最先端ソフトウェア工学ゼミ
AI・データ分析ゼミ

斉藤功樹、百足勇人、塚本啓太、宮城俊秀

アジェンダ

- ゼミでの目標・テーマ
  - 目標設定のための調査
  - 関連調査を受けた目標設定
- Convolutional Neural Network (CNN)
- Deep Q Network ～Q学習～
  - Q学習
  - Deep Q Network
- まとめ・所感

ゼミでの目標・テーマ

- 個別ゼミ1で行ったこと
  - 機械学習のライブラリの使い方
  - データの扱い方(欠損値など)
- 個別ゼミ2で行いたいことのアイディアを抽出

AIを使った結果でお客様を納得させる

AIによるテストデータの自動生成

従来のカバレッジに相当する指標

AIが出した答えが間違っている場合の直し方

AIのバグの定義

- 同時に以下のような問題が起こったことも議論
  - 画像分類のアプリで黒人をゴリラと認識
  - チャットボットが差別的な発言をする
- テーマ
  - 機械学習で生成されたモデルの品質保証についての考え方

目標設定のための調査

- まず以下のような内容を調査
  - AIが学習した結果に対しての攻撃手法に関する研究
  - ブラックボックステスト手法に関する研究
- 攻撃(間違わせる)手法の一例
- Adversarial examples
  - AIが正しく認識できている画像に対して摂動を与えることで、違う物体に認識させるような手法
  - 人間には元の画像との違いがほとんどわからない
  - 自動運転の際には標識に細工をすることで誤認識させる研究も出てきている

関連調査を受けた目標設定

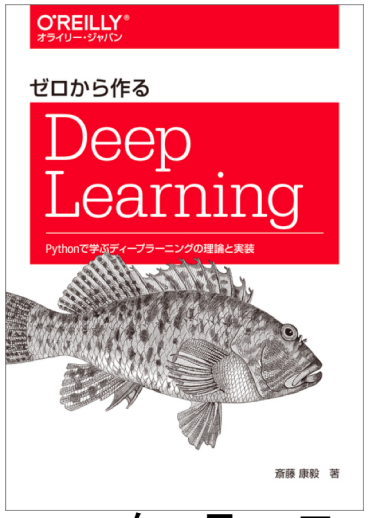
- AIの結果を保証する上で、どういった攻撃を受けるのか研究論文等から調査を実施
- しかしながら
  - モデルを作成する、Deep Learningの手法が理論的に理解できていない
  - そのため、攻撃手法を学んでも、モデル作成時に何を気をつける必要があるのか、実際の活用を行う上で必要な点が抜けていることがわかった
- そこで本ゼミで以下を実施
  - Deep Learningの手法を数学的に理解
  - 強化学習の手法及びDeep Learningと組み合わせたDQNの仕組みの理解
  - 上記について、実際にコードを書いて、学習手法の理解も深める

Convolutional Neural Network (CNN)

- Deep Neural Networkの一つ
  - 入出力層と隠れ層を持ち**非線形モデル**を構築

- 画像・動画認識，言語認識，レコメンドに応用

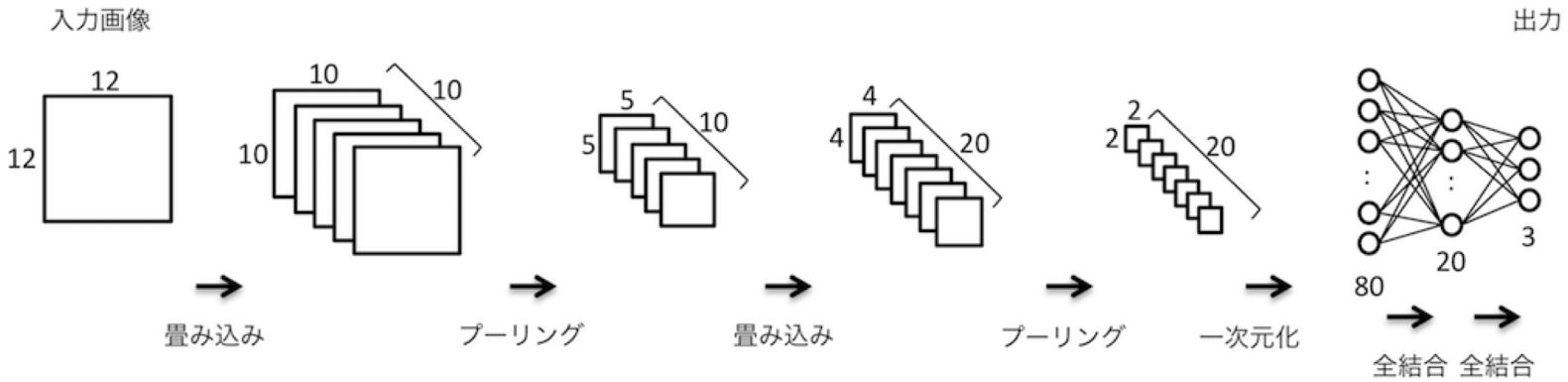
- Deep Learningを学ぶ題材としてCNNを採用



- ゼロから作るDeep Learning ——Pythonで学ぶディープラーニングの理論と実装
  - 斎藤 康毅 著，オライリー・ジャパン 出版
  - GitHub https://github.com/oreilly-japan/deep-learning-from-scratch

CNNの構成

構成：畳み込み層 + プーリング層 + 全結合層



https://qiita.com/eijian/items/06b1ba1276d1bfd77b93

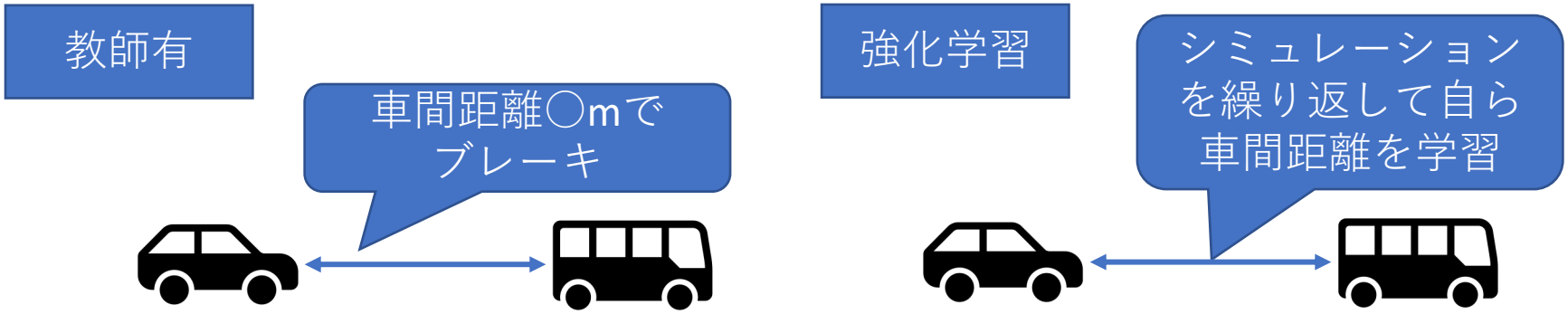
- 畳み込み層（Convolutional Layer）
  - フィルタをかけることで領域の特徴マップを生成する層
    - 画像内に含まれるパターンを検出する
- プーリング層（Pooling Layer）
  - 特徴マップから代表値（最大値，平均値）を算出する層
    - 抽出された特徴の位置感度を低下させる

CNNを通して学んだこと

- 誤差逆伝播法：
  微分式の計算を簡単な式の計算で代替
- 隠れ層：
  サイズ，数，層の深さ，プーリング方法
- 活性化関数：
  ステップ関数，シグモイド関数，ReLU
- パラメータ最適化手法：
  SGD，Momentum，AdaGrad，Adam
- 損失関数：
  2乗和誤差，交差エントロピー誤差

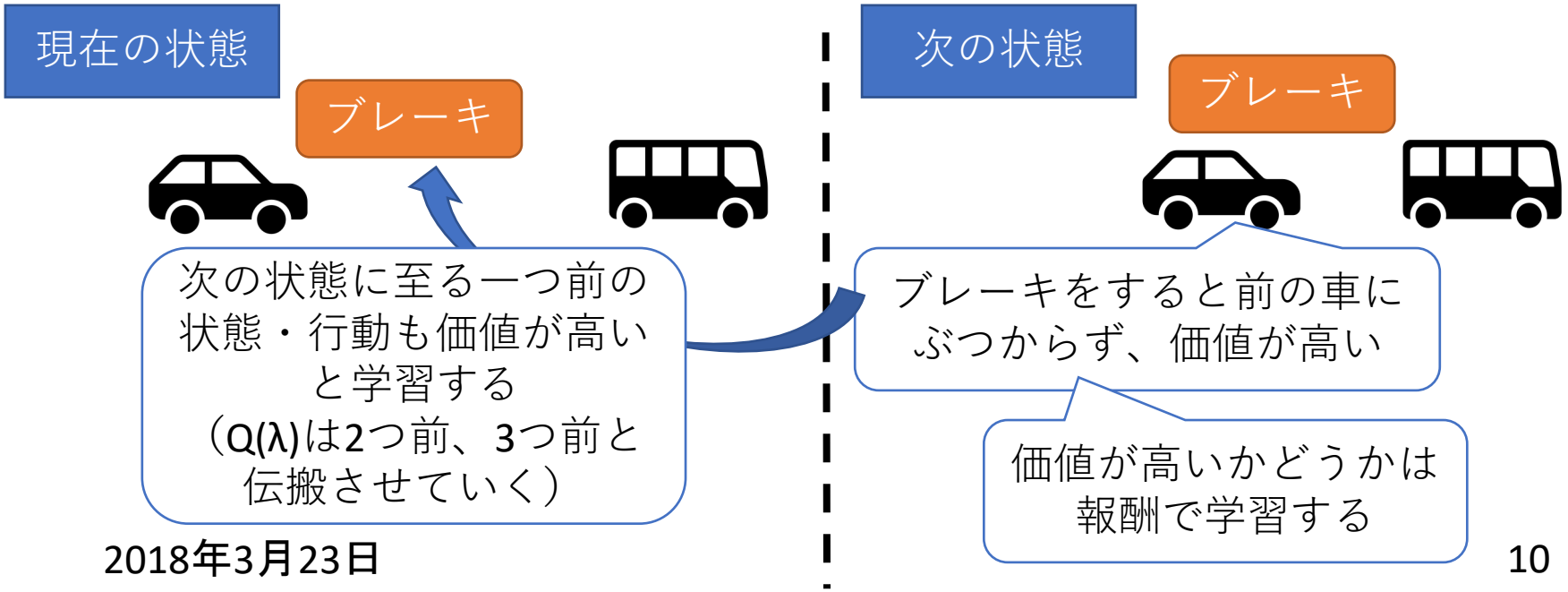
Deep Q Network ～Q学習～

- Q学習とは
  - 強化学習の一種
  - 強化学習とは
    - Wikipediaより
    - ある環境内におけるエージェントが、現在の状態を観測し、取るべき行動を決定する問題を扱う機械学習の一種
    - 強化学習は一連の行動を通じて報酬が最も多く得られるような方策(policy)を学習する
  - 例：AlphaGo、自動運転など
  - 自動運転で例えると



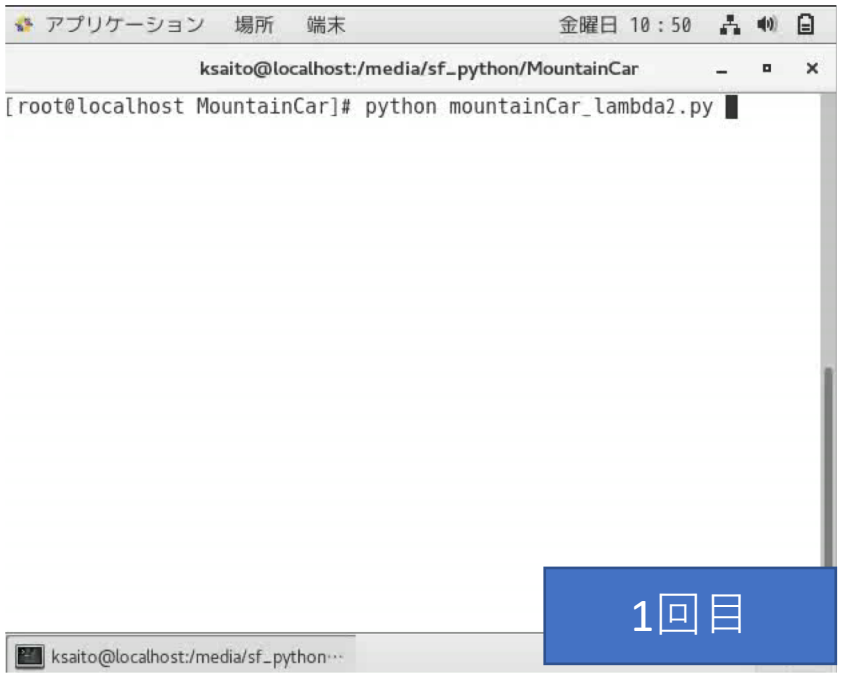
Deep Q Network ～Q学習～

- Q学習とは
  - 強化学習では、行動価値関数を学習によって求める
    - ある状態において、行動ごとに価値を与える
  - Q学習は、現在の状態から次の状態に移った際に、次の状態の中で最も行動価値関数の値が高い状態に近づけるように学習する
  - 何が価値が高いかは報酬を与えることで学習をする
  - 自動運転の例（イメージ）



Deep Q Network ～Q学習～

- MountainCar：車の山登り問題
  - パワー不足の車を使って山を登る問題
  - 状態：位置、速度
  - 行動：前進、何もしない、後退

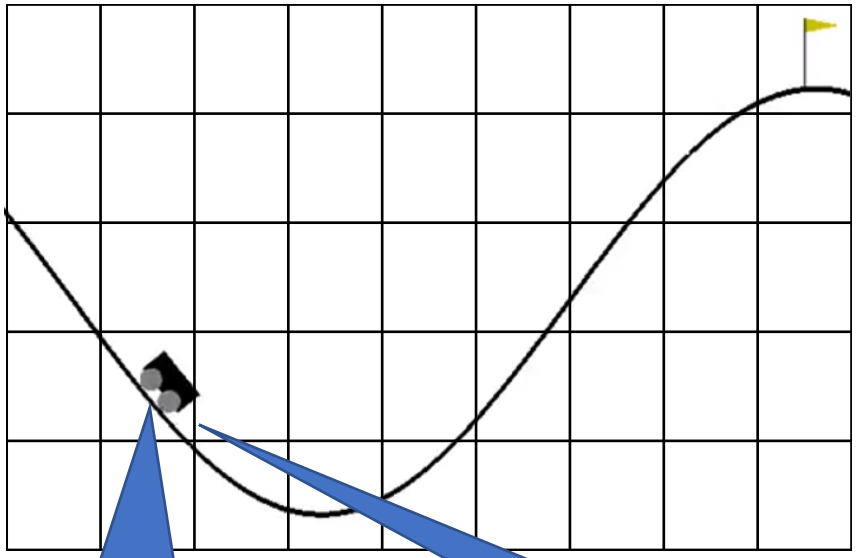


Deep Q Network ～Q学習～

- 課題
  - 状態を離散化する必要がある
    - 状態は基本的に連続値であるが、連続値だと計算量が膨大になるため、離散化して計算できるレベルにする必要がある
  - 報酬の与え方を工夫する必要がある
    - 報酬の与え方によっては学習が終わらないこともある
  - シミュレーションを繰り返す必要がある
    - MountainCarでも普通のQ学習だと500回前後、Q(λ)では200回前後

Q学習の課題

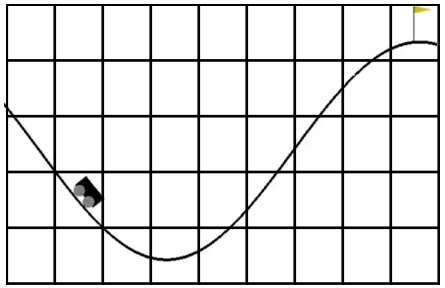
- 状態を離散化する必要がある
- 離散化が難しいものは？



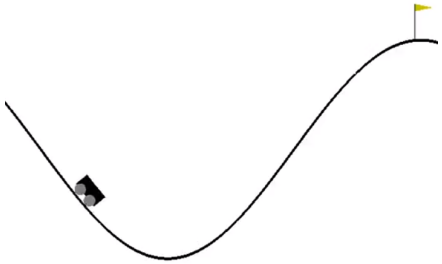
ビデオゲーム

実世界の映像

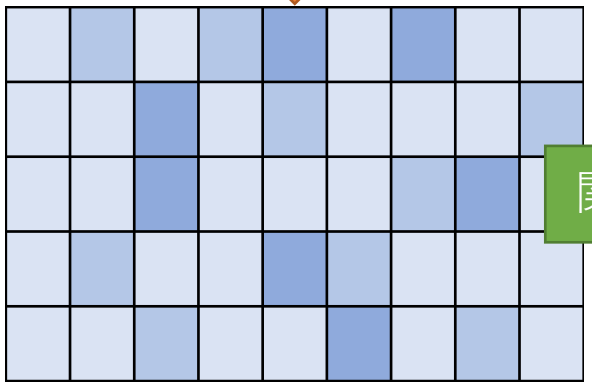
Deep Q Networkのアイデア



離散化した状態

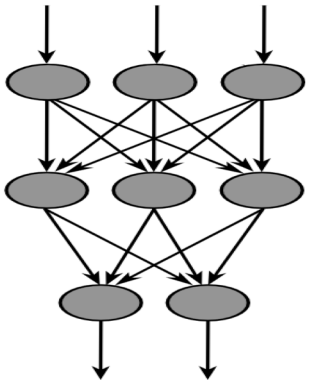


連続値のままの状態

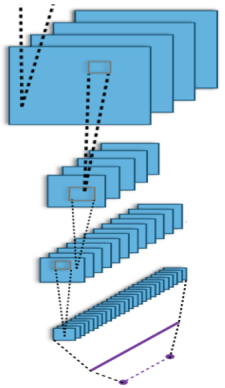


Q関数

関数近似



(ディープ)ニューラルネットワーク



後退	何もしない	前進
1	0	2

行動価値

後退	何もしない	前進
1	0	2

行動価値

←	止	→
1	0	2

Deep Q Networkによる学習時のコツ

- Experience Replay
  - データをそのまま学習すると時間方向の相関が強くなってしまうので、一旦メモリにおいてからランダムサンプリング
- Fixed Target Q-Network
  - ミニバッチ学習中が終わってからQ-Networkの重みを更新
- 報酬のクリッピング
  - 成功したら+1、失敗したら-1で報酬を固定
- 誤差関数のクリッピング
  - 二乗誤差の絶対値が1以下/以上のときで関数形を変える

まとめ（百足）

- 深層学習について、重みの更新の仕組みから具体的な利用方法まで、メンバーと議論しつつ学ぶことができ、ブラックボックスという印象が薄れた
- Adversarial Examplesなどの脆弱性も、学習の仕組みをついた攻撃のため、その仕組みを理解して対策を考えるアプローチも必要と感じた

まとめ（斉藤）

- Deep Learningの脆弱性を学ぶことができ、 AIの品質評価という観点での知見を得られた
- 強化学習とDQNについて、理論的な学習から実装まで経験でき、ディスカッションを通して実践的な知見を得られた

まとめ(宮城)

- Deep Learningについて、これまではライブラリにデータを入れて使っているだけだったが、パラメーターの更新の仕組みを議論するなかで、実際には何をしているかを理解できた
- 合わせてDeep Learningへの攻撃手法を学んだことで、活用する際に注意すべきポイントの知見を得られた

まとめ（塚本）

- Deep Learningの仕組みを知ることで,
  脆弱性（adversarial examples）への理解が深まった.
- 実用的なモデルを構築することの難しさを
  感じた.
- Deep LearningはGPUがないと手元で動かすのが
  非常に辛かった.