Machine Learning Basics

Weizi Li

Department of Computer Science
University of Memphis

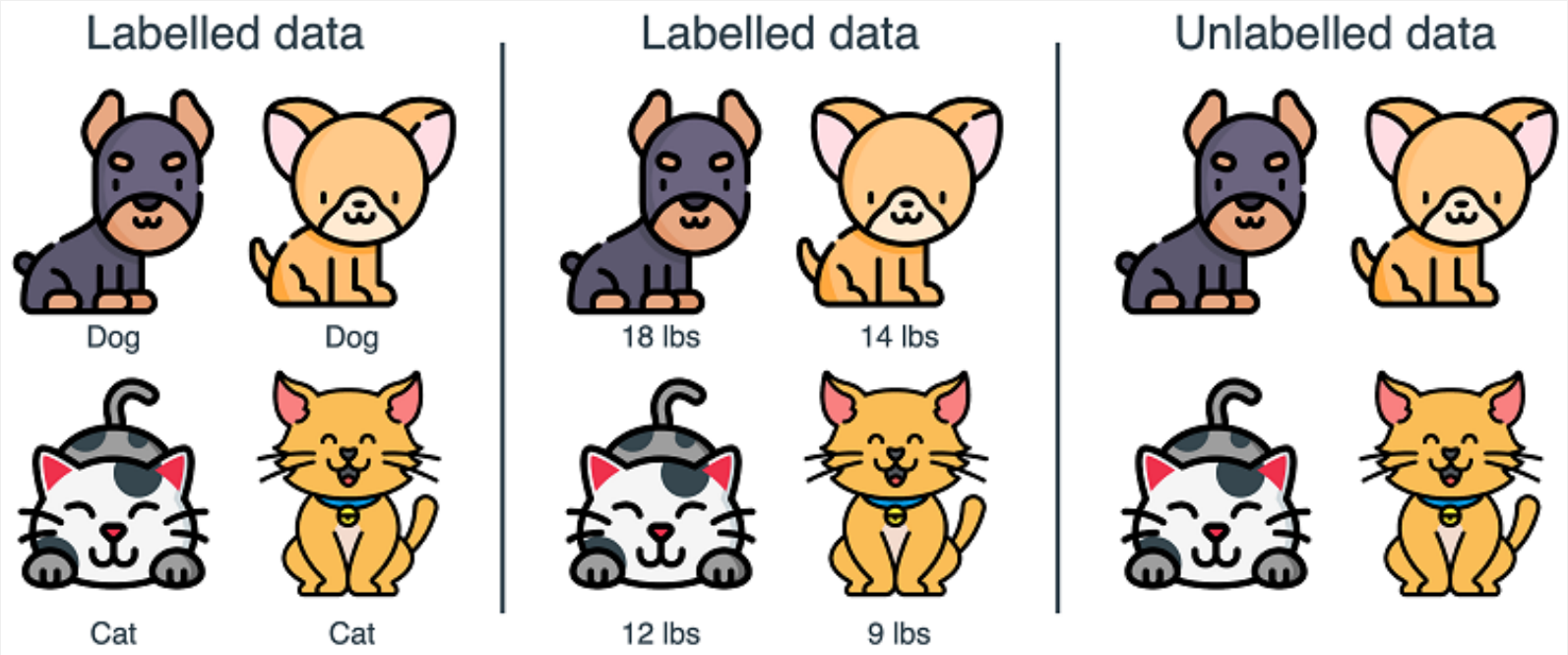
Outline

- Learning Paradigms
- Learning Pipeline

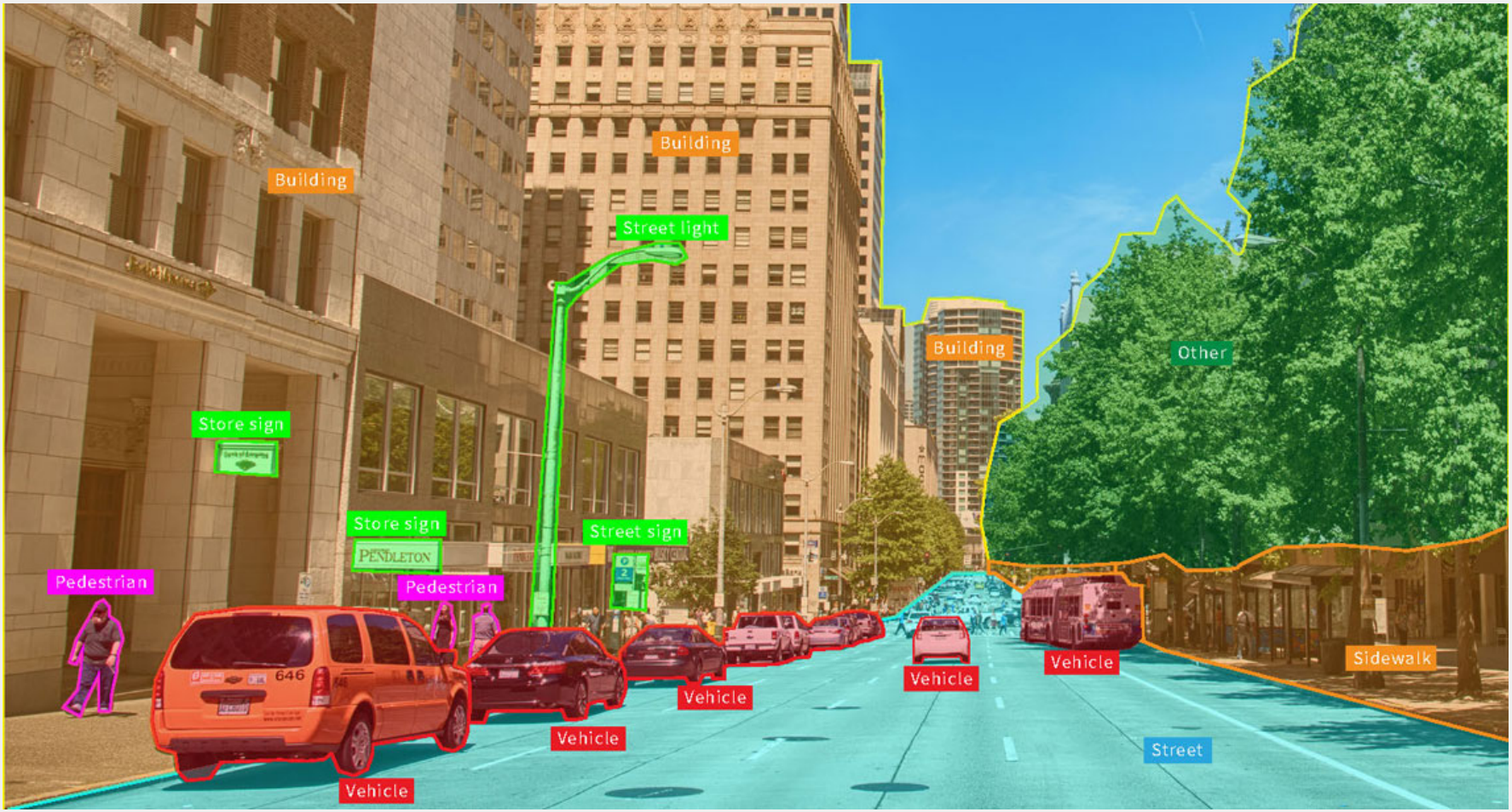
Learning Paradigms

- Supervised learning
- Unsupervised learning
- Reinforcement learning

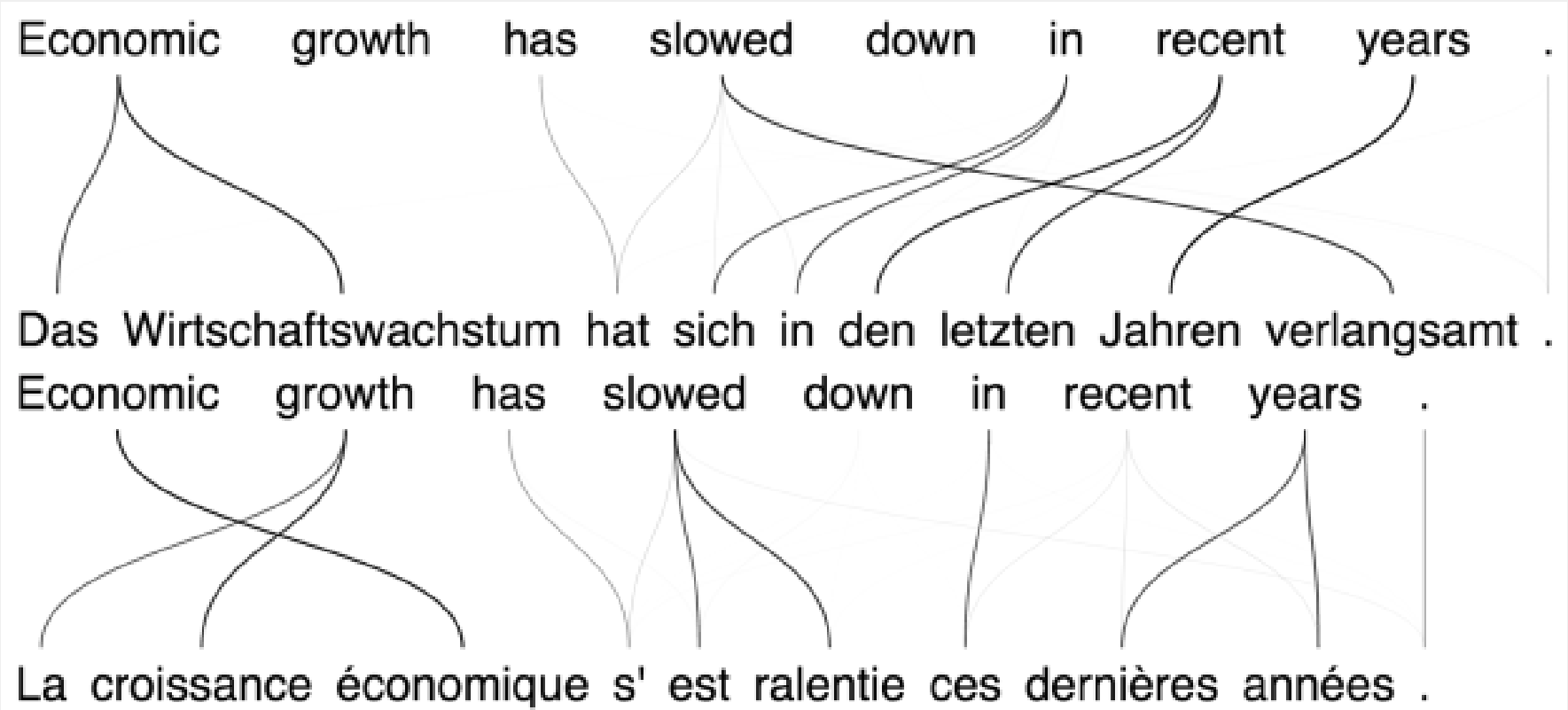
- Uses labelled data, hence "supervised"



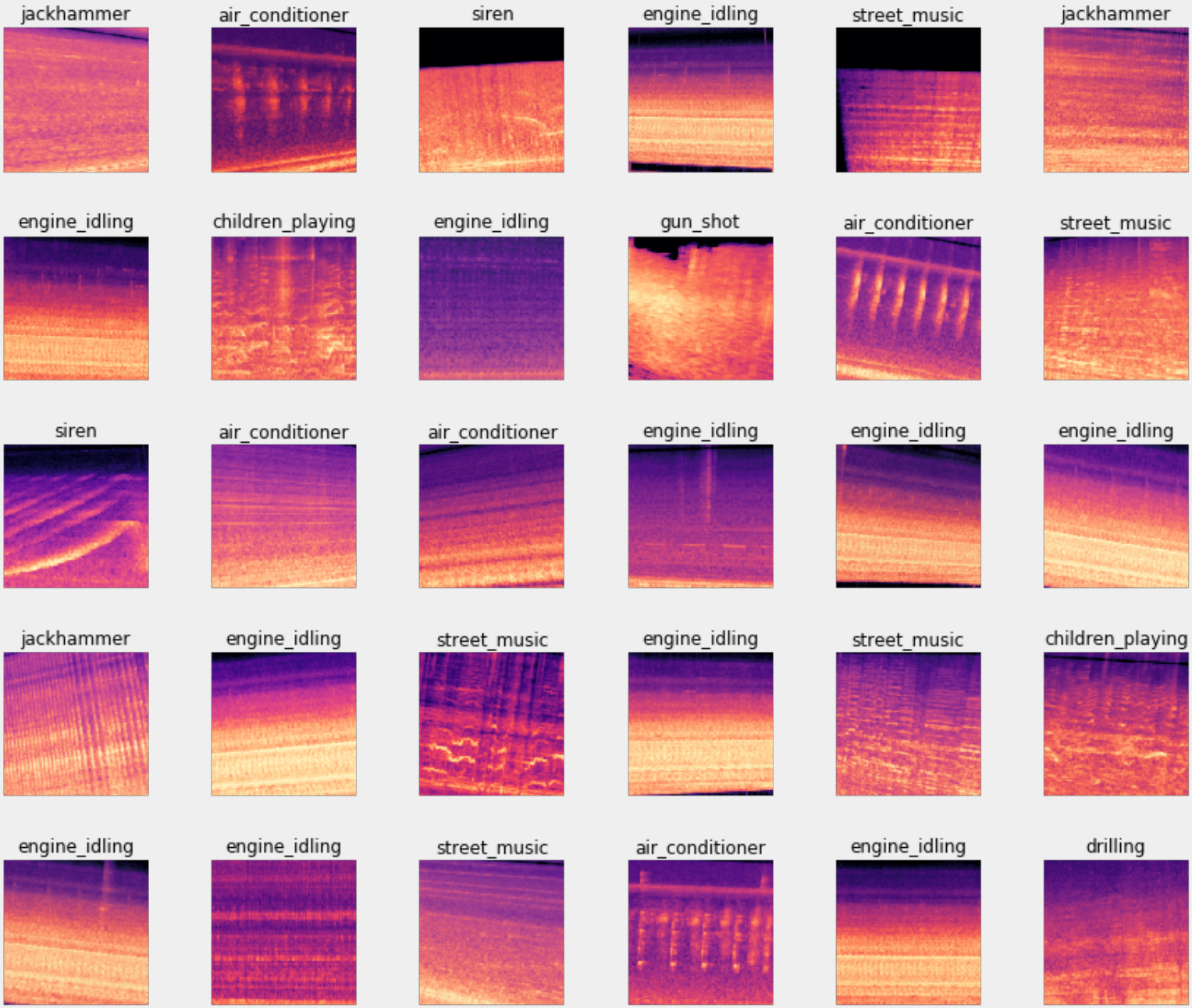
Supervised Learning: Labelled Data



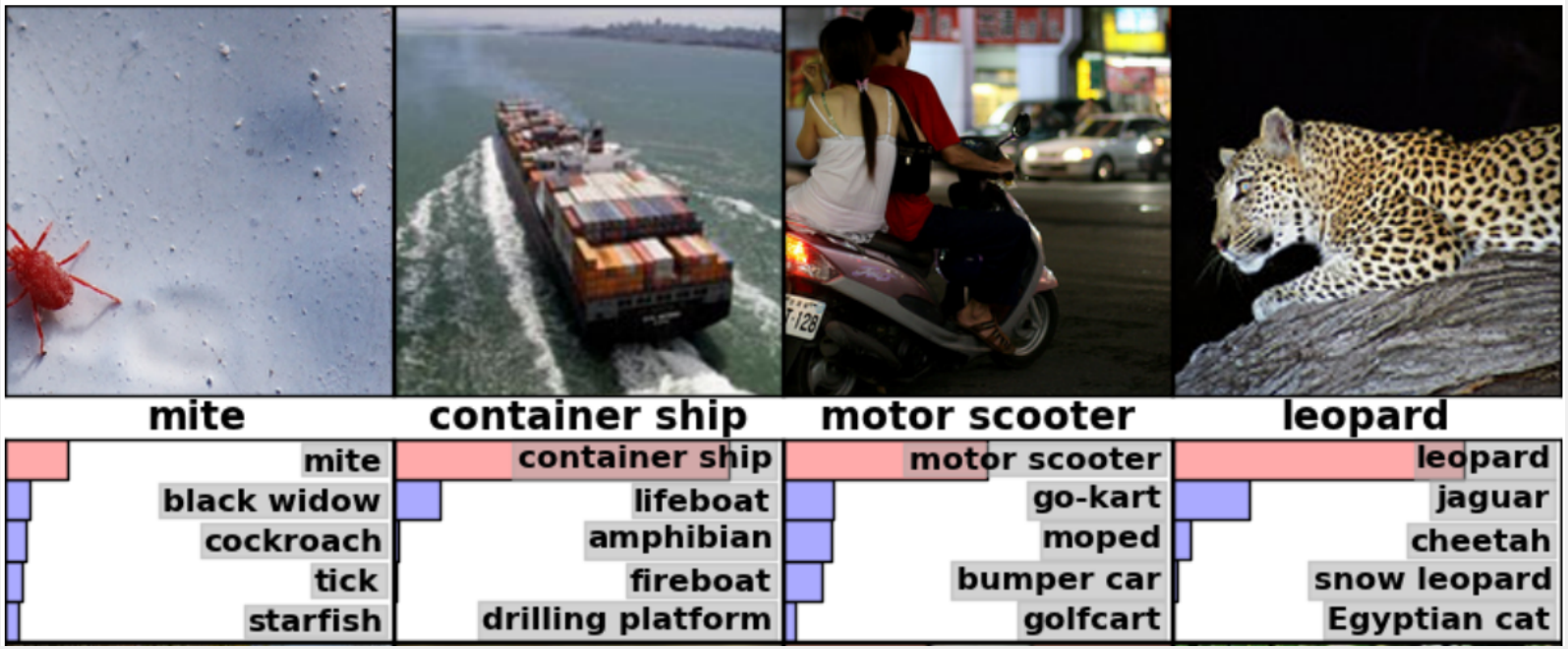
Supervised Learning: Labelled Data



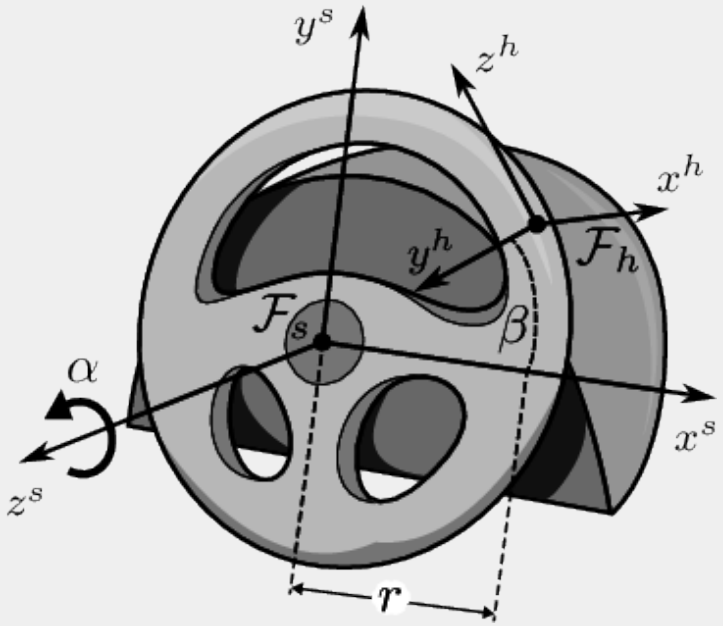
Supervised Learning: Labelled Data



- Classification: predict categorical labels (discrete values)
- E.g., ImageNet: 1,000 object classes (categories), 1M+ images, labels are crowd-sourced



- Regression: predict numerical labels (continuous values)
- E.g., stock price, temperature, continuous control commands, etc.

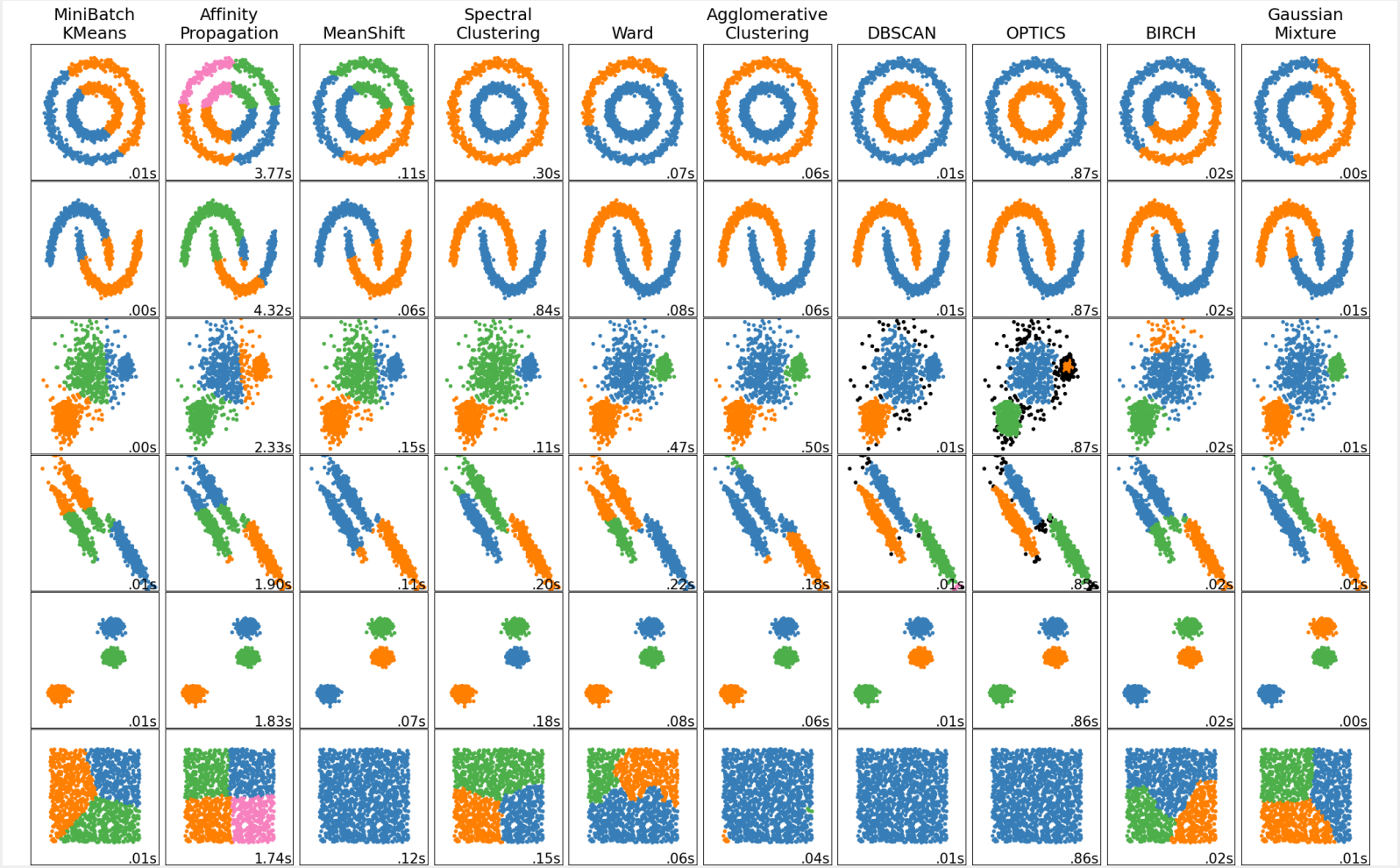


- Training set: train a model
- Validation set: tune a model through its hyperparameters
- Test set: test a model
- Example ratio: 6:2:2

- Assumption 1: data are from the same distribution (usually unknown)
- Assumption 2: training data are i.i.d. (independent and identically distributed)
- Note: non-i.i.d. data may or may not break supervised learning

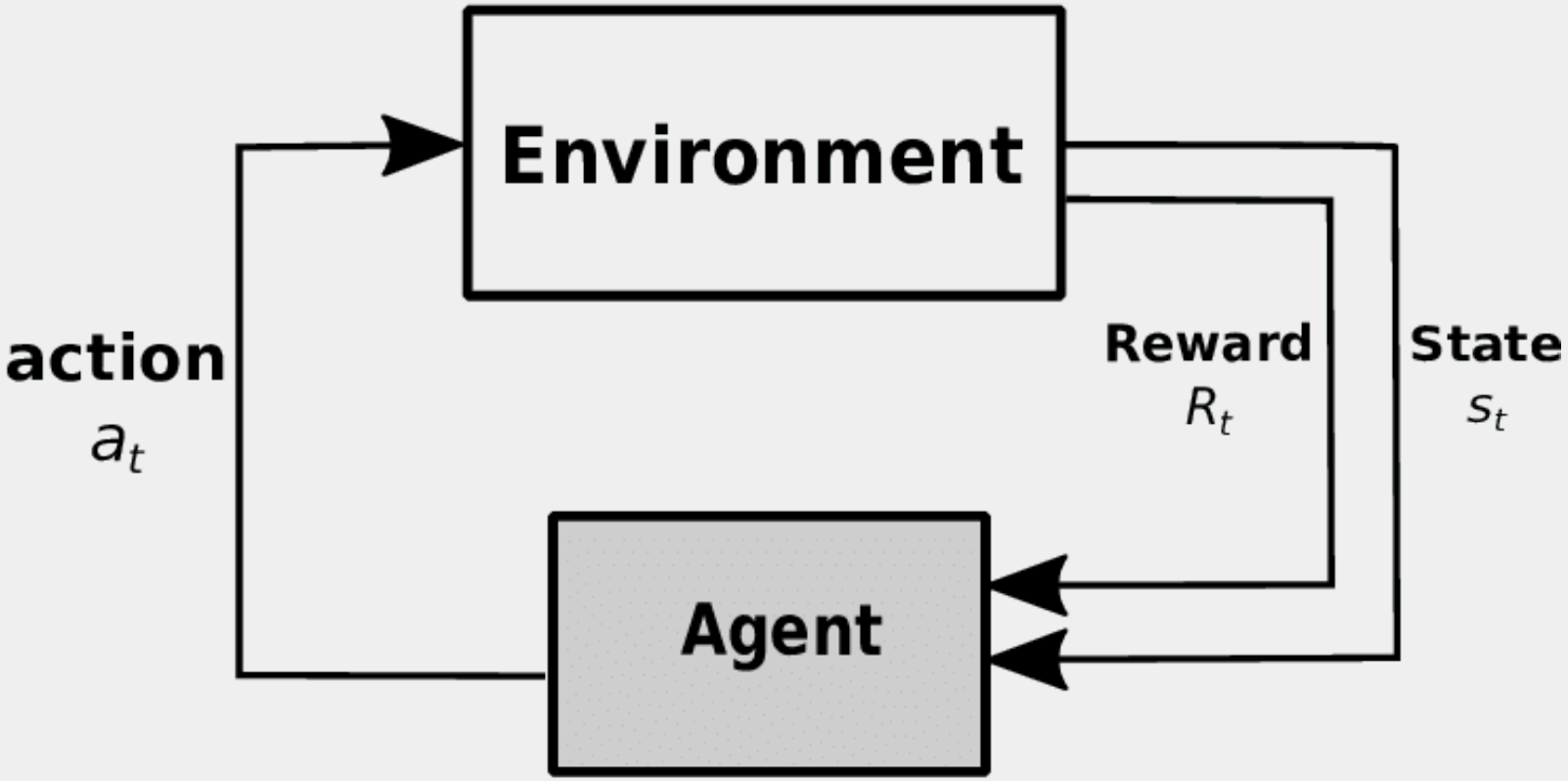
- Uses unlabelled data, hence “unsupervised”
- Tasks: clustering, generative models, ...

- Goal: discover hidden structures

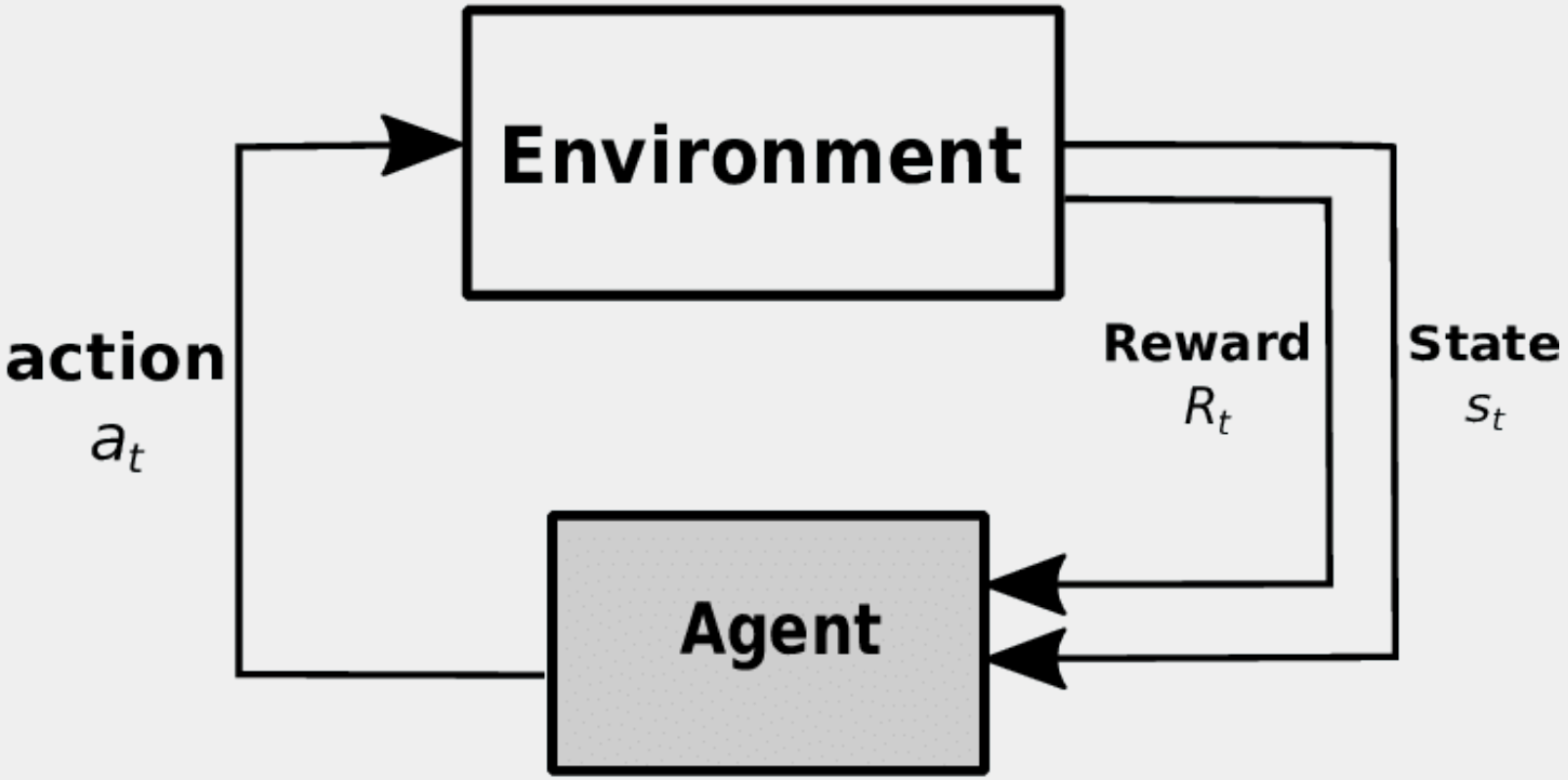


- Goal: generate synthetic data (image, sound, etc)

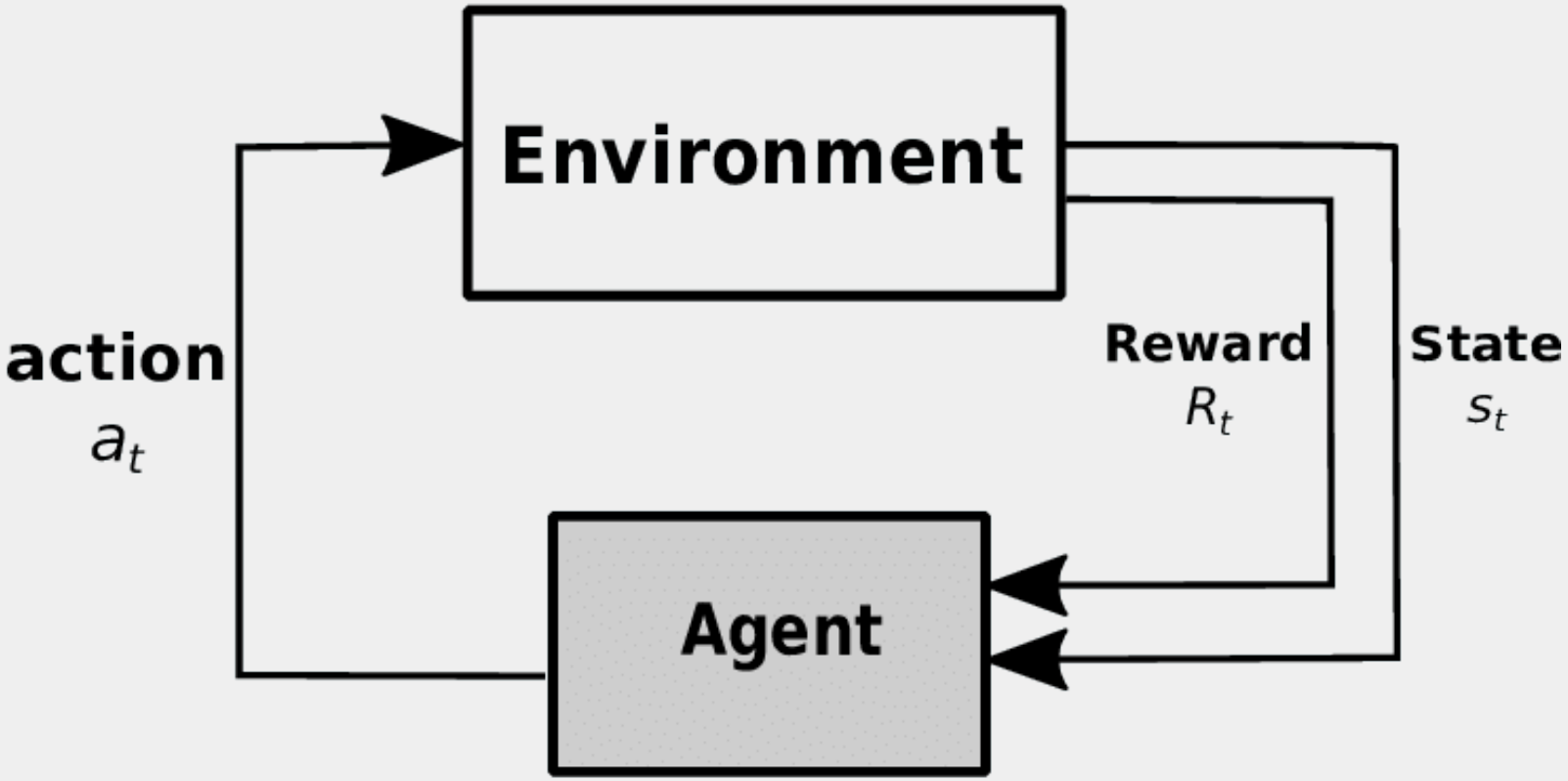
- Sequential decision making: interactions between Agent and Environment



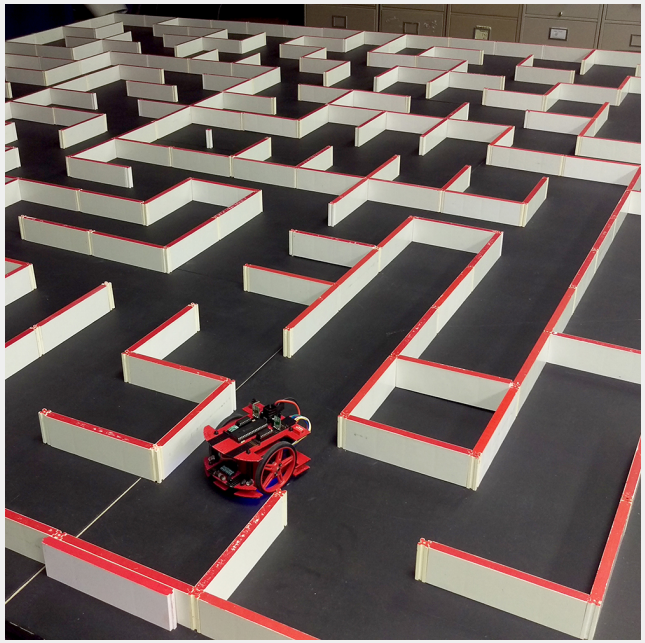
- Agent chooses an action to execute in the current state of Environment



- Environment provides reward to Agent and transits Agent to the next state



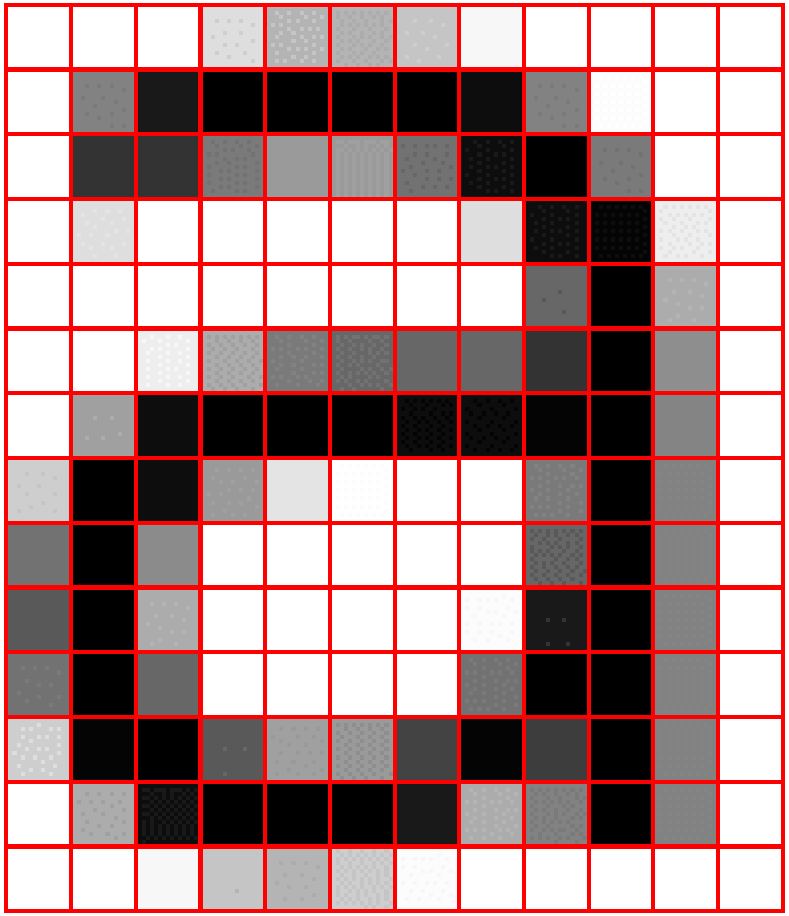
- Agent performs a sequence of actions, observes their "rewards," and learns an optimal policy
- E.g., Go, robot and maze, Atari game, etc.



- Supervised learning
  - Solve the recognition problem
  - Assume i.i.d. data
  - Cannot pass human performance (i.e., ground truth)
    - Although for ImageNet: human 5% error, best model 3.57% error
- Reinforcement learning
  - Solve the decision problem
  - Learn via trial and error, no explicit supervisor only indirect, delayed feedback
  - Action order (time) matters $\rightarrow$ non-i.i.d. data
    - E.g., autonomous driving via a front-facing camera (image at t affects action at $t+1$ then affects image at $t+1$)
  - Superhuman potential

Learning Pipeline

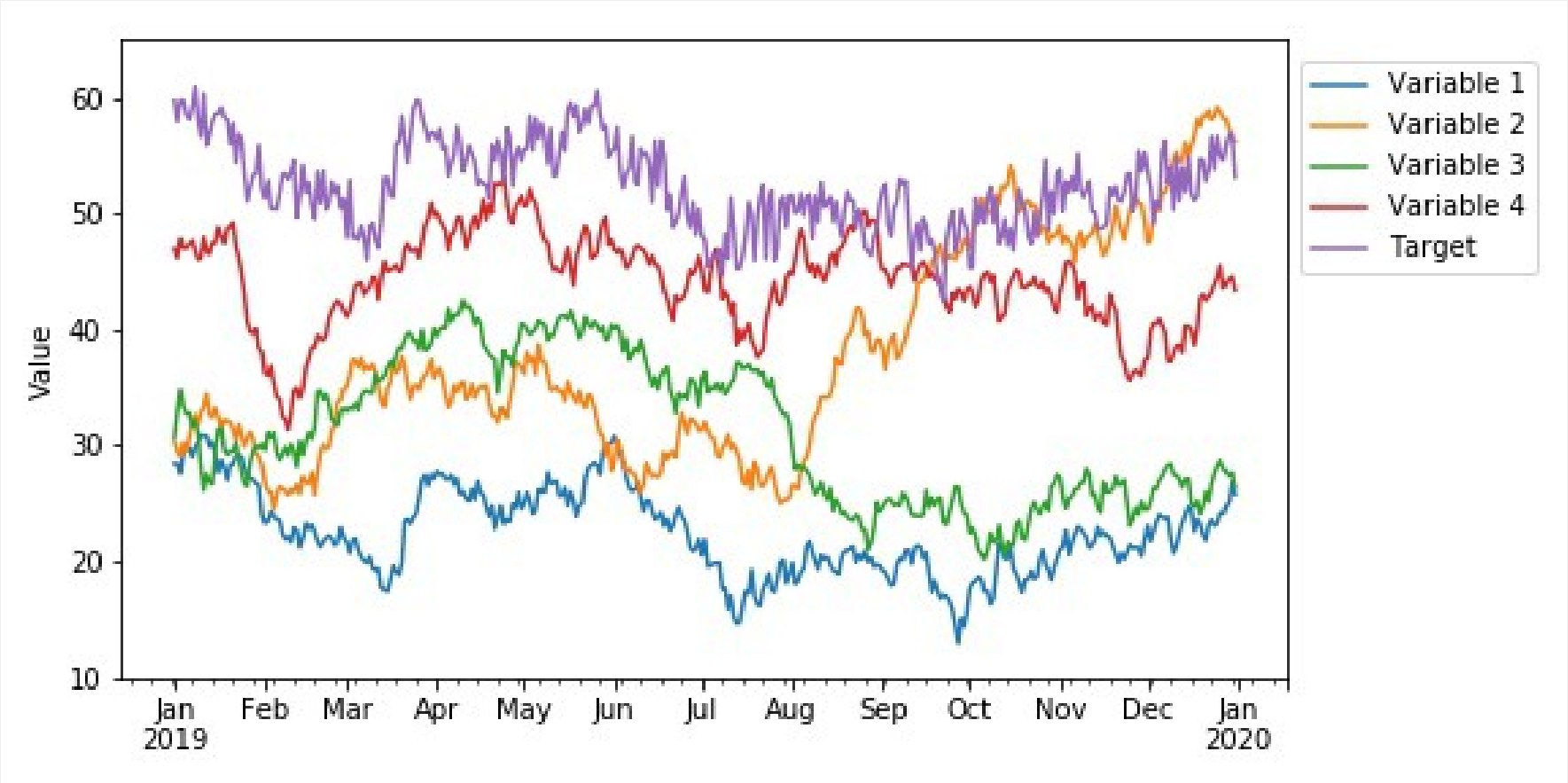
a



1.0	1.0	1.0	0.9	0.6	0.6	0.6	1.0	1.0	1.0	1.0	1.0
1.0	0.5	0.0	0.0	0.0	0.0	0.0	0.0	0.5	1.0	1.0	1.0
1.0	0.2	0.2	0.5	0.6	0.6	0.5	0.0	0.0	0.5	1.0	1.0
1.0	0.9	1.0	1.0	1.0	1.0	1.0	0.9	0.0	0.0	0.9	1.0
1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	0.5	0.0	0.5	1.0
1.0	1.0	1.0	0.5	0.5	0.5	0.5	0.5	0.4	0.0	0.5	1.0
1.0	0.4	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.5	1.0
0.9	0.0	0.0	0.6	1.0	1.0	1.0	1.0	0.5	0.0	0.5	1.0
0.5	0.0	0.6	1.0	1.0	1.0	1.0	1.0	0.5	0.0	0.5	1.0
0.5	0.0	0.7	1.0	1.0	1.0	1.0	1.0	0.0	0.0	0.5	1.0
0.6	0.0	0.6	1.0	1.0	1.0	1.0	0.5	0.0	0.0	0.5	1.0
0.9	0.1	0.0	0.6	0.7	0.7	0.5	0.0	0.5	0.0	0.5	1.0
1.0	0.7	0.1	0.0	0.0	0.0	0.1	0.9	0.8	0.0	0.5	1.0
1.0	1.0	1.0	0.8	0.8	0.9	1.0	1.0	1.0	1.0	1.0	1.0

- raw data $\rightarrow$ feature engineering via human experts $\rightarrow$ model training and tuning $\rightarrow$ outcome


Affenpinscher
Brussels Griffon
Cavalier King Charles Spaniel
Chihuahua
Chinese Crested
English Toy Spaniel
Havanese
Italian Greyhound
Japanese Chin
Maltese
Manchester Terrier
Miniature Pinscher
Papillon
Pekingese
Pomeranian
Pug
Shih Tzu
Silky Terrier
Toy Fox Terrier
Toy Poodle
Yorkshire Terrier


Value
60
50
40
30
20
10
Jan
2019
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
2020
Variable 1
Variable 2
Variable 3
Variable 4
Target

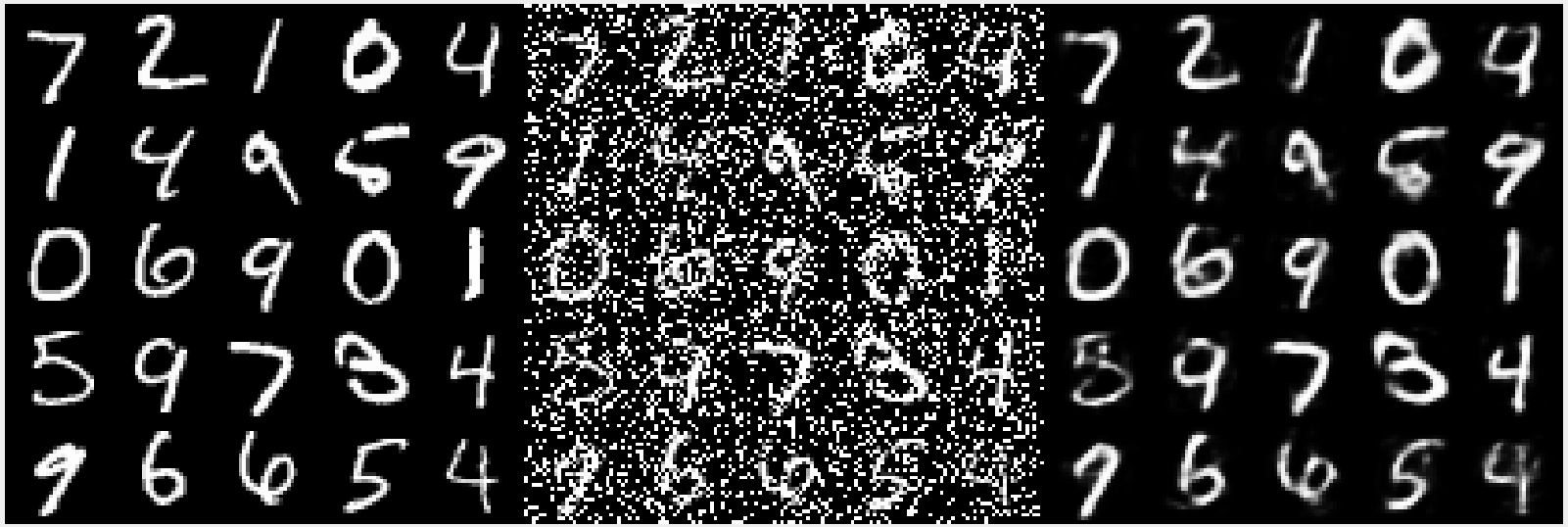
- raw data $\rightarrow$ model training and tuning $\rightarrow$ outcome (a.k.a. "end-to-end learning")

- Pros: easy to set-up, powerful (if works)

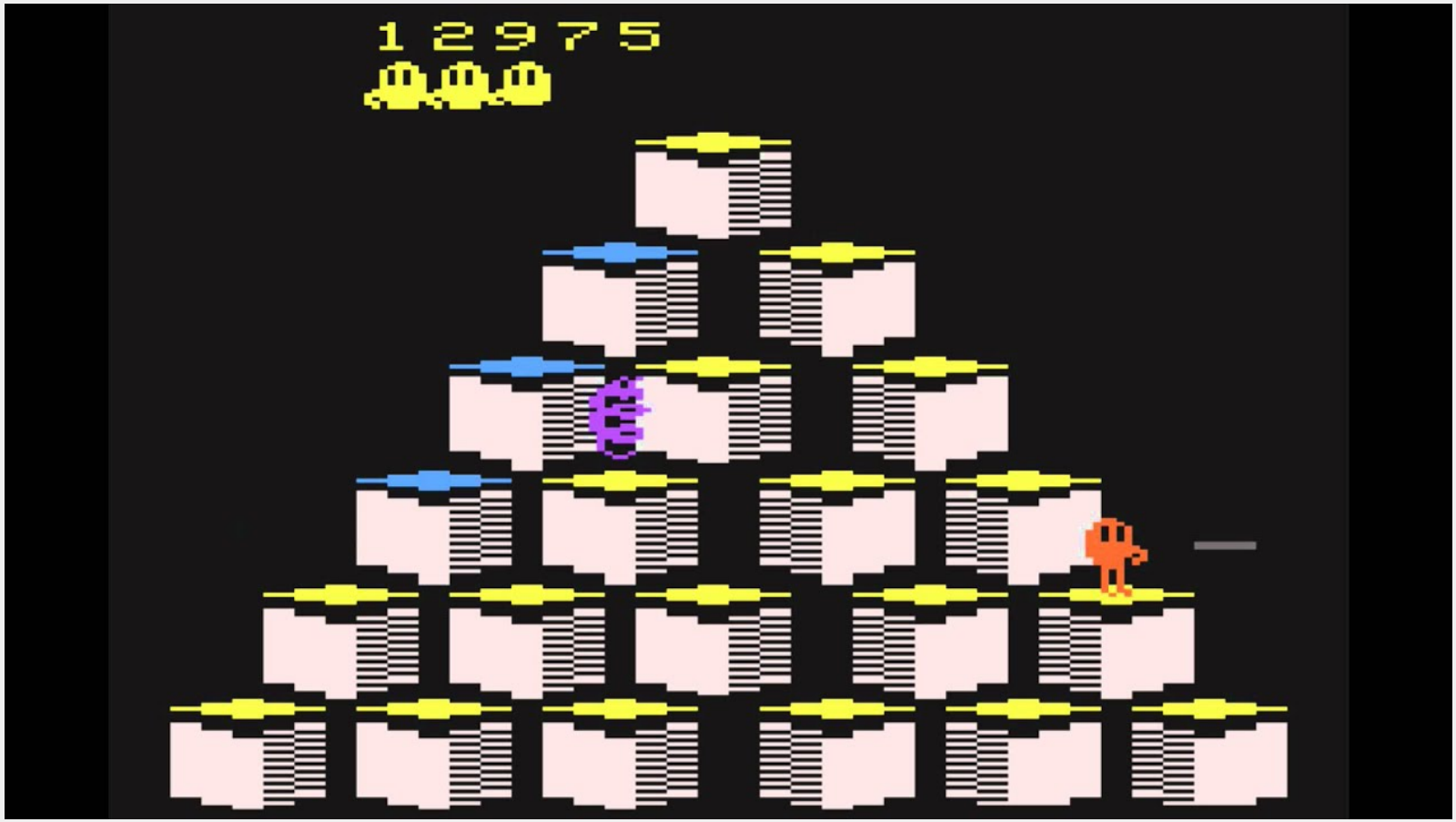
- Cons:
  - blackbox (no human-interpretable features)
  - difficult to defend adversarial attacks
  - data hungry
  - computation intensive
  - hyperparameter search is a pain

- Steering angle prediction = 90k images + 3080 (GPU) + 16 hours

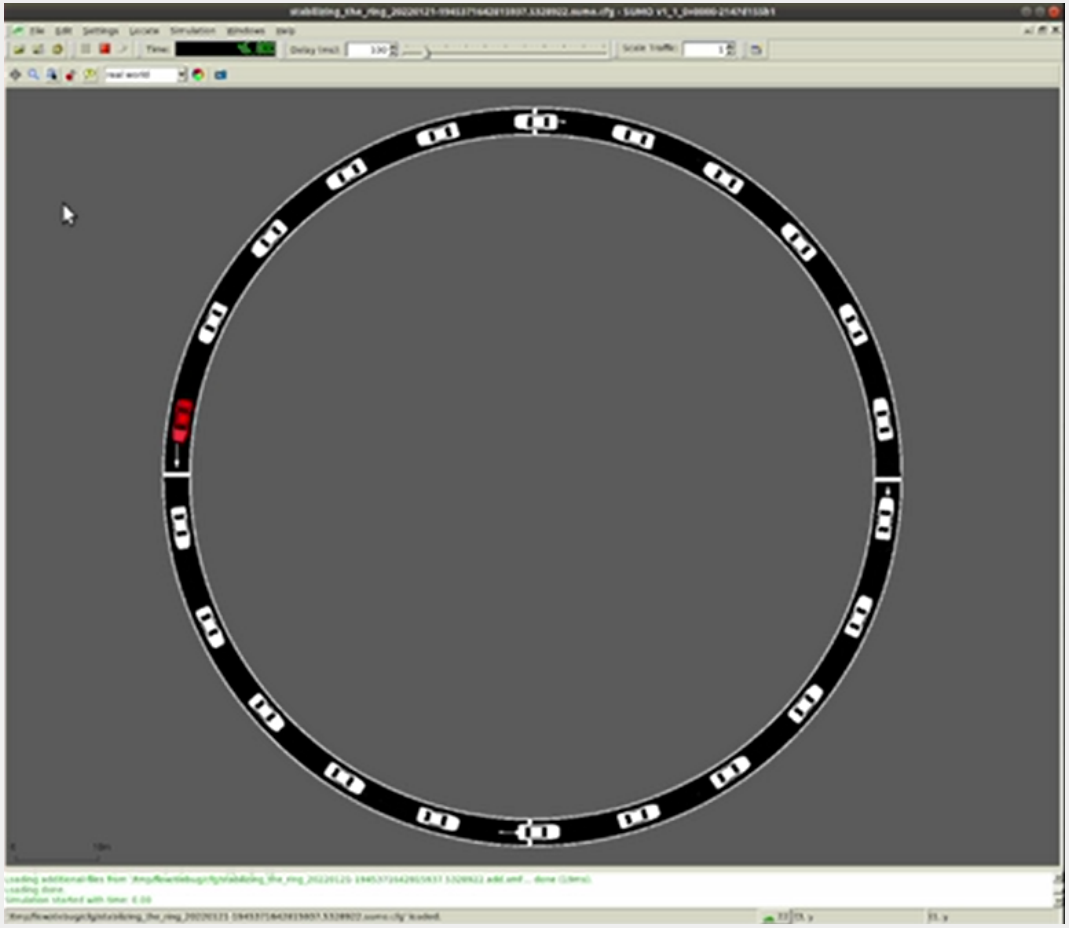
- De-noising Autoencoder: 75k images + 3080 (GPU) + 4 hours



- Q-bert: DQN (algorithm) + 3070 TI (GPU) + 2–3 hours



- Traffic on a ring: PPO (algorithm) + Intel core-i9 11900k (CPU) + 6 hours



- Pattern recognition (reporting in accuracy) $\rightarrow$ supervised learning
  - How to obtain (at least 20k) labelled data?
- Pattern discovery or generation (show the found or generated patterns) $\rightarrow$ unsupervised learning
  - How to obtain (at least 20k) pattern-specific data?
- Sequential decision making (show agent-environment interactions) $\rightarrow$ reinforcement learning
  - How to build the environment?
- computing resources required vs. computing resources possessed