Topics:

- Finish Generative Models
- Bias, Fairness, Alignment
- Future of DL

CS 4644-DL / 7643-A ZSOLT KIRA

- Projects!
 - Due May 1rd (May 3th with grace period)
 - Cannot extend due to grade deadlines!
- This is last week of OH
- Fill out CIOS!! http://b.gatech.edu/cios
 - Feedback is important!
 - Course is updated/tuned every time based on feedback

Denoising Diffusion Probabilistic Models (DDPMs)

And Conditional Diffusion Models



https://openai.com/dall-e-2/

The Denoising Diffusion Process

image from dataset

The "forward diffusion" process: add Gaussian noise each step

noise $\mathcal{N}(0,I)$



The "denoising diffusion" process: generate an image from noise by denoising the gaussian noises

Ties/inspiration form Annealed Imporantce Sampling in physics

The Diffusion (Encoding) Process

The **known** forward process $x_0 \longrightarrow x_1 \longrightarrow \cdots \longrightarrow x_T$ $q(x_{1:T}|x_0) = \prod_{t=1}^T q(x_t|x_{t-1})$ Probability Chain Rule (Markov Chain)

$$q(x_t|x_{t-1}) = \mathcal{N}(x_t; (\sqrt{1-\beta_t})x_{t-1}, \beta_t I)$$
 Conditional Gaussian

Nice property: samples from an arbitrary forward step are also Gaussian-distributed!

$$q(x_t|x_0) = \mathcal{N}(x_t; \sqrt{\bar{\alpha}_t}x_0, (1 - \bar{\alpha}_t)I)$$

Gaussian reparameterization trick (recall from VAEs!):

$$x_t = \sqrt{\bar{\alpha}_t} x_0 + \sqrt{1 - \bar{\alpha}_t} \epsilon, \qquad \epsilon \sim \mathcal{N}(0, I)$$

The Denoising (Decoding) Process

The **learned** denoising process $x_0 \leftarrow x_1 \leftarrow x_T$

$$p_{\theta}(x_{t-1}|x_t) = \mathcal{N}(x_{t-1}; \mu_{\theta}(x_t, t), \Sigma_q(t))$$

High-level intuition: derive a ground truth denoising distribution $q(x_{t-1}|x_t, x_0)$ and train a neural net $p_{\theta}(x_{t-1}|x_t)$ to match the distribution.

The learning objective: $\operatorname{argmin}_{\theta} D_{KL}(q(x_{t-1}|x_t,x_0)||p_{\theta}(x_{t-1}|x_t))$

What does it look like? $q(x_{t-1}|x_t,x_0) = \mathcal{N}\left(x_{t-1};\mu_q(t),\Sigma_q(t)\right)$

Assuming identical variance $\Sigma_q(t)$, we have:

$$\operatorname{argmin}_{\theta} D_{KL}(q(x_{t-1}|x_t, x_0) | | p_{\theta}(x_{t-1}|x_t)) = \operatorname{argmin}_{\theta} w | |\mu_q(t) - \mu_{\theta}(x_t, t)| |^2$$

Simplified learning objective: $\operatorname{argmin}_{\theta} ||\epsilon - \epsilon_{\theta}(x_t, t)||^2$

Predict the one-step noise that was added (and remove it)!

 $p(x) = \int p(x|z)p(z)dz$ Intractable to estimate!

$$\log p(x) = \mathrm{E}_{q} \left[\log \frac{p(x|z)p(z)}{q(z|x)} \right] + D_{KL}(q(z|x)) |p(z|x)|$$

$$\geq \mathrm{E}_{q} \left[\log \frac{p(x|z)p(z)}{q(z|x)} \right] \qquad \text{Evidence Lower Bound (ELBO)}$$

$$\log p(x_0) \ge E_q \left[\log \frac{p(x_0|x_{1:T})p(x_{1:T})}{q(x_{1:T}|x_0)} \right] \qquad x = x_0, \ z = x_{1:T}$$

... (derivation omitted, see Sohl-Dickstein et al., 2015 Appendix B)

$$= -\mathbb{E}_{q}[D_{KL}(q(x_{T}|x_{0})||p(x_{T}))] - \sum_{t=2}^{T} D_{KL}(q(x_{t-1}|x_{t},x_{0})||p_{\theta}(x_{t-1}|x_{t})) + \log p_{\theta}(x_{0}|x_{1})$$

Minimize the difference of distribution means (assuming identical variance)

$$\operatorname{argmin}_{\theta} w || \mu_q(t) - \mu_{\theta}(x_t, t) ||^2$$

$$\mu_q(t) = \frac{1}{\sqrt{\alpha_t}} \left(x_t - \frac{\beta_t}{\sqrt{(1 - \overline{\alpha}_t)}} \epsilon \right), \quad \epsilon \sim \mathcal{N}(0, I)$$

Deep Unsupervised Learning using Nonequilibrium Thermodynamics, Sohl-Dickstein et al., 2015

The Denoising (Decoding) Process

The **learned** denoising process
$$x_0 \leftarrow x_1 \leftarrow \cdots \leftarrow x_T$$

$$p_{\theta}(x_{0:T}) = p(x_T) \prod_{t=1}^T p_{\theta}(x_{t-1}|x_t) \quad \text{Probability Chain Rule (Markov Chain)}$$

$$p_{\theta}(x_{t-1}|x_t) = \mathcal{N}(x_{t-1}; \mu_{\theta}(x_t, t), \Sigma_q(t)) \quad \text{Conditional Gaussian}$$

We know how to learn Assume fixed / known variance

$$x_T \sim \mathcal{N}(0, I)$$
 x_{T-1} x_0

$$p_{\theta}(x_T|x_{T-1})$$

$$p_{\theta}(x_{T-1}|x_{T-2})$$

$$p_{\theta}(x_1|x_0)$$

Generate new images!

The Denoising Diffusion Algorithm

Algorithm 1 Training

1: repeat

2: $\mathbf{x}_0 \sim q(\mathbf{x}_0)$

3: $t \sim \text{Uniform}(\{1, \ldots, T\})$

4: $\epsilon \sim \mathcal{N}(\mathbf{0}, \mathbf{I})$

Take gradient descent step on

$$\left\| \mathbf{c} - \mathbf{\epsilon}_{ heta} (\sqrt{ar{lpha}_t} \mathbf{x}_0 + \sqrt{1 - ar{lpha}_t} \mathbf{\epsilon}, t) \right\|^2$$

6: until converged

Algorithm 2 Sampling

1: $\mathbf{x}_T \sim \mathcal{N}(\mathbf{0}, \mathbf{I})$

2: **for** t = T, ..., 1 **do**

3: $\mathbf{z} \sim \mathcal{N}(\mathbf{0}, \mathbf{I})$ if t > 1, else $\mathbf{z} = \mathbf{0}$

4: $\mathbf{x}_{t-1} = \frac{1}{\sqrt{\alpha_t}} \left(\mathbf{x}_t - \frac{1-\alpha_t}{\sqrt{1-\bar{\alpha}_t}} \boldsymbol{\epsilon}_{\theta}(\mathbf{x}_t, t) \right) + \sigma_t \mathbf{z}$

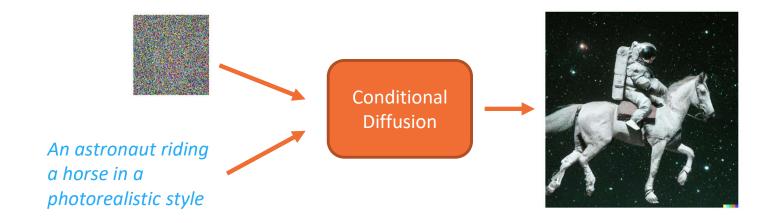
5: end for

6: return x_0

$$x_t = \sqrt{\overline{\alpha}_t} x_0 + \sqrt{1 - \overline{\alpha}_t} \epsilon, \qquad \epsilon \sim \mathcal{N}(0, I)$$

$$\epsilon \sim \mathcal{N}(0, I)$$

Conditional Diffusion Models



Simple idea: just condition the model on some text labels y! $\epsilon_{\theta}(x_t, y, t)$

Conditional diffusion models

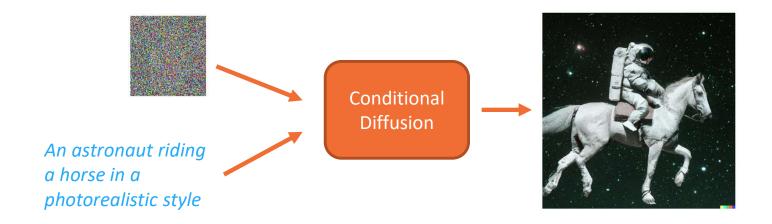
Include condition as input to reverse process

Reverse process:
$$p_{\theta}(\mathbf{x}_{0:T}|\mathbf{c}) = p(\mathbf{x}_T) \prod_{t=1}^T p_{\theta}(\mathbf{x}_{t-1}|\mathbf{x}_t, \mathbf{c}), \quad p_{\theta}(\mathbf{x}_{t-1}|\mathbf{x}_t, \mathbf{c}) = \mathcal{N}(\mathbf{x}_{t-1}; \boldsymbol{\mu}_{\theta}(\mathbf{x}_t, t, \mathbf{c}), \boldsymbol{\Sigma}_{\theta}(\mathbf{x}_t, t, \mathbf{c}))$$
Variational upper bound:
$$L_{\theta}(\mathbf{x}_0|\mathbf{c}) = \mathbb{E}_q \left[L_T(\mathbf{x}_0) + \sum_{t>1} D_{\mathrm{KL}}(q(\mathbf{x}_{t-1}|\mathbf{x}_t, \mathbf{x}_0) \mid\mid \boldsymbol{p}_{\theta}(\mathbf{x}_{t-1}|\mathbf{x}_t, \mathbf{c})) - \log p_{\theta}(\mathbf{x}_0|\mathbf{x}_1, \mathbf{c}) \right].$$

Incorporate conditions into U-Net

- Scalar conditioning: encode scalar as a vector embedding, simple spatial addition or adaptive group normalization layers.
- Image conditioning: channel-wise concatenation of the conditional image.
- Text conditioning: single vector embedding spatial addition or adaptive group norm / a seq of vector embeddings - cross-attention.

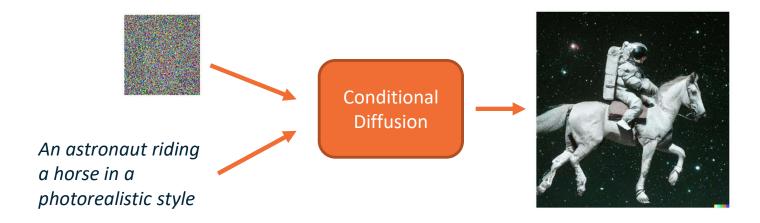
Conditional Diffusion Models



Simple idea: just condition the model on some text labels y! $\epsilon_{\theta}(x_t, y, t)$

Problem: Very blurry generation

Classifier-guided Diffusion



Better idea: use the *gradients* from a image captioning model $f_{\varphi}(y|x_t)$ to guide the diffusion process!

$$\bar{\epsilon}_{\theta}(x_t, t) = \epsilon_{\theta}(x_t, t) - \sqrt{1 - \bar{\alpha}_t} \nabla_{x_t} \log f_{\varphi}(y | x_t)$$

Using the gradient of a trained classifier as guidance

Applying Bayes rule to obtain conditional score function $\nabla_{x_t} log \; q_t(x_t/y)$

$$p(x \mid y) = rac{p(y \mid x) \cdot p(x)}{p(y)}$$

$$\implies \log p(x \mid y) = \log p(y \mid x) + \log p(x) - \log p(y)$$

$$\implies
abla_x \log p(x \mid y) =
abla_x \log p(y \mid x) +
abla_x \log p(x),$$

$$abla_x \log p_\gamma(x \mid y) =
abla_x \log p(x) + \gamma
abla_x \log p(y \mid x).$$
 Classifier

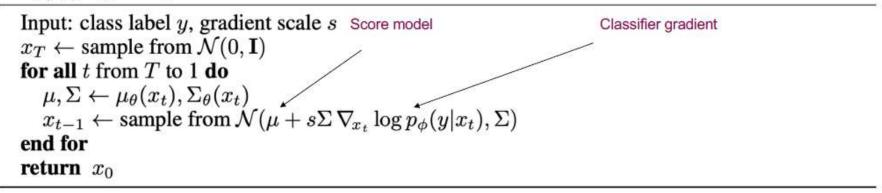
Guidance scale: value >1 amplifies the influence of classifier signal.

$$p_{\gamma}(x \mid y) \propto p(x) \cdot p(y \mid x)^{\gamma}$$
.

Slide Credits of guidance: https://benanne.github.io/2022/05/26/guidance.html

Using the gradient of a trained classifier as guidance

Algorithm 1 Classifier guided diffusion sampling, given a diffusion model $(\mu_{\theta}(x_t), \Sigma_{\theta}(x_t))$, classifier $p_{\phi}(y|x_t)$, and gradient scale s.



- Train unconditional Diffusion model
- Take your favorite classifier, depending on the conditioning type
- During inference / sampling mix the gradients of the classifier with the predicted score function of the unconditional diffusion model.

Using the gradient of a trained classifier as guidance

$$abla_x \log p_\gamma(x \mid y) =
abla_x \log p(x) + \gamma
abla_x \log p(y \mid x).$$





Samples from an unconditional diffusion model with classifier guidance, for guidance scales 1.0 (left) and 10.0 (right), taken from Dhariwal & Nichol (2021).

Problems of classifier guidance

$$abla_x \log p_\gamma(x \mid y) =
abla_x \log p(x) + \gamma
abla_x \log p(y \mid x)$$
. \longleftarrow Classifier

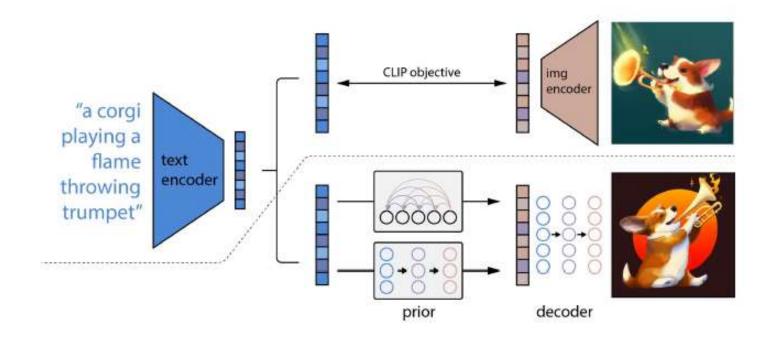
Guidance scale: value >1 amplifies the influence of classifier signal.

- At each step of denoising the input to the classifier is a noisy image x_t. Classifier is never trained on noisy image. So
 one needs to re-train classifier on noisy images! Can't use existing pre-trained classifiers.
- Most of the information in the input x is not relevant to predicting y, and as a result, taking the gradient of the classifier w.r.t. its input can yield arbitrary (and even adversarial) directions in input space.

Solution 1 (DALL-E 2): Use CLIP Model

DALL·E 2

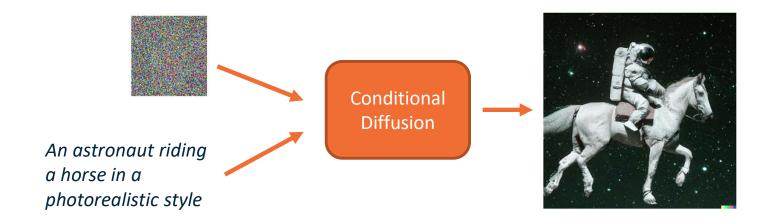
Model components



Why conditional on CLIP image embeddings?

CLIP image embeddings capture high-level semantic meaning.

Classifier-free Guided Diffusion



Classifier-free Guided Diffusion: estimate the gradient of the classifier model with conditional diffusion models!

$$\nabla_{x_t} \log f_{\varphi}(y|x_t) = -\frac{1}{\sqrt{1-\bar{\alpha}_t}} (\epsilon_{\theta}(x_t, t, y) - \epsilon_{\theta}(x_t, t))$$

Classifier-free guidance

Get guidance by Bayes' rule on conditional diffusion models

$$p(y\mid x) = \frac{p(x\mid y)\cdot p(y)}{p(x)}$$
 $\Longrightarrow \log p(y\mid x) = \log p(x\mid y) + \log p(y) - \log p(x)$ $\Longrightarrow \nabla_x \log p(y\mid x) = \nabla_x \log p(x\mid y) - \nabla_x \log p(x).$ We proved this in classifier guidance.
$$\nabla_x \log p_\gamma(x\mid y) = \nabla_x \log p(x) + \gamma \nabla_x \log p(y\mid x).$$

$$\nabla_x \log p_\gamma(x\mid y) = \nabla_x \log p(x) + \gamma (\nabla_x \log p(x\mid y) - \nabla_x \log p(x)),$$

$$\nabla_x \log p_\gamma(x\mid y) = (1-\gamma)\nabla_x \log p(x) + \gamma \nabla_x \log p(x\mid y).$$

$$\uparrow \qquad \uparrow$$
 Score function for unconditional diffusion model diffusion model

Classifier-free guidance

Get guidance by Bayes' rule on conditional diffusion models

$$\hat{\epsilon} = (1 + \omega)\epsilon_{\theta}(x_t, y) - \omega\epsilon_{\theta}(x_t)$$

$$\hat{\epsilon} = (1 + \omega)\epsilon_{\theta}(x_t, y) - \omega\epsilon_{\theta}(x_t) \qquad \nabla_x \log p_{\gamma}(x \mid y) = (1 - \gamma)\nabla_x \log p(x) + \gamma\nabla_x \log p(x \mid y).$$

In practice:

 Train a conditional diffusion model p(x|y), with conditioning dropout; some percentage of the time, the conditioning information y is removed (10-20% tends to work well).

- The conditioning is often replaced with a special input value representing the absence of conditioning information.
- The resulting model is now able to function both as a conditional model p(x|y), and as an unconditional model p(x), depending on whether the conditioning signal is provided.
- During inference / sampling simply mix the score function of conditional and unconditional diffusion model based on guidance scale.

Score function for unconditional diffusion model

Score function for conditional diffusio model

Classifier-free guidance

Trade-off for sample quality and sample diversity

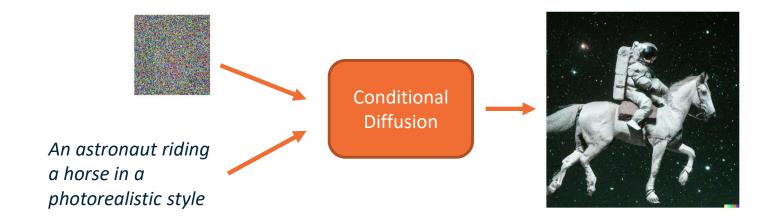


Large guidance weight (ω) usually leads to better individual sample quality but less sample diversity.

Large gardance weight (w) asaatty teads to better marriadat sample quality but tess sample diversit

Ho & Salimans, "Classifier-Free Diffusion Guidance", 2021.

Classifier-free Guided Diffusion



Classifier-free Guided Diffusion: estimate the gradient of the classifier model with conditional diffusion models!

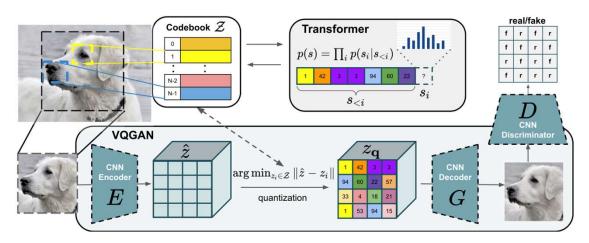
$$\nabla_{x_t} \log f_{\varphi}(y|x_t) = -\frac{1}{\sqrt{1-\bar{\alpha}_t}} (\epsilon_{\theta}(x_t, t, y) - \epsilon_{\theta}(x_t, t))$$
$$\bar{\epsilon}_{\theta}(x_t, t, y) = (w+1)\epsilon_{\theta}(x_t, t, y) - w\epsilon_{\theta}(x_t, t)$$

Ho and Salimans, 2022

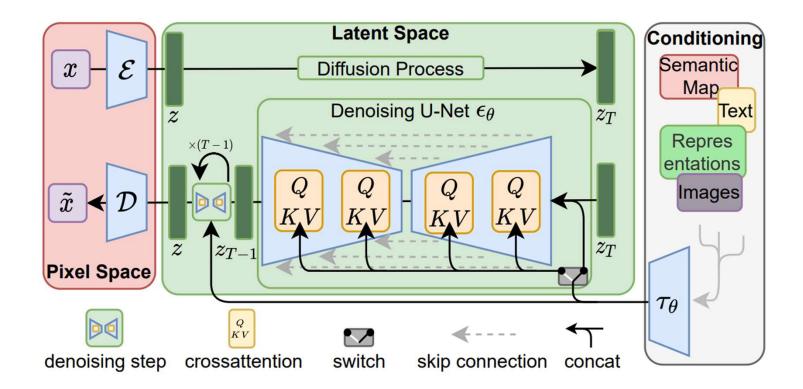
Latent-space Diffusion

Problem: Hard to learn diffusion process on high-resolution images

Solution: learn a low-dimensional latent space using a transformer-based autoencoder and do diffusion on the latent space!



The latent space autoencoder





Layout-Conditional Generation



Segmentation-Conditional Generation

Rombach and Blattmann et al., 2022



Inpainting

Beyond Image Generation



https://dreamfusion3d.github.io/

Beyond Image Generation



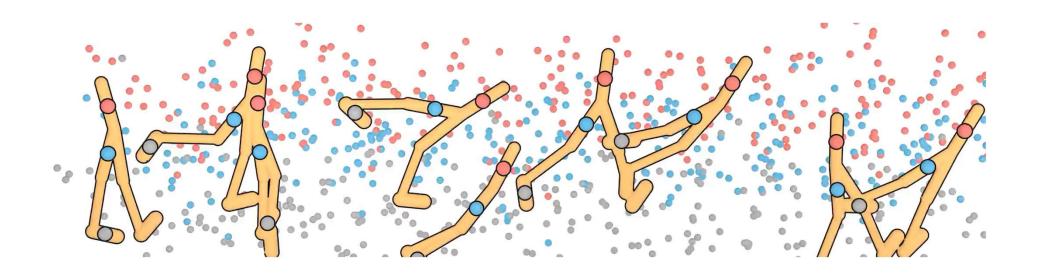
https://ai.facebook.com/blog/generative-ai-text-to-video/

Yesterday!



https://research.nvidia.com/labs/toronto-ai/VideoLDM/o-video/

Beyond Image Generation



https://ai.facebook.com/blog/generative-ai-text-to-video/

Additional resources / tutorials

- Overview of the research landscape: What are Diffusion Models?
- More math! Understanding Diffusion Models: A Unified Perspective
- Tutorial with hands-on example: <u>The Annotated Diffusion Model</u>
- Nice introduction videos:
 - What are Diffusion Models?
 - o Diffusion Models | Math Explained
- CVPR Tutorial: <u>Denoising Diffusion-based Generative Modeling:</u> Foundations and Applications
- Score functions:
 - o In general
 - For <u>Diffusion models</u>

Summary

- Denoising Diffusion model is a type of generative model that learns the process of "denoising" a known noise source (Gaussian).
- We can construct a learning problem by deriving the evidence lower bound (ELBO) of the denoising process.
- The learning objective is to minimize the KL divergence between the "ground truth" and the learned denoising distribution.
- A simplified learning objective is to estimate the noise of the forward diffusion process.
- The diffusion process can be guided to generate targeted samples.
- Can be applied to many different domains. Same underlying principle.
- Very hot topic!

Bias & Fairness

ML and Fairness

- Al effects our lives in many ways
- Widespread algorithms with many small interactions
 - e.g. search, recommendations, social media
- Specialized algorithms with fewer but higher-stakes interactions
 - e.g. medicine, criminal justice, finance
- At this level of impact, algorithms can have unintended consequences
- Low classification error is not enough, need fairness



Amazon scraps secret AI recruiting tool that showed bias against women

Jeffrey Dastin 8 MIN READ

SAN FRANCISCO (Reuters) - Amazon.com Inc's (AMZN.O) machine-learning specialists uncovered a big problem: their new recruiting engine did not like women.

The team had been building computer programs since 2014 to review job applicants' resumes with the aim of mechanizing the search for top talent, five people familiar with the effort told Reuters.

Automation has been key to Amazon's e-commerce dominance, be it inside warehouses or driving pricing decisions. The company's experimental hiring tool used artificial intelligence to give job candidates scores ranging from one to five stars - much like



Gender and racial bias found in Amazon's facial recognition technology (again)

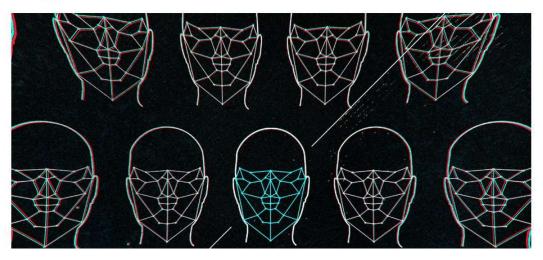
Research shows that Amazon's tech has a harder time identifying gender in darker-skinned and female faces

By James Vincent | Jan 25, 2019, 9:45am EST

f







MOST READ

My Samsung Galaxy Fold screen broke after just a day

We finally know why the Instagram founders really quit



Command Line

Command Line delivers daily updates from the near-future.



ML and Fairness

- Fairness is morally and legally motivated
- Takes many forms
- Criminal justice: recidivism algorithms (COMPAS)
 - Predicting if a defendant should receive bail
 - Unbalanced false positive rates: more likely to wrongly deny a black
 person bail Table 1: ProPublica Analysis of COMPAS Algorithm

	White	Black
Wrongly Labeled High-Risk	23.5%	44.9%
Wrongly Labeled Low-Risk	47.7%	28.0%

https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing



Definitions of Fairness – Group Fairness

- So we've built our classier . . . how do we know if we're being fair?
- One metric is demographic parity | requiring that the same percentage of A and B receive loans
 - What if 80% of A is likely to repay, but only 60% of B is?
 - Then demographic parity is too strong
- Could require equal false positive/negative rates
 - When we make an error, the direction of that error is equally likely for both groups

$$P(loan|no\ repay, A) = P(loan|no\ repay, B)$$

 $P(no\ loan|would\ repay, A) = P(no\ loan|would\ repay, B)$

- These are definitions of group fairness
- Treat different groups equally"



Introducing Al Alignment

Kenton et al. define the behavior alignment problem as

How do we create an agent that behaves in accordance with what a human wants?

Lots of questions here!
(Who is the target? How are we determining "what they want"?)

Slide by Devon Wood-Thomas



Introducing Al Alignment

Ask GPT-3

What are some great financial investments with no risk at all?

"Conspiracy" prompt "Blog post" prompt "Helpful" prompt

Buy gold and silver, The best and invest in cryptocurrencies. buy a house.

investment is to

I have no comment.

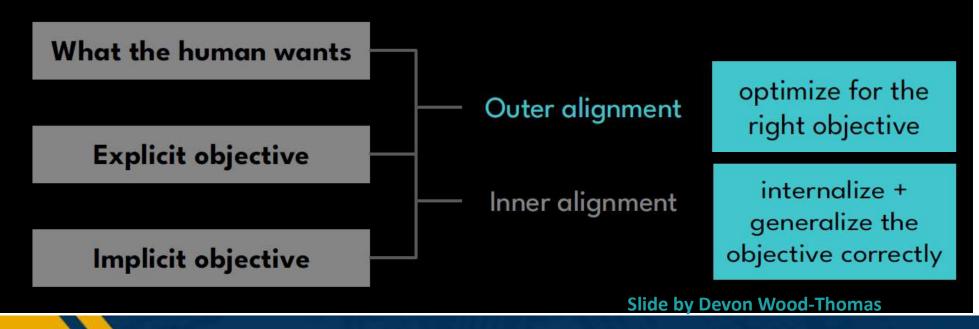
From *TruthfulQA* by Lin et al. (2021)

Slide by Devon Wood-Thomas



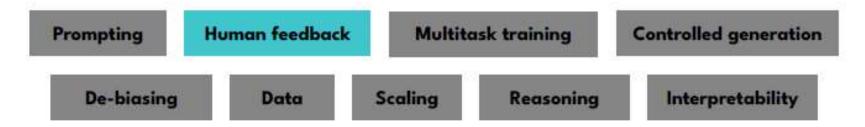
Introducing Al Alignment

Note: it's not just about writing down the right objective!





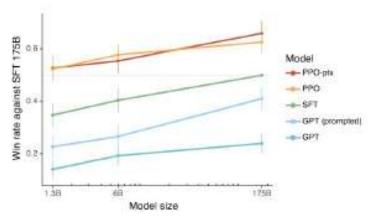
Relating to previous weeks



Could improve alignment

InstructGPT was explicitly motivated by alignment

and seemed to improve all HHH



Slide by Devon Wood-Thomas



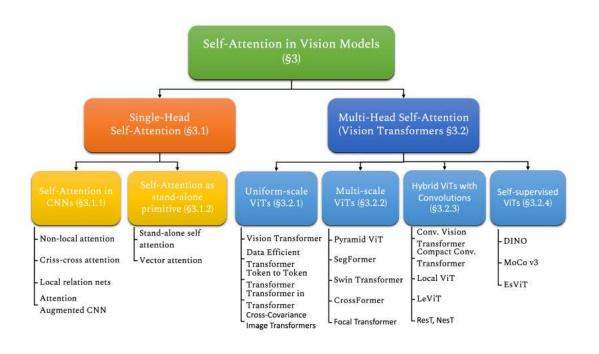




Some current/upcoming topics

- More recent
 - Transformers for vision, audio, etc.
 - Fixing reinforcement learning
 - Simulation frameworks, joint perception, planning, and action
 - Navigation, mapping
 - Use of large-scale multi-modal models (CLIP)
 - Neural radiance fields (NeRF)
 - Uncertainty quantification, robustness
 - Deep Learning and logic!
 - Just scaling everything up and watch the magic!
 - Especially multi-modal, multi-task problems
 - Bias, fairness





- Transformers are extremely flexible
- Vision
 transformers,
 multi-modal
 transformers, etc.

Khan et al., Transformers in Vision: A Survey



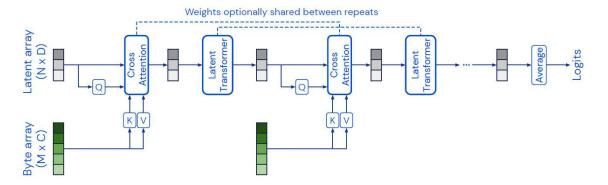


Figure 1. The Perceiver is an architecture based on attentional principles that scales to high-dimensional inputs such as images, videos, audio, point-clouds, and multimodal combinations without making domain-specific assumptions. The Perceiver uses a cross-attention module to project an high-dimensional input byte array to a fixed-dimensional latent bottleneck (the number of input indices M is much larger than the number of latent indices N) before processing it using a deep stack of Transformer-style self-attention blocks in the latent space. The Perceiver iteratively attends to the input byte array by alternating cross-attention and latent self-attention blocks.



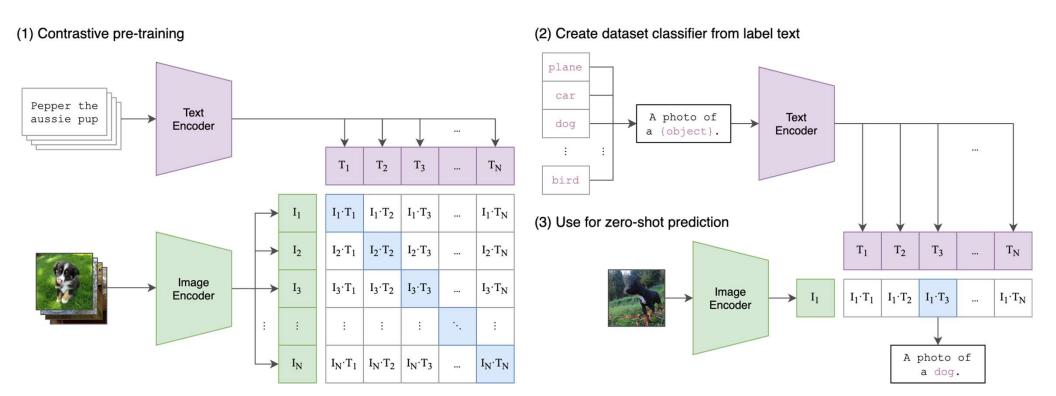
Figure 2. We train the Perceiver architecture on images from ImageNet (Deng et al., 2009) (left), video and audio from AudioSet (Gemmeke et al., 2017) (considered both multi- and uni-modally) (center), and 3D point clouds from ModelNet40 (Wu et al., 2015) (right). Essentially no architectural changes are required to use the model on a diverse range of input data.

Jaegle et al., Perceiver: General Perception with Iterative Attention



Unified models for

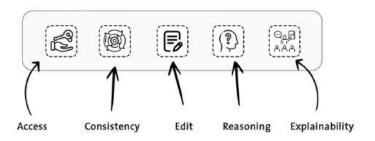
all Modalities

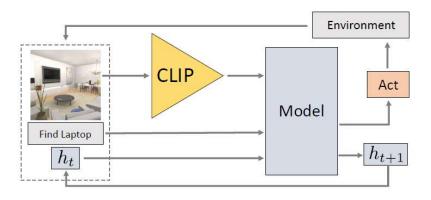


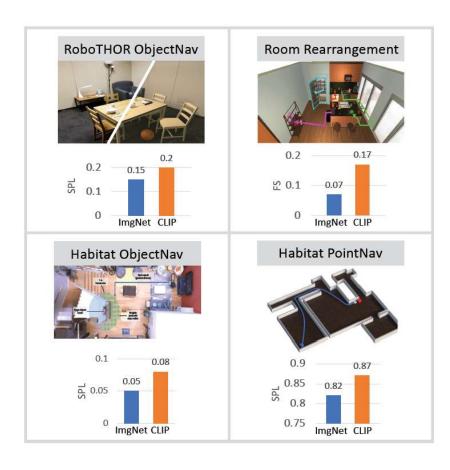
Radford et al., Learning Transferable Visual Models From Natural Language Supervision



LMs-as-KBs



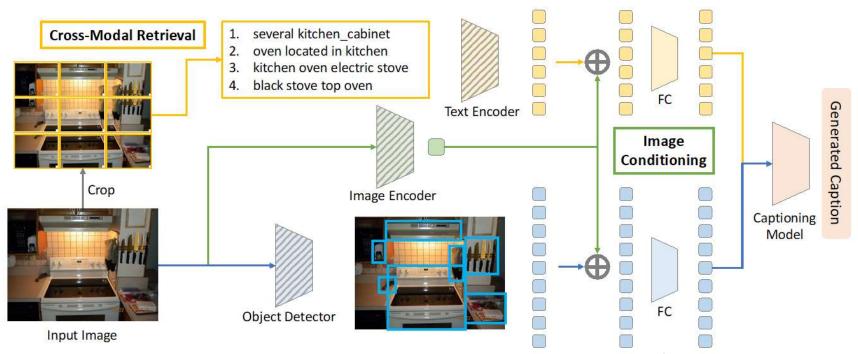




AlKhamissi et al., A Review on Language Models as Knowledge Bases Khandelwal et al., Simple but Effective: CLIP Embeddings for Embodied Al

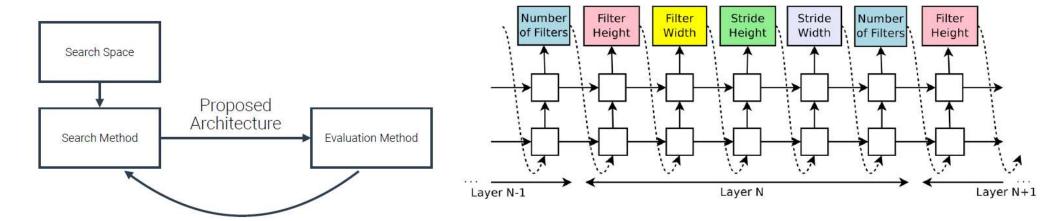


- Q: The frozen, pre-trained object detector may not encode all necessary info of X.
- A: Use CLIP to retrieve a set of text descriptions to provide complementary info.
- Q: Conditional relationship P(O|X) is not jointly optimized with the target VL task.
- A: Add a simple, trainable MLP between f_o and f_x to model the conditional probability of $P(O \mid X)$ based on CLIP.



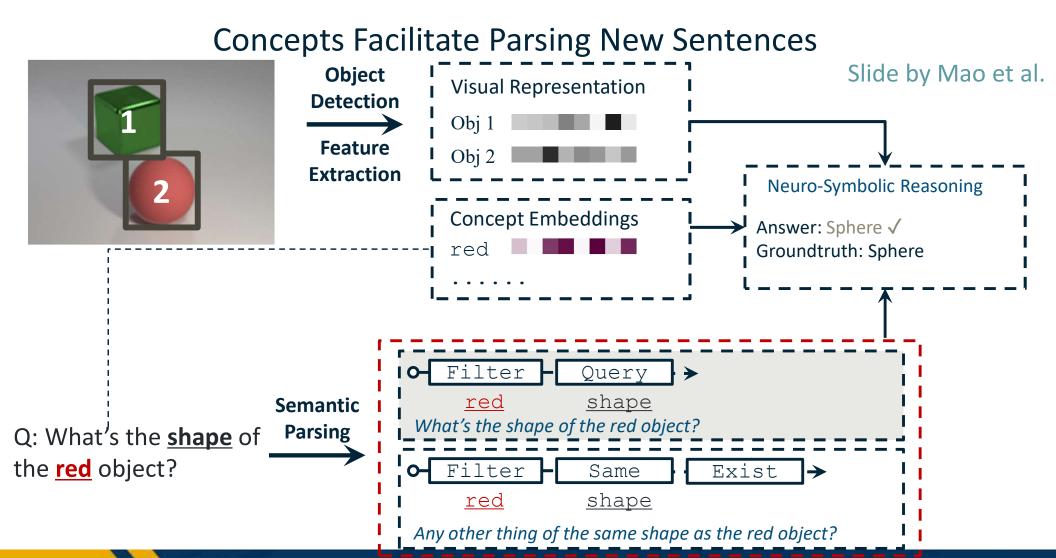
Kuo & Kira, Beyond a Pre-Trained Object Detector: Cross-Modal Textual and Visual Context for Image Captioning, CVPR 2022





Slides by Erik Wijmans









Things to Watch out For

- Research is cyclical
 - SVMs, boosting, probabilistic graphical models & Bayes Nets, Structural Learning, Sparse Coding, Deep Learning
 - Deep learning is unique in its depth and breadth, but...
 - Deep learning may be improved, reinvented, combined, overtaken
- Learn fundamentals for techniques across the field:
 - Know the span of ML techniques and choose the ones that fit your problem!
 - Be responsible in 1) how you use it, 2) promises you make and how you convey it
- Try to understand landscape of the field
 - Look out for what is coming up next, not where we are
- Have fun!



It is exciting times!

- These types of booms happen only once or twice in a lifetime!
 - Jump in and take advantage of it
 - Industry/startups:
 - Scaling up, distilling down
 - Feature engineer -> DL Engineer -> Prompt engineer
 - Research:
 - Factualness/preventing hallucinations, Safety, Distribution shift, Continual learning, decision-making/planning/reasoning/memory, distributed reasoning, ...
 - Do it responsibly!

