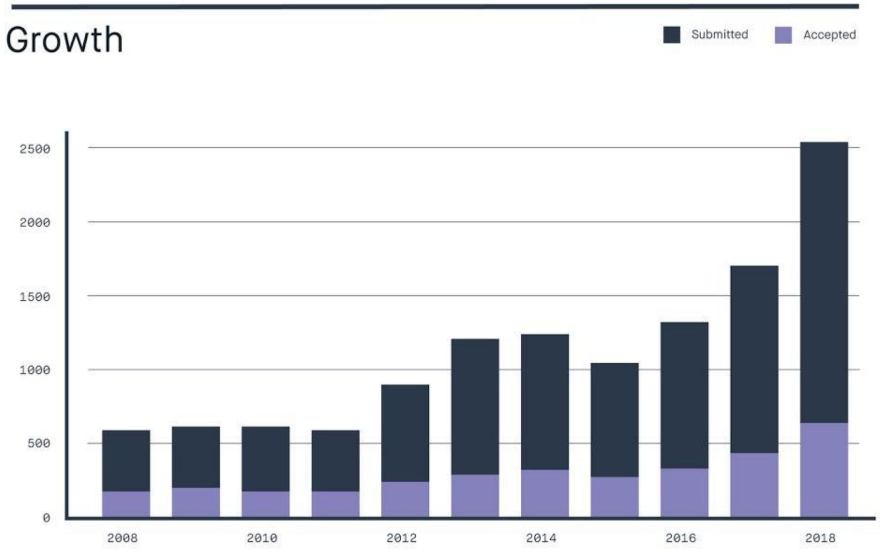
Daniel Jiang

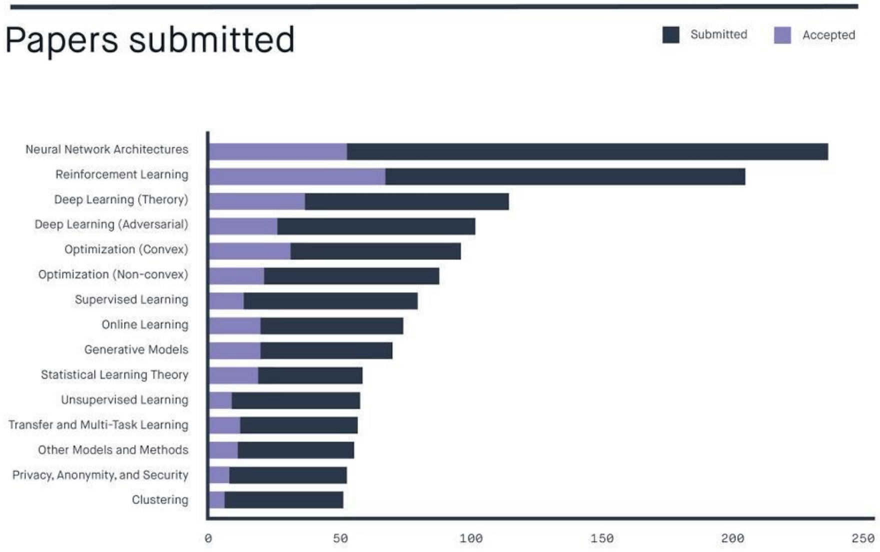
Stockholmsmässan, Stockholm, Sweden

Themes

- Tons of Reinforcement Learning
- Quite a bit of Theory and Analysis
- Steps toward addressing important issues:
    - Modeling uncertainty in our predictions
    - Security and adversarial attacks
    - Understanding the dynamics of our models
    - Logic and reasoning in our models

ICML Statistics





Source: https://peltarion.com/article/icml-2018-an-ai-party-in-our-own-backyard

Tutorial: A Tour of RL and Controls

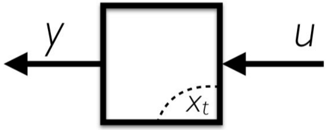
Control Theory 🤔

~~Reinforcement Learning~~ is the study of how to use past data to enhance the future manipulation of a dynamical system

(Recht, 2018)

Tutorial: A Tour of RL and Controls

Reinforcement Learning ~~Control theory~~ is the study of discrete dynamical systems with inputs



$$p(x_{t+1} \mid \text{past}) = p(x_{t+1} \mid x_t, u_t)$$

Markov Decision Process (MDP)

x_t is the *state*, and it takes values in [d]

u_t is called the *input*, and takes values in [p].

(Recht, 2018)

Tutorial: A Tour of RL and Controls

Extraordinary Claims Require
Extraordinary Evidence*

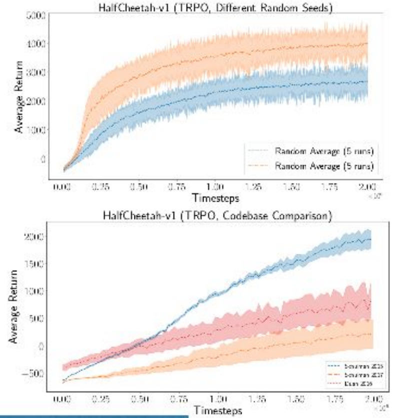
* only if your prior is correct

blog.openai.com/openai-baselines-dqn/

"Reinforcement learning results are tricky to reproduce: performance is very noisy, algorithms have many moving parts which allow for subtle bugs, and many papers don't report all the required tricks."

"RL algorithms are challenging to implement correctly; good results typically only come after fixing many seemingly-trivial bugs."

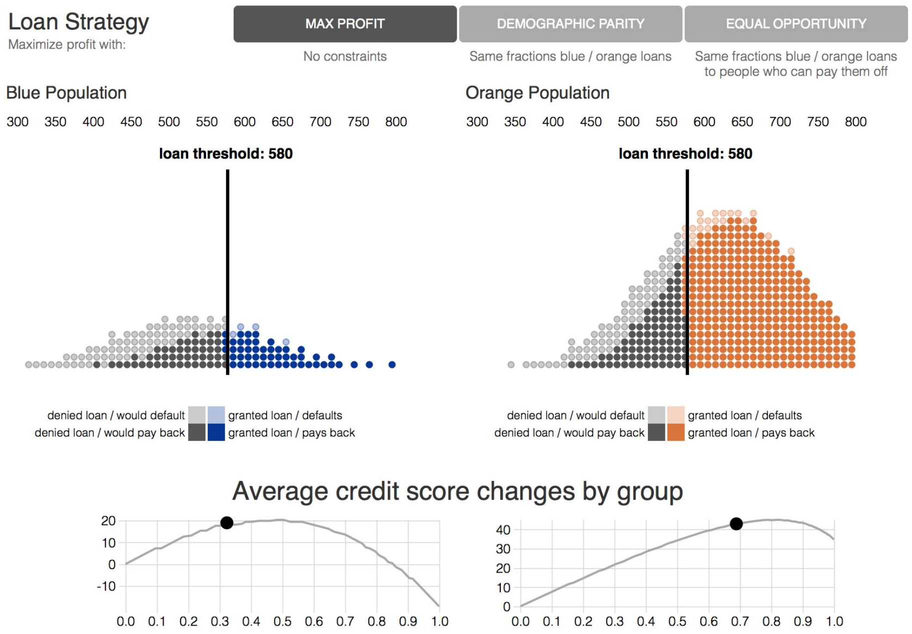
arxiv:1709.06560

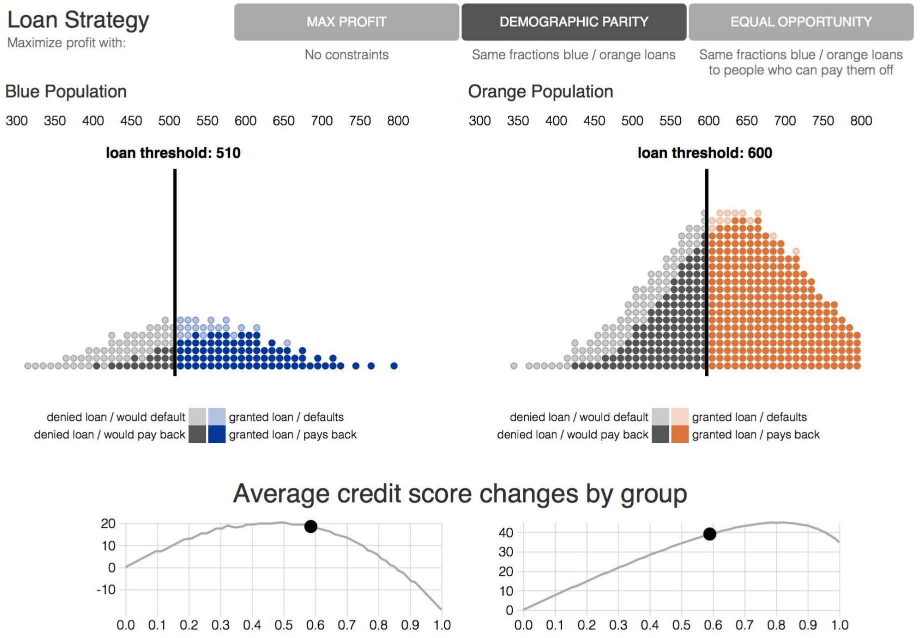


There has to be a better way!

(Recht, 2018)

Best Paper: Delayed Impact of Fair ML





(Liu et al., 2018)

Best Paper: Obfuscated Gradients Give a False Sense of Security

- Examines adversarial defense proposals from ICLR 2018
  - Finds that 7 out of 9 rely on obfuscated gradients
    - 6 of these 7 fully fall to the newly proposed attacks

Defense	Dataset	Distance	Accuracy
Buckman et al. (2018)	CIFAR	0.031 (ℓ_∞)	0%*
Ma et al. (2018)	CIFAR	0.031 (ℓ_∞)	5%
Guo et al. (2018)	ImageNet	0.005 (ℓ_2)	0%*
Dhillon et al. (2018)	CIFAR	0.031 (ℓ_∞)	0%
Xie et al. (2018)	ImageNet	0.031 (ℓ_∞)	0%*
Song et al. (2018)	CIFAR	0.031 (ℓ_∞)	9%*
Samangouei et al. (2018)	MNIST	0.005 (ℓ_2)	55%**
Madry et al. (2018)	CIFAR	0.031 (ℓ_∞)	47%
Na et al. (2018)	CIFAR	0.015 (ℓ_∞)	15%

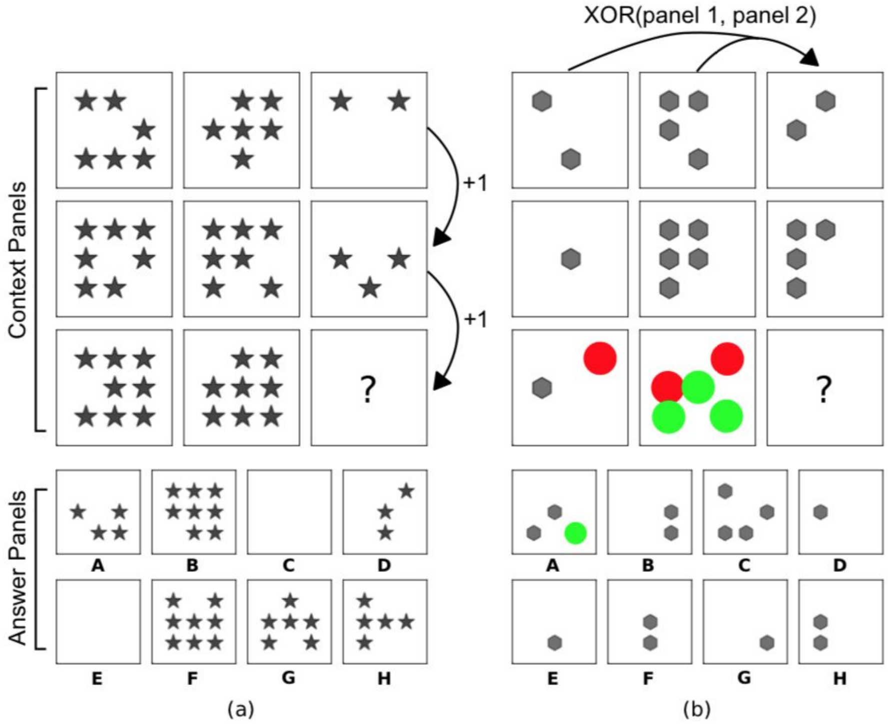
(Athalye et al., 2018)

Best Paper: Obfuscated Gradients Give a False Sense of Security

- Gradient obfuscation types
  - Shattered gradients: Some part of network is non-differentiable
    - Solution: Replace that part with differentiable approximation
  - Stochastic gradients: Random transformations
    - Solution: Differentiate through the random transformation
  - Vanishing or exploding gradients
    - Solution: Reparameterization

(Athalye et al., 2018)

Measuring abstract reasoning in neural networks



(Barrett et al., 2018)

Measuring abstract reasoning in neural networks

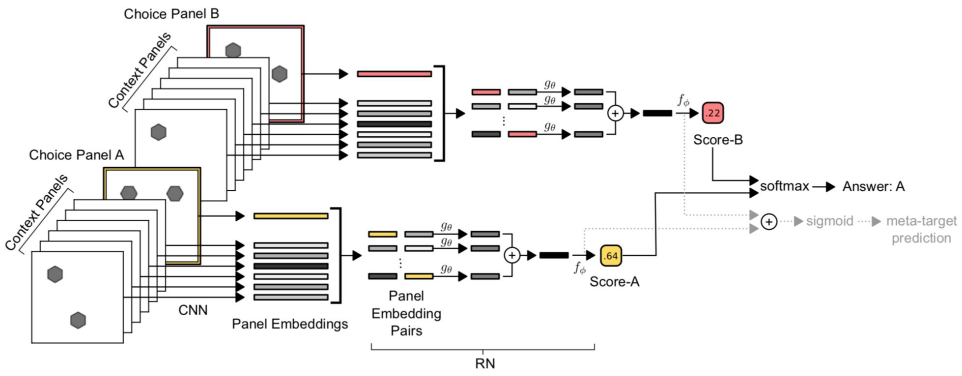
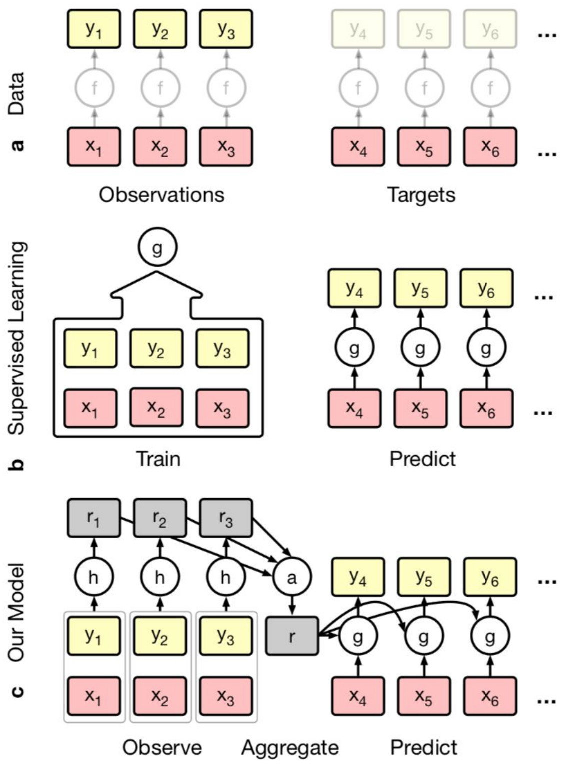


Figure 3. **WReN model** A CNN processes each context panel and an individual answer choice panel independently to produce 9 vector embeddings. This set of embeddings is then passed to an RN, whose output is a single sigmoid unit encoding the "score" for the associated answer choice panel. 8 such passes are made through this network (here we only depict 2 for clarity), one for each answer choice, and the scores are put through a softmax function to determine the model's predicted answer.

Model	Test (%)
WReN	**62.6**
Wild-ResNet	48.0
ResNet-50	42.0
LSTM	35.8
CNN + MLP	33.0
Blind ResNet	22.4

(Barrett et al., 2018)

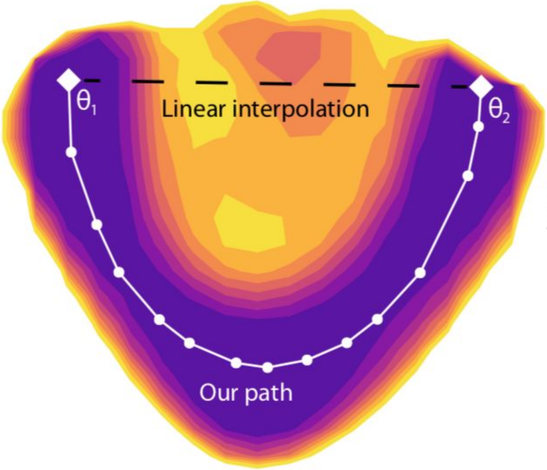
Conditional Neural Processes

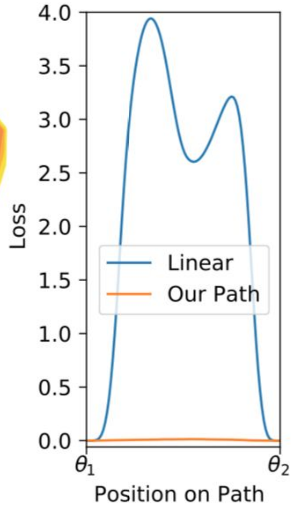


(Garnelo et al., 2018)

Essentially No Barriers in Neural Network Energy Landscape

- Claims that neural net minima form a connected manifold (or a single connected component)

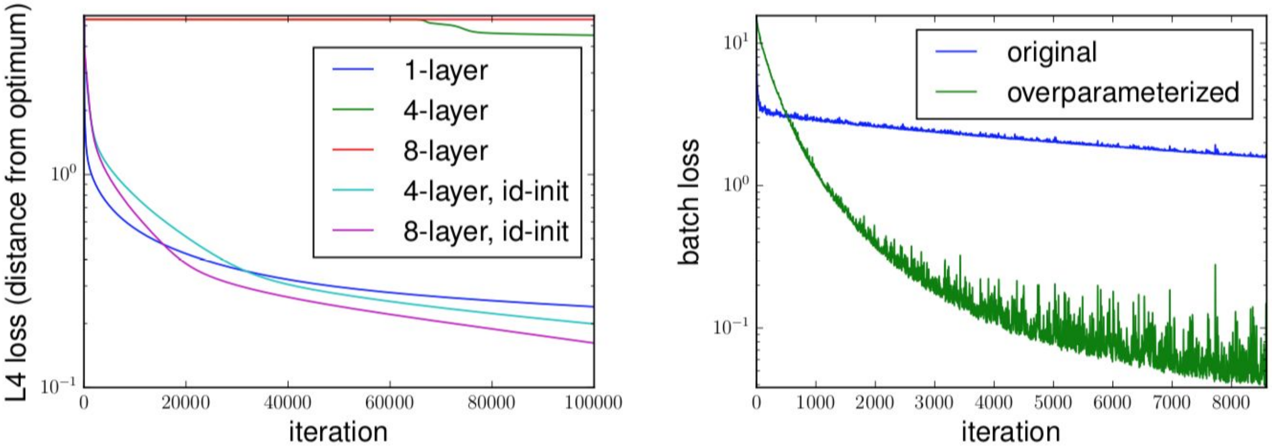




(Draxler et al., 2018)

Implicit Acceleration by Overparameterization

- Finds that overparameterized linear networks converge faster



(Arora et al., 2018)

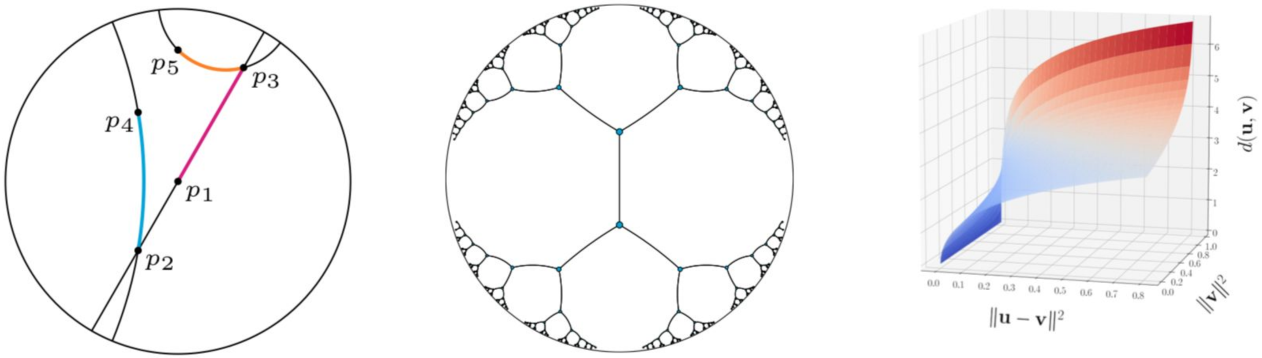
Hyperbolic embeddings (ICML 2018)

- Learning Continuous Hierarchies in the Lorentz Model of Hyperbolic Geometry
  - (Nickel & Kiela, 2018)
- Hyperbolic Entailment Cones for Learning Hierarchical Embeddings
  - (Ganea et al., 2018)
- Representation Tradeoffs for Hyperbolic Embeddings
  - (Sa et al., 2018)

Hyperbolic Embeddings (NIPS 2017)

Poincaré Embeddings for Learning Hierarchical Representations - Maximilian Nickel, Douwe Kiela (NIPS 2017)

$$d(\boldsymbol{u}, \boldsymbol{v}) = \operatorname{arcosh}\left(1 + 2\frac{\|\boldsymbol{u} - \boldsymbol{v}\|^2}{(1 - \|\boldsymbol{u}\|^2)(1 - \|\boldsymbol{v}\|^2)}\right).$$

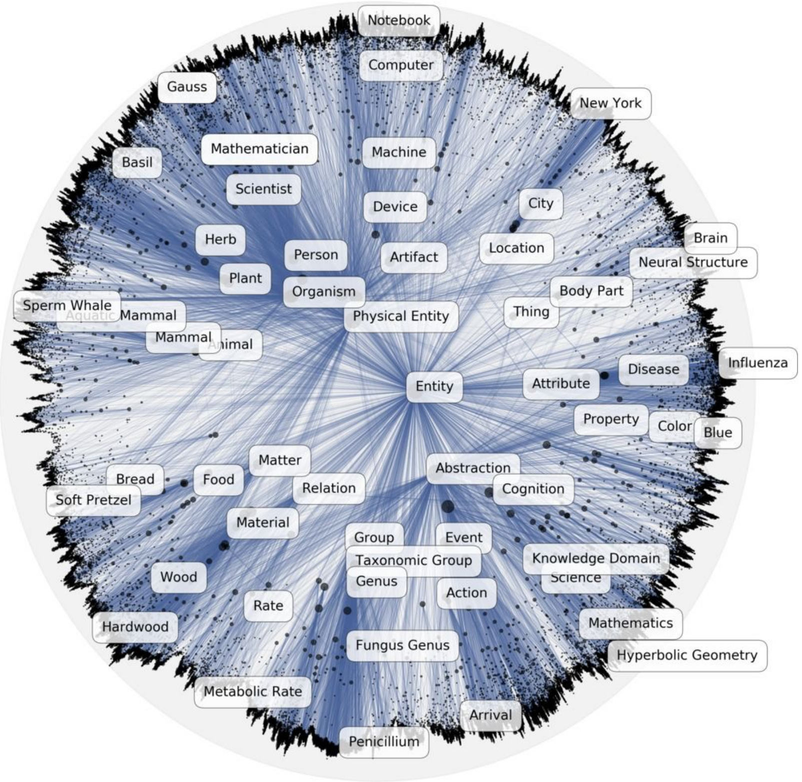


(a) Geodesics of the Poincaré disk (b) Embedding of a tree in $\mathcal{B}^2$ (c) Growth of Poincaré distance

(Nickel & Kiela, 2017)

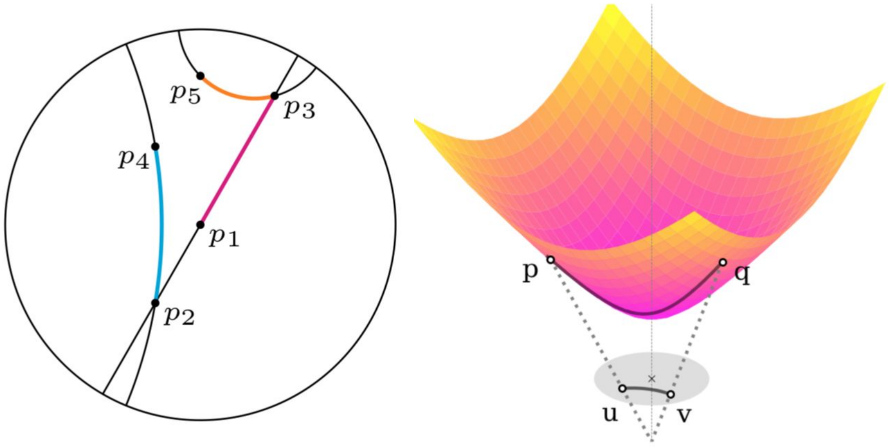
Hyperbolic Embeddings (NIPS 2017)

			Dimensionality					
			5	10	20	50	100	200
WordNet Reconstruction	Euclidean	Rank	3542.3	2286.9	1685.9	1281.7	1187.3	1157.3
		MAP	0.024	0.059	0.087	0.140	0.162	0.168
	Translational	Rank	205.9	179.4	95.3	92.8	92.7	91.0
		MAP	0.517	0.503	0.563	0.566	0.562	0.565
	Poincaré	Rank	4.9	4.02	3.84	3.98	3.9	**3.83**
		MAP	0.823	0.851	0.855	0.86	0.857	**0.87**
WordNet Link Pred.	Euclidean	Rank	3311.1	2199.5	952.3	351.4	190.7	81.5
		MAP	0.024	0.059	0.176	0.286	0.428	0.490
	Translational	Rank	65.7	56.6	52.1	47.2	43.2	40.4
		MAP	0.545	0.554	0.554	0.56	0.562	0.559
	Poincaré	Rank	5.7	**4.3**	4.9	4.6	4.6	4.6
		MAP	0.825	0.852	0.861	**0.863**	0.856	0.855

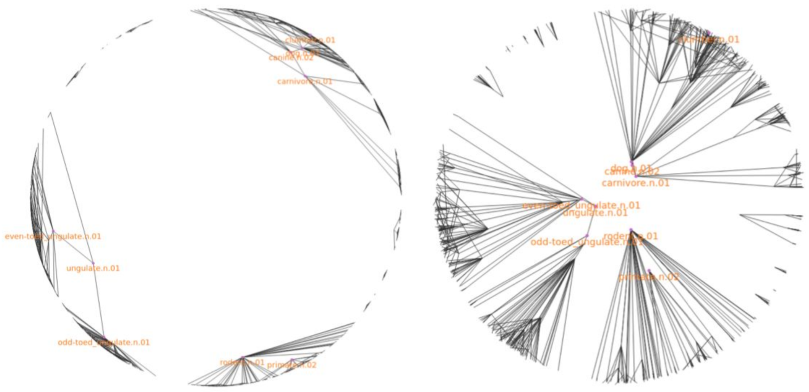


(Nickel & Kiela, 2017)

Hyperbolic Embeddings (ICML 2018)



(a) Geodesics in the Poincaré disk. (b) Lorentz model of hyperbolic geometry.



(Nickel & Kiela, 2018)

(Ganea et al., 2018)

References

- Sanjeev Arora, Nadav Cohen, Elad Hazan. On the Optimization of Deep Networks: Implicit Acceleration by Overparameterization
- Anish Athalye, Nicholas Carlini, David Wagner. Obfuscated Gradients Give a False Sense of Security: Circumventing Defenses to Adversarial Examples. ICML, 2018.
- David G.T. Barrett, Felix Hill, Adam Santoro, Ari S. Morcos, Timothy Lillicrap. Measuring abstract reasoning in neural networks. ICML, 2018.
- Felix Draxler, Kambis Veschgini, Manfred Salmhofer, Fred A. Hamprecht. Essentially No Barriers in Neural Network Energy Landscape. ICML, 2018.
- Octavian-Eugen Ganea, Gary Bécigneul, Thomas Hofmann. Hyperbolic Entailment Cones for Learning Hierarchical Embeddings. ICML, 2018.
- Marta Garnelo, Dan Rosenbaum, Chris J. Maddison, Tiago Ramalho, David Saxton, Murray Shanahan, Yee Whye Teh, Danilo J. Rezende, S. M. Ali Eslami. Conditional Neural Processes. ICML, 2018.
- Lydia Liu, Sarah Dean, Esther Rolf, Max Simchowitz, Moritz Hardt. Delayed Impact of Fair Machine Learning. ICML, 2018.
- Maximilian Nickel, Douwe Kiela. Poincaré Embeddings for Learning Hierarchical Representations. NIPS, 2017.
- Maximilian Nickel, Douwe Kiela. Learning Continuous Hierarchies in the Lorentz Model of Hyperbolic Geometry. ICML, 2018.
- Benjamin Recht. A Tour of Reinforcement Learning: The View from Continuous Control. ICML 2018 Tutorial. https://people.eecs.berkeley.edu/~brecht/l2c-icml2018/.
- Christopher De Sa, Albert Gu, Christopher Ré, Frederic Sala. Representation Tradeoffs for Hyperbolic Embeddings. ICML, 2018.

ICML 2019 is in California!

Acknowledgements

Thanks to Gerald, the NSF program manager, Jaeyoung, ICSI, and the NSF for funding and supporting my travel to ICML.

Thank you!