The 26th
Symposium on Sensing
via Image Information

SSII 2020

弱教師付き機械学習の新展開
～限られた情報からでも精度良く～

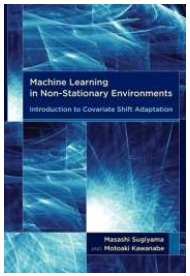
2020.6.10

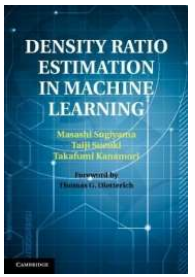
杉山 将 (理研 AIP／東京大学)

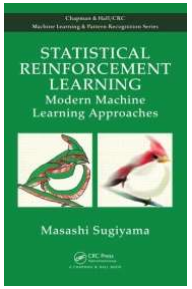
自己紹介

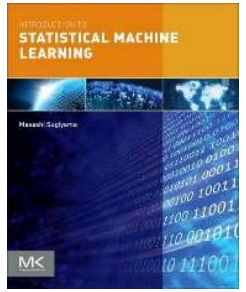
現職：

- 理化学研究所・センター長：研究者とともに
- 東京大学・教授：学生とともに
- 企業・技術顧問：エンジニアとともに



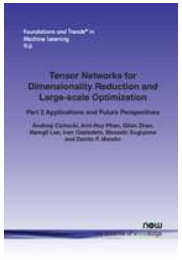


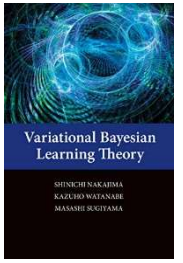


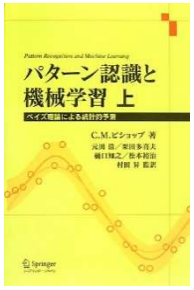


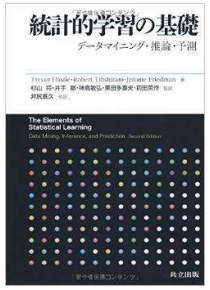
専門分野：

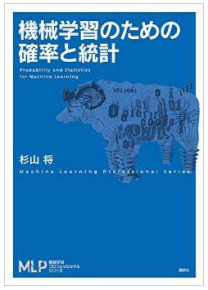
- 機械学習の数学的な基礎研究
  （コンピュータ科学，統計学など）
- 機械学習技術の実世界応用
  （画像，言語，脳波，ロボット，医療，生命など）











発表の流れ

1. 機械学習研究分野の動向
2. 理研AIPセンターの紹介
3. 最新の機械学習技術の紹介
4. まとめと今後の展望

人工知能

- 自動運転車，会話ロボット，コンピュータ囲碁など，私達の身の回りの様々な場面で人工知能が利用されはじめている

http://www.cnbc.com/2015/10/14/tesla-rolls-out-autopilot-technology.html

http://www.softbank.jp/corp/group/sbr/news/press/2014/20141029_01/

http://gigazine.net/news/20160317-google-alphago/

- これらの人工知能システムの背後では，コンピュータに人のような学習能力を身につけさせる機械学習の技術が用いられている

人工知能・機械学習分野の歴史

■ 人工知能（論理的）：
- 1960年代：
  記号処理，論理推論
- 1980年代：
  エキスパートシステム

■ ニューラルネット（脳型）：
- 1960年代：
  パーセプトロン（1層）
- 1990年代：
  誤差逆伝播法（多層）

■ 機械学習（統計的）：
- 2000年代：統計・凸最適化，ベイズ推論
- 2010年代：深層学習

■ 次世代知能（将来）：
- 知能の要素技術を更に高度化
- 知能の要素技術を統合した高度な推論

機械学習分野の国際会議

- ICML: International Conference on Machine Learning（1980年から）
  - データからの学習に関する会議
  - 2000年頃からは統計的な機械学習に関する最難会議

- NeurIPS: Neural Information Processing Systems（1987年から）
  - もともとは神経情報処理システム（脳型の人工知能）に関する国際会議
  - 2000年頃からは，統計的な機械学習理論に関する最難関国際会議
  - 神経科学のセッションがあるのがICMLとの違い

ICML, NeurIPSのこれまでの動向

- 参加者数，論文投稿数が激増：

ICML	2013	2014	2015	2016	2017	2018	2019	2020
参加者数	900	1200	1600	3000+	2400	5000	6200	???
論文投稿数	1204	1238	1037	1327	1701	2473	3424	4990
論文採択数	283	310	270	322	433	618	773	1088

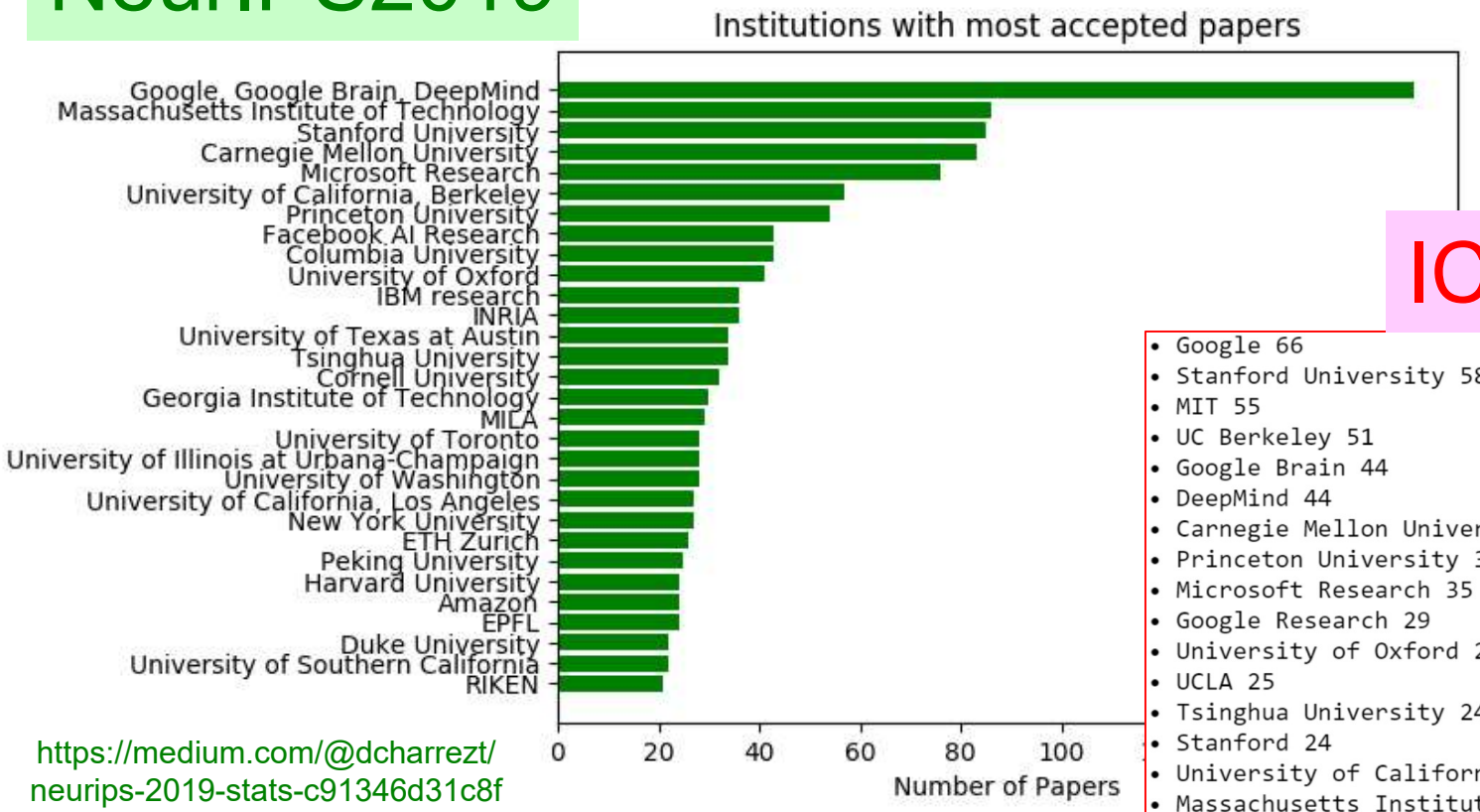
NeurIPS	2013	2014	2015	2016	2017	2018	2019	2020
参加者数	1200	2400	3800	6000+	7500+	8000+	13000+	???
論文投稿数	1420	1678	1838	2500	3240	4856	6743	10000?
論文採択数	360	414	403	568	678	1011	1428	???

- 企業のスポンサーも非常に活発：
  - 2000年代前半：アメリカの大手IT企業
  - 2000年代後半：世界中の大手IT企業
  - 2010年代：非ITを含む様々な業種のスタートアップ～大企業

ICML, NeurIPSの最近の動向

- ICML, NeurIPSとも北米のIT企業・大学が独占

NeurIPS2019



https://medium.com/@dcharrezt/neurips-2019-stats-c91346d31c8f

ICML2020

- Google 66
- Stanford University 58
- MIT 55
- UC Berkeley 51
- Google Brain 44
- DeepMind 44
- Carnegie Mellon University 37
- Princeton University 35
- Microsoft Research 35
- Google Research 29
- University of Oxford 25
- UCLA 25
- Tsinghua University 24
- Stanford 24
- University of California, Berkeley 22
- Massachusetts Institute of Technology 22
- Harvard University 21
- Duke University 21
- University of Washington 20
- University of Pennsylvania 20
- Facebook AI Research 20
- Cornell University 20

https://twitter.com/SergeyI49013776/status/1267768532529557504

・ RIKEN 18

NeurIPS2015と2019の比較

- 論文投稿数，参加者数とも激増：
  - 日本の論文採択数は増加，割合2~3%程度で大きな変化なし
  - 競争が激化する中，日本は一定のプレゼンスを維持できている
- 2015年：機械学習技術そのものの議論が中心
  - アルファ碁，自動運転車，会話ロボットなどが登場し，技術のさらなる発展への期待が高まる
  - 研究，ビジネスとも，北米の企業，大学が支配的
- 2019年：機械学習の技術開発競争が激化するとともに，機械学習を取り巻く環境に関する議論が活性化
  - 機械学習の他の科学分野への応用
  - 公平性などの社会課題への取り組み
  - 米中の企業の競争が激化
  - マイノリティの支援など多様性の重視へ

発表の流れ

1. 機械学習研究分野の動向
2. 理研AIPセンターの紹介
3. 最新の機械学習技術の紹介
4. まとめと今後の展望

理化学研究所
革新知能統合研究(AIP)センター

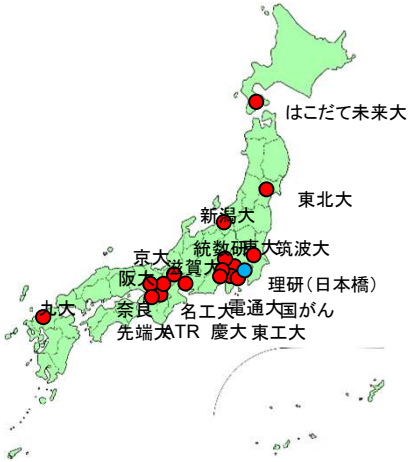
- 文科省のAIPプロジェクト(2016～2025年度)を推進する研究組織:

1. 次世代基盤技術開発(機械学習アルゴリズム, 深層学習の理論, 最適化理論, 基礎数理)
2. サイエンスを発達(再生医療, がん, 遺伝, 材料, 脳)
3. 社会実装に貢献(自然災害, インフラ管理, 高齢者ヘルスケア, 観光)
4. 倫理・社会的課題への対応(AI倫理, 法制度, 人間とAIのインタラクション, プライバシーとデータ流通)
5. 人材育成(国内外の学生, 企業のエンジニア)

研究組織

- **理論・応用・社会の3研究グループ**：
  - 44チーム，常勤研究員150名
- **国内大学・研究所の研究者・学生**：
  - 300人の客員研究員，150人の学生
- **産業界の研究者・エンジニア**：
  - 4連携センター，40企業と共同研究
- **海外の大学・研究所の研究者・学生**：
  - 米・加・英・独・仏・中・韓・豪・以などの40以上の組織とMOU，のべ150名のインターン

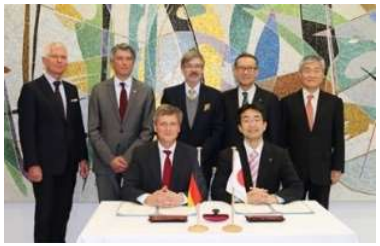
日本橋を中心に，
全国各地に組織を展開



企業との連携センター

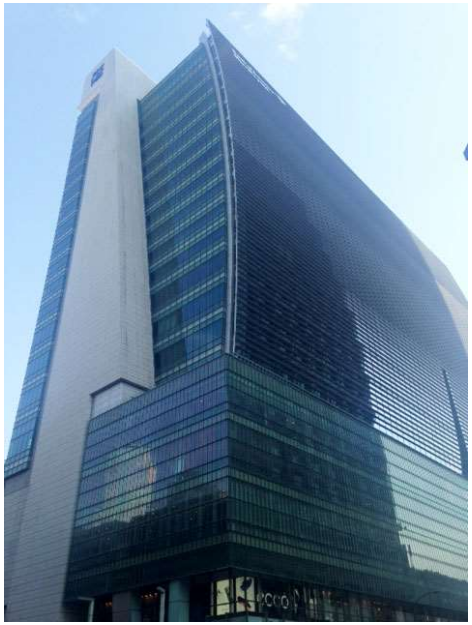
NEC　FUJITSU

TOSHIBA　FUJIFILM



AIPセンターの研究拠点

- オフィスは日本橋駅直結
- 国・産学官の垣根を超えた情報交換スペースを設置
  - お近くに起こしの際はお立ち寄りください！
- GPUクラスタRAIDEN所有



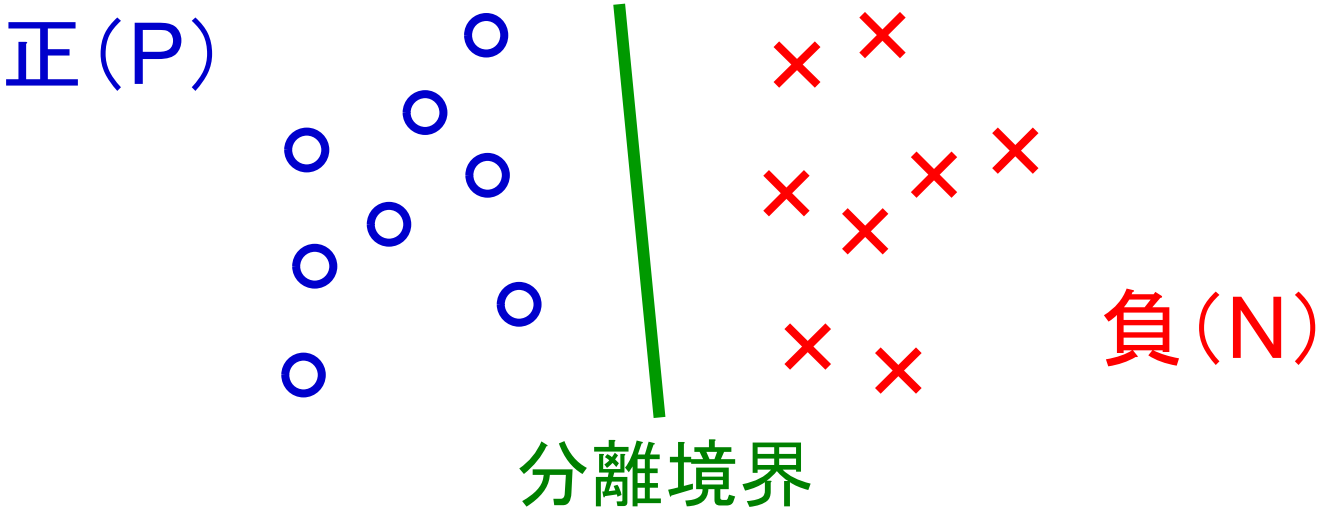
発表の流れ

1. 機械学習研究分野の動向
2. 理研AIPセンターの紹介
3. 最新の機械学習技術の紹介
   - A) 弱教師付き機械学習
   - B) ロバスト機械学習
4. まとめと今後の展望

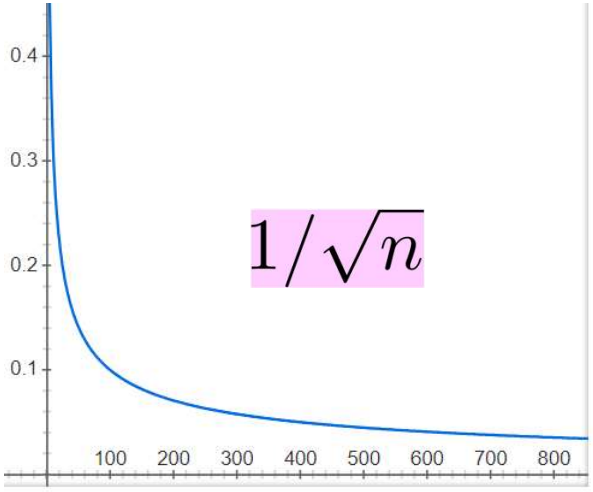
限られた情報からの機械学習

- 良質なビッグデータがあれば，現在の機械学習技術によってヒトを超える性能が達成できる:
  - 画像理解，音声認識，言語翻訳，商品推薦．．．
- しかし，応用分野によっては，良質なビッグデータが簡単に取れない
  - 医療データ解析
  - インフラの管理
  - 自然災害の防災・減災
  - 機能材料の開発
- 限られた情報からの学習が重要！

2クラスの教師付き分類

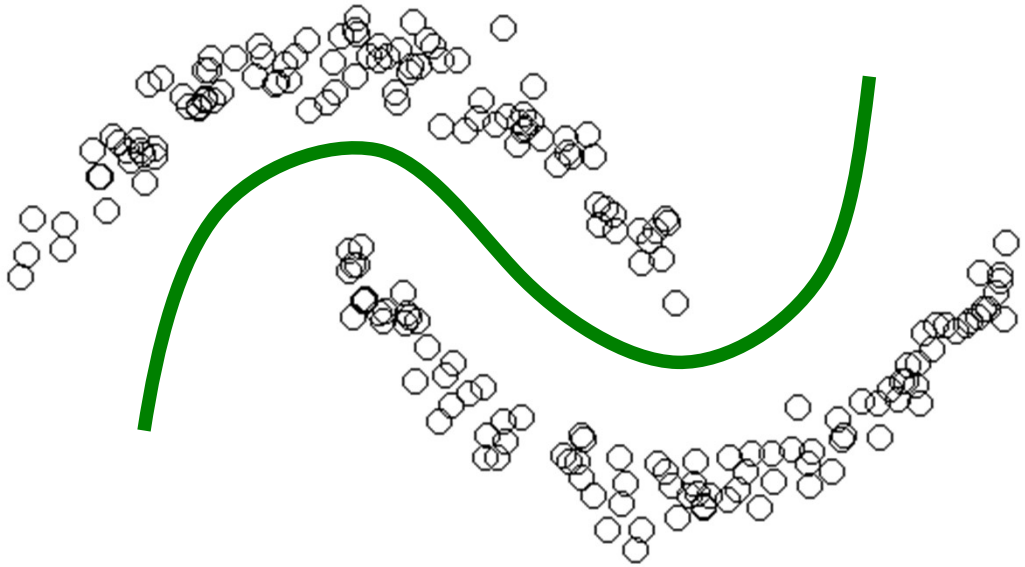


- 大量のラベル付きデータを用いれば，精度良く分類境界が学習できる
- ラベル付きデータ数nに対して，分離境界の推定誤差は $1/\sqrt{n}$ の速さで減っていく



教師なし分類

- ラベル付きデータの収集にはコストがかかるため，容易に入手できるラベルなしデータを用いる



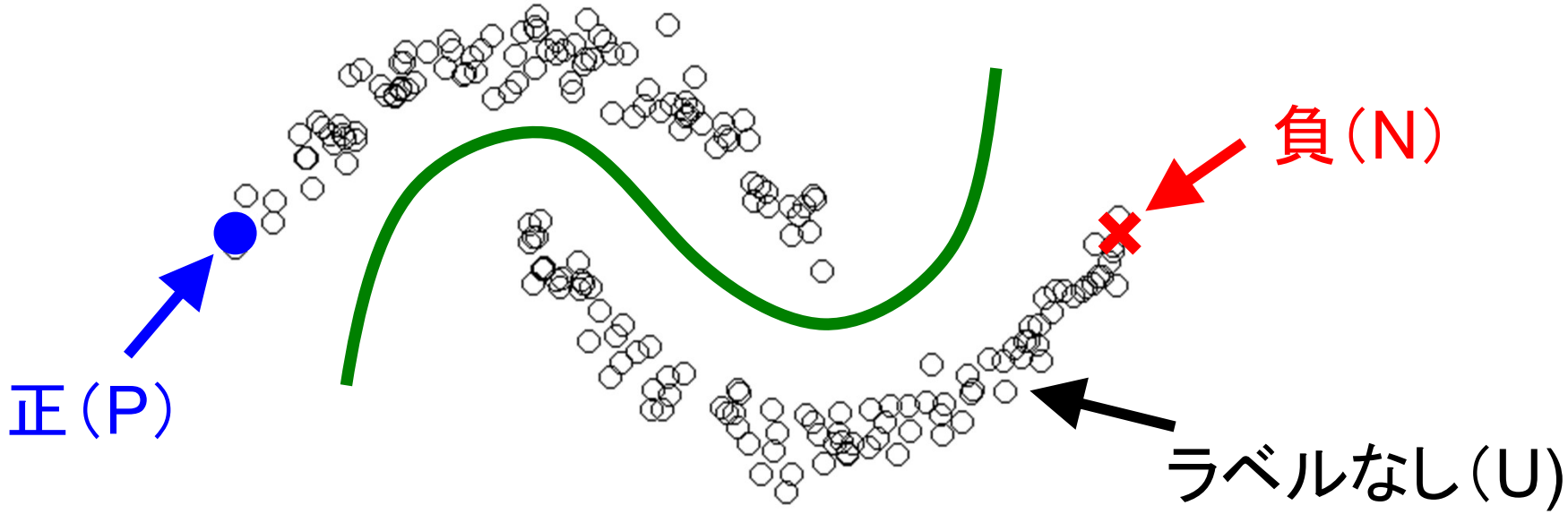
ラベルなし（U）

- 教師なし分類はただのクラスタリングに過ぎない
- データがクラス毎にクラスタに分かれていないと，正しく分類できない

半教師付き分類

Chapelle, Schölkopf & Zien (MIT Press 2006) and many

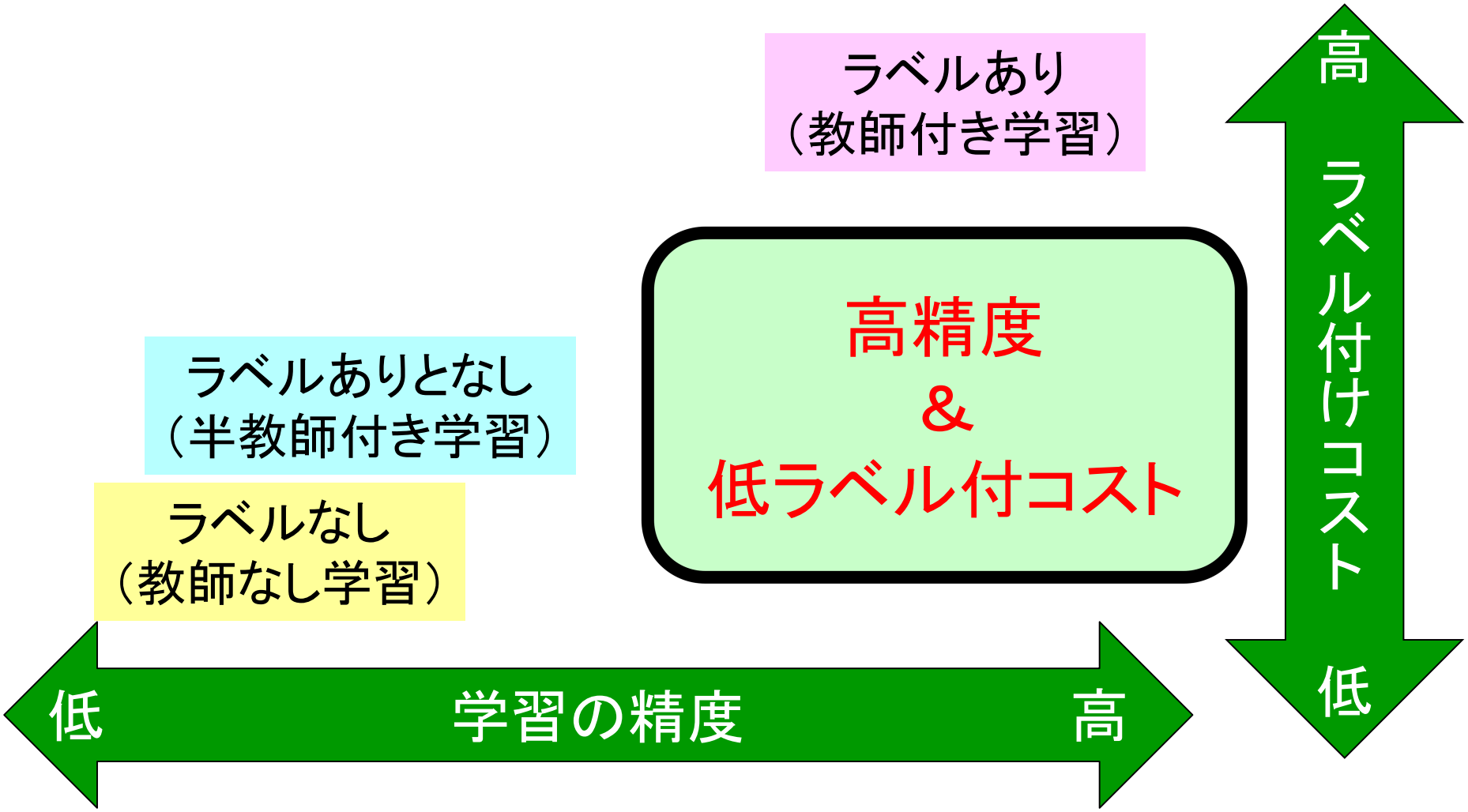
- ラベル付きデータとラベルなしデータ両方を活用
- ラベルなしデータがなすクラスタ構造に従って分類



- 同じクラスタに属するデータが同じラベルを持つとき，うまく分類できる
- そのような仮定が常に成り立つとは限らない

分類問題の分類

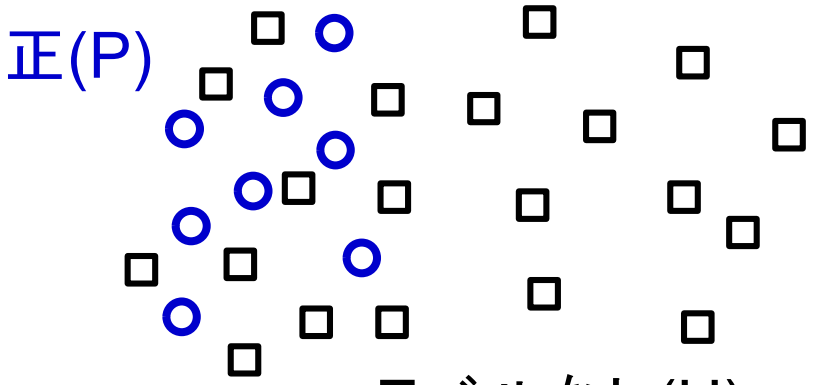
- 高精度でラベル付コストの低い分類手法が重要！



(1)PU分類

du Plessis, Niu & Sugiyama (NIPS2014, ICML2015)
Niu, du Plessis, Sakai, Ma & Sugiyama (NIPS2016)
Kiryo, du Plessis, Niu & Sugiyama (NIPS2017)
Hsieh, Niu & Sugiyama (ICML2019)

- 負例を集めるのが大変:
  - クリック vs. 非クリック
  - 友達 vs. 非友達

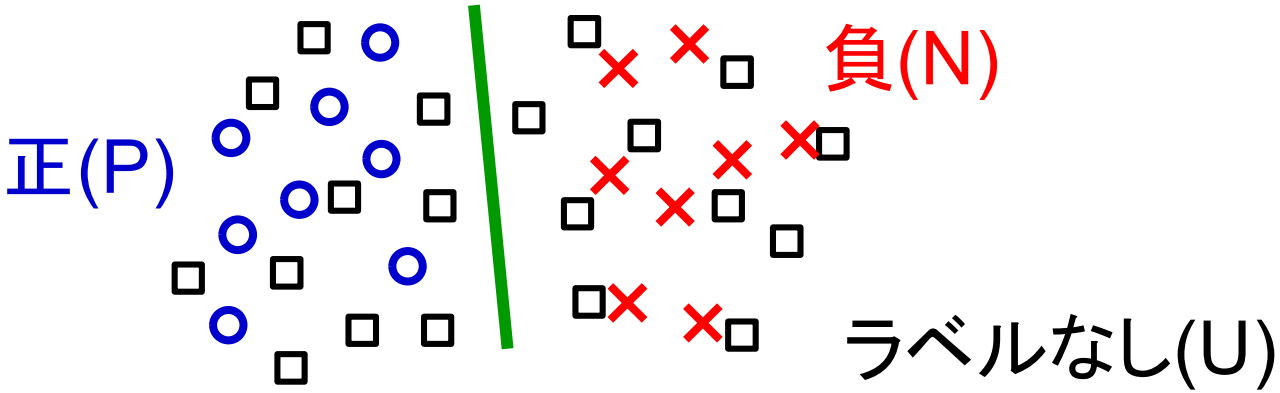


- 正例とラベルなしデータだけから，最適な分類ができる:
  - Uを雑音がのったNとみなして，PとUを分ける
  - Uの雑音を補正する

$1/\sqrt{n}$

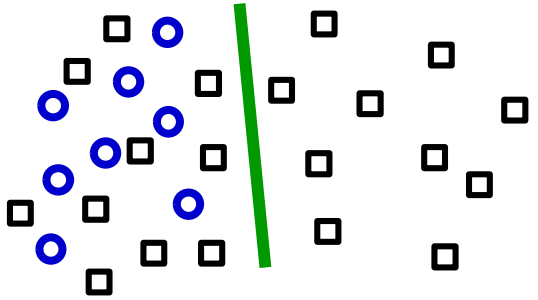
(2)PNU分類

Sakai, du Plessis, Niu & Sugiyama (ICML2017)
Sakai, Niu & Sugiyama (MLJ2018)

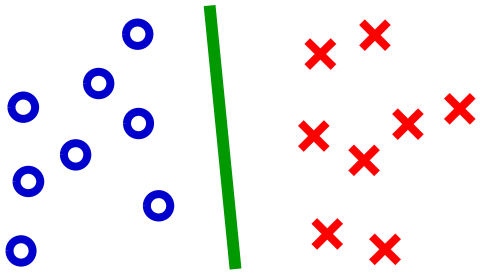


- 分解した3つの問題はそれぞれ最適に解ける:
  - それらの学習規準を組み合わせても最適 $1/\sqrt{n}$

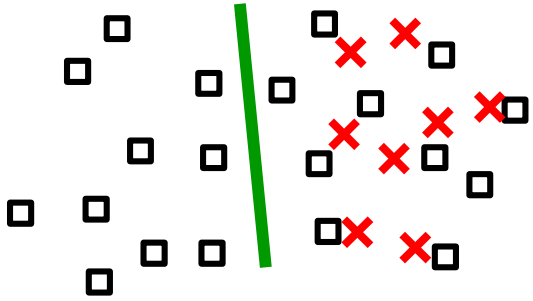
正とラベルなし



正と負



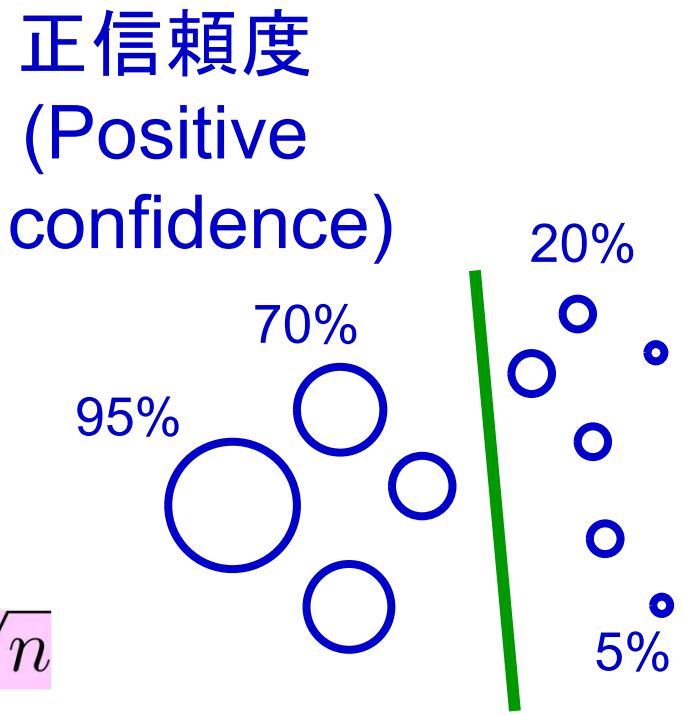
負とラベルなし



（3）Pconf分類

Ishida, Niu & Sugiyama (NeurIPS2018)

- 正クラスのデータしか取れない:
  - 他社のデータは取れず自社のデータしか取れない
  - 成功例は入手できても失敗例は入手できない
- 信頼度さえ分かれば,
  最適な分類ができる:
  - PconfからNconfを生成:
    確率rで正 → 確率(1-r)で負
  - PとUの分布の違いを
    重点サンプリングで補正



$1/\sqrt{n}$

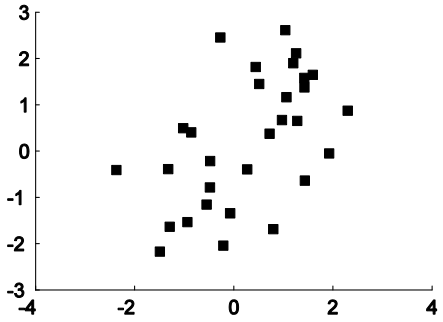
(4)UU分類

du Plessis, Niu & Sugiyama (TAAI2013)
Lu, Niu, Menon & Sugiyama (ICLR2019)
Charoenphakdee, Lee & Sugiyama (ICML2019)
Lu, Zhang, Niu & Sugiyama (AISTATS2020)

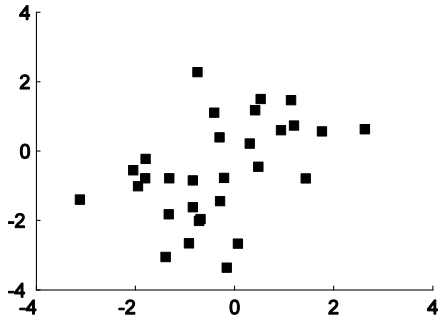
- 完全に教師なしでも，クラス比の異なるラベルなしデータが2セットあれば，最適な分類ができる：

$1/\sqrt{n}$

クラス比=4:6



クラス比=7:3



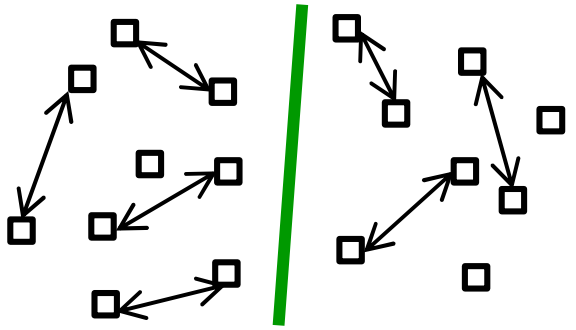
  - PU分類では，Uを雑音がのったNとみなして雑音補正
  - UU分類では，Pにも雑音がのっている

（5）SU分類

Bao, Niu & Sugiyama (ICML2018)

- 財産，宗教，政治など，デリケートな質問に対して，明示的に趣向を回答するのははばかられる
  - 「あの人と同じ」であれば回答しやすい！
- 類似データ対とラベルなしデータだけから，最適な分類ができる
  - SをばらすとU→UU分類

類似(similar)

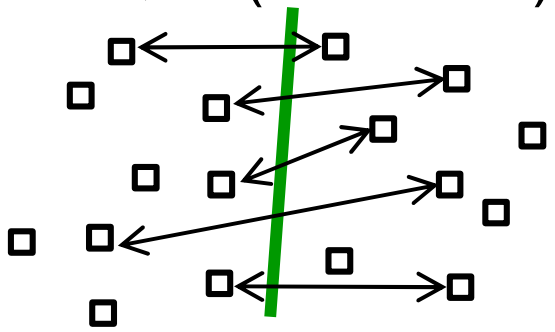


$1/\sqrt{n}$

- 非類似データ対からでも分類できる
  - PNU分類と同様に，SU, DU, SDを組み合わせたSDU分類も可能

Shimada, Bao, Sato & Sugiyama (arXiv2019)
Dan, Bao & Sugiyama (arXiv2020)

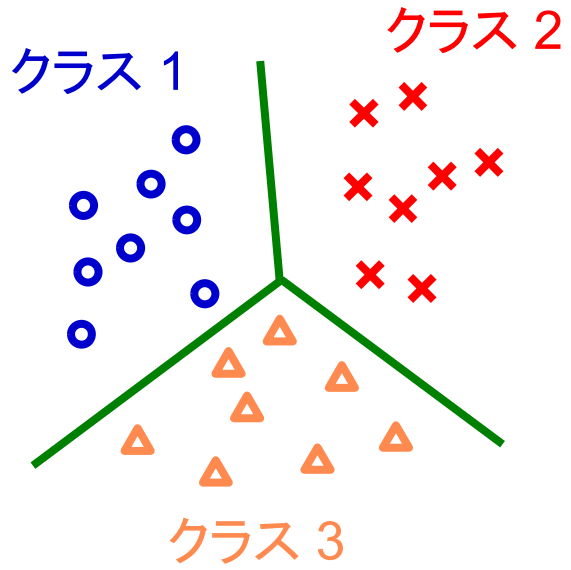
非類似(dissimilar)



（6）捕ラベル分類

Ishida, Niu & Sugiyama (NIPS2017)
Ishida, Niu, Menon & Sugiyama (ICML2019)
Feng, Kaneko, Han, Niu, An & Sugiyama (ICML2020)
Chou, Niu, Lin & Sugiyama (ICML2020)

- 多クラスの訓練データのラベル付けは高コスト
  - 多数の候補クラスから正しいものを選ぶ必要がある
- 補ラベル：パターンが属さないクラスのラベル
  - 「クラス1でない」
  - 補ラベルをつけるのは低コスト
- 捕ラベルだけから，
  最適な分類ができる：$1/\sqrt{n}$
  - 必ずラベルを間違える
    雑音を考えて，雑音補正

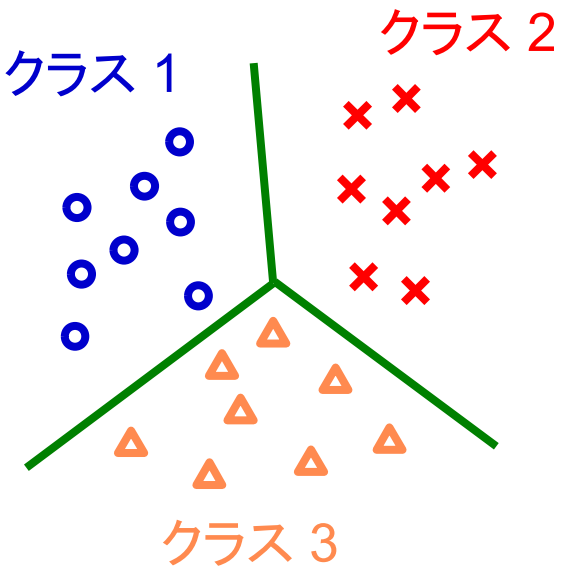


（7）部分ラベル分類

- 多クラスの訓練データのラベル付けは高コスト
  - 多数の候補クラスから正しいものを選ぶ必要がある
- 部分ラベル：Nguyen and Caruana (KDD2008)
  - 「クラス１か２」
  - 部分ラベルをつけるのは低コスト
- 部分ラベルだけから，
  最適な分類ができる：$1/\sqrt{n}$
  - 正しいラベルを逐次的に探索

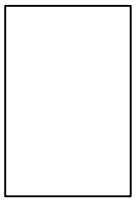
    Lv, Xu, Feng, Niu, Geng & Sugiyama (ICML2020)
  - データ生成モデルの明示的な定式化

    Feng, Lv, Han, Xu, Niu, Geng, An & Sugiyama (submitted)



弱教師付き学習のまとめ

- 紹介したすべての手法は，
  分類誤差を弱教師データから（不偏）推定：
  - あらゆる弱教師データを組み合わせられる
- 任意のモデル，損失，正則化に適用可能：
  - 理論解析は線形モデル，実応用は深層モデル
  - ロバスト損失や凸損失など自在に選べる
  - スパース化やデータ拡張も容易
- 書籍：Sugiyama, Sakai, Ishida, Nan, Bao & Niu
  Machine Learning from Weak Supervision,
  MIT Press, 2020?



- 生成モデルアプローチも可能：

Zhang, Charoenphakdee & Sugiyama (arXiv2019)
Zhang, Charoenphakdee, Wu & Sugiyama (arXiv2020)

発表の流れ

1. 機械学習研究分野の動向
2. 理研AIPセンターの紹介
3. 最新の機械学習技術の紹介
   - A) 弱教師付き機械学習
   - B) ロバスト機械学習
4. まとめと今後の展望

ロバスト機械学習

- 雑音・攻撃・不確定性に対する耐性が重要:
  - センサー誤差，ヒューマンエラー，敵対的攻撃，環境変化，標本化バイアス，．．．
- 従来のアプローチ:
  - 教師なし異常除去:なかなかうまくいかない
  - ロバスト損失，正則化:それほどロバストでない
- 研究の観点:
  - 訓練データの出力雑音:ラベル誤差
  - 訓練データのバイアス:転移学習
  - テストデータの入力雑音:敵対的攻撃

訓練データの出力雑音（1）

- 雑音遷移行列T：
  - ラベルがyからy’へ変わる確率p(y’|y)

$$T = \begin{array}{c} \\ y \end{array} \begin{array}{c} y' \\ \begin{array}{|c|c|c|} \hline 1 & 0 & 0 \\ \hline 0.1 & 0.8 & 0.1 \\ \hline 0.5 & 0.5 & 0 \\ \hline \end{array} \end{array}$$

- 損失をT^{-1}で補正すればよい：(Patrini et al.,CVPR 2017)
  - 実は，前述の弱教師付き学習はこの方法と等価
- 未知のTをデータから推定したい：
  - Tのマスクを事前知識として利用
    Han, Yao, Niu, Zhou, Tsang, Zhang & Sugiyama (NeurIPS2018)
  - Tと分類器を同時学習
    Xia, Xiu, Wang, Han, Gong, Niu & Sugiyama (NeurIPS2019)
  - Tを分解して推定
    Yao, Liu, Han, Gong, Deng, Niu, Sugiyama & Tao (submitted)
  - 非還元性を利用（PU学習）
    Yao, Liu, Han, Gong, Niu, Sugiyama & Tao (arXiv2020)

訓練データの出力雑音(2)

- ニューラルネットの記憶効果: Arpit et al. (ICML2017), Zhang et al. (ICLR2017)
  - 確率的勾配法は，雑音なしデータに早く適合
- 2つのニューラルネットによる共教示(co-teaching):
  - 損失の小さいデータを選んで教え合う

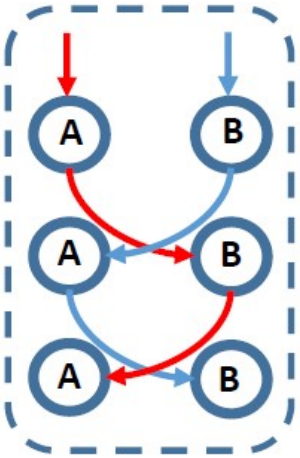
Han, Yao, Yu, Niu, Xu, Hu, Tsang & Sugiyama (NeurIPS2018)

  - 意見が一致しないものだけを選ぶ

Yu, Han, Yao, Niu, Tsang & Sugiyama (ICML2019)

  - 損失の大きいデータに対して勾配上昇

Han, Niu, Yu, Yao, Xu, Tsang & Sugiyama (ICML2020)

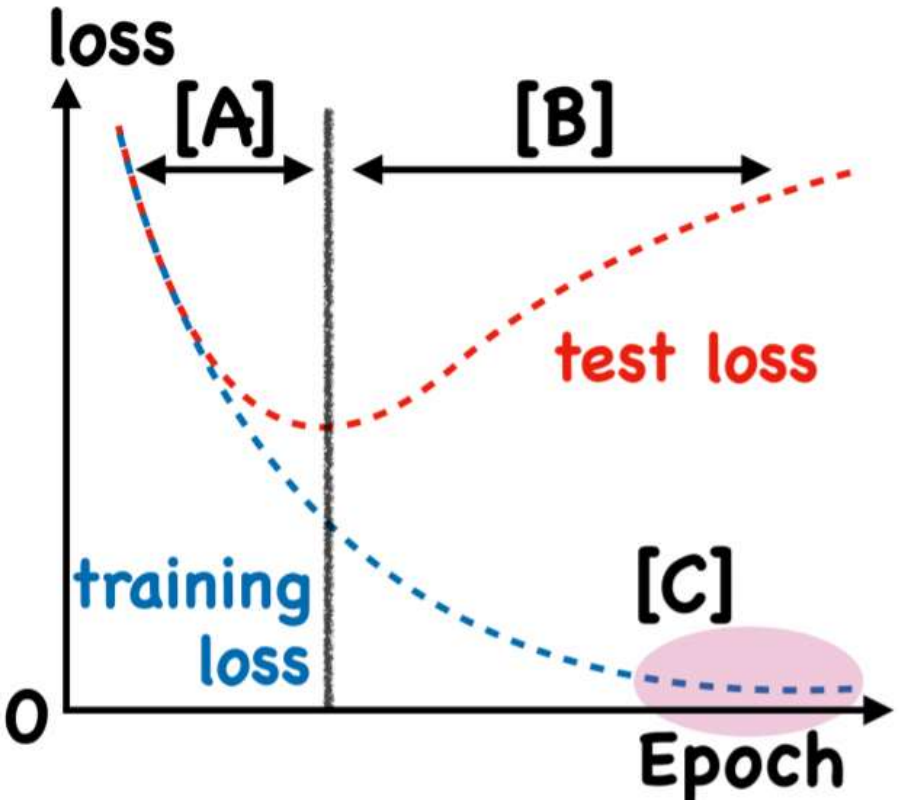


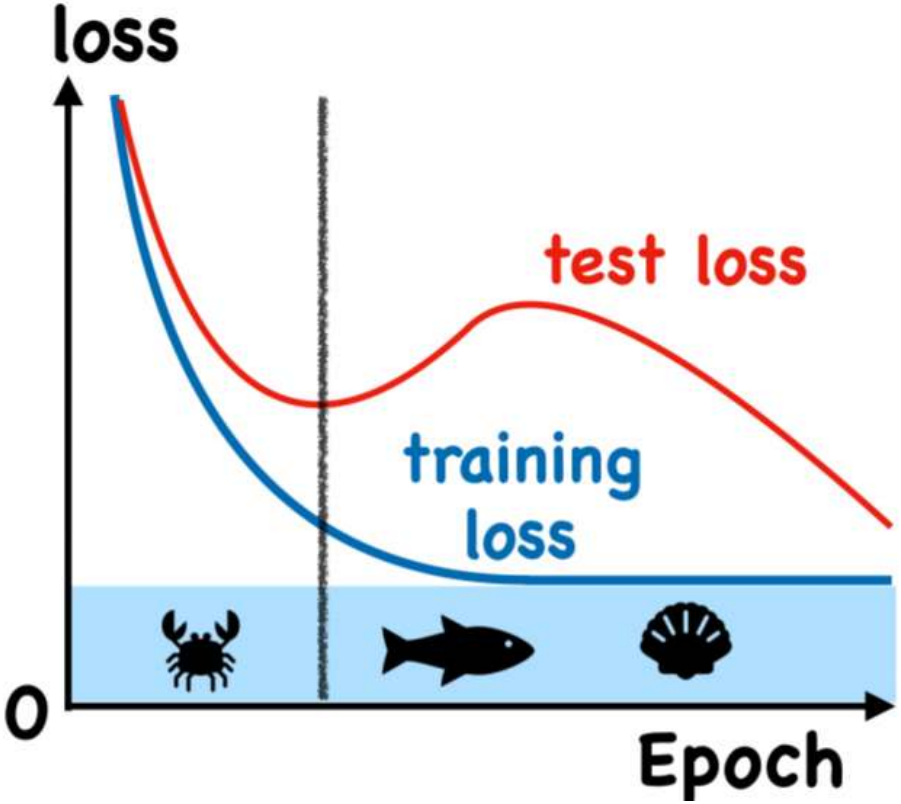
- 理論は無いが実験的には超ロバスト:
  - 50%のデータのラベルをランダムに変えてもうまくいく

訓練データの出力雑音(3)

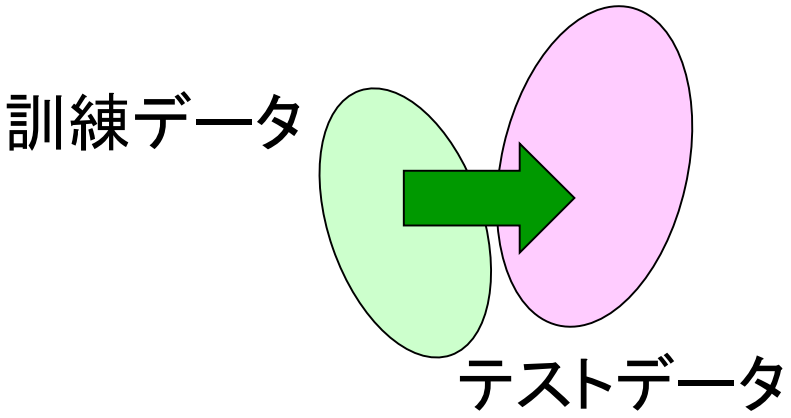
- ニューラルネットは学習しすぎると過適合する
- 訓練誤差を洪水(flooding)させて，過適合を防止

Ishida, Yamane, Sakai, Niu & Sugiyama (ICML2020)





訓練データのバイアス(1)



- 訓練データの分布がテストデータと異なる
- 転移学習:分布を合わせる
  - 入力分布だけを合わせてもうまくいかない
  - そもそも分布が大きく違うときはうまくいかない
- データ生成メカニズムの転移: Teshima, Sato & Sugiyama (ICML2020)
  - 見た目の分布が違っても,データ生成メカニズムの共通点を見つけて転移
- 転移のための重みと分類器を動的に同時学習:
  - 確率的勾配法を活用

Fang, Lu, Niu & Sugiyama(arXiv2020)

訓練データのバイアス(2)

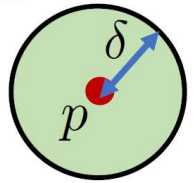
- テストデータの分布が予想できないとき
  どうするか？
- 分布ロバスト学習：
  最悪のテスト分布を想定
  - 実用上あまりうまくいかない

$$\min_{\theta} \sup_{q \in \mathcal{Q}_p} \mathbb{E}_{q(x,y)}[\ell(g_\theta(x), y)]$$

$$\mathcal{Q}_p = \{q \mid \mathrm{D}_f(q\|p) \le \delta\}$$

"f-divergence ball"

[Bagnell 2005, Ben-Tal+ 2013, Namkoong+ 2016, 2017]

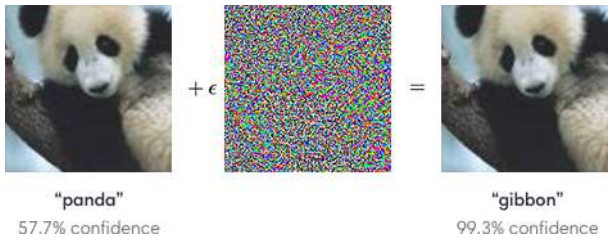


- 分類ではロバストにならないことを証明：
  Hu, Niu, Sato & Sugiyama (ICML2018)
- 収束保証のために損失関数が満たすべき
  条件を解明：
  Bao, Scott & Sugiyama (COLT2020)
- 保守的になり過ぎない新しい定式化：
  Zhang, Xu, Han, Niu, Cui, Sugiyama & Kankanhalli (ICML2020)

テストデータの入力雑音(1)

- ニューラルネットは敵対的攻撃によって簡単に間違えさせられる

Goodfellow et al. (ICLR2015)



- 出力を安定化させたい:

$$\forall \epsilon, \left(\|\epsilon\|_2 < c \Rightarrow t_X = \underset{i}{\operatorname{argmax}} \{F(X+\epsilon)_i\} \right)$$

- リプシッツ・マージン学習:

Tsuzuku, Sato & Sugiyama (NeurIPS2018)

  - 各層のリプシッツ定数を計算し,
    ニューラルネット全体のリプシッツ定数 L_F を求める:

$$\|F(X) - F(X+\epsilon)\|_2 \leq L_F \|\epsilon\|_2$$

  - 予測マージンが大きくなるように学習:

$$\forall i \neq t_X, (F_{t_X} \geq F_i + \sqrt{2} c L_F)$$

  - 間違えない範囲を理論的に保証できる!

テストデータの入力雑音(2)

Ni, Charoenphakdee, Honda & Sugiyama (NeurIPS2019)

- 実際には，敵対的攻撃に対する防御は難しい:
  - 医療などの安全性が極度に重要な応用では，難しい
    テストデータは棄却し，人に分類してもらう方が実際的
- 方法1:予測信頼度の低いデータを棄却
  - 従来法は損失に制限があり，分類性能が良くない
  - 一般の損失に対して収束保証できる棄却規準を提案.
    実験性能の良いクロスエントロピー損失にも適用可能
- 方法2:分類機と棄却器を学習
  - 二値分類に対しては収束保証があり有望
  - 多値分類では収束保証のために損失が満たすべき
    条件が(ほぼ)満たされない

発表の流れ

1. 機械学習研究分野の動向
2. 理研AIPセンターの紹介
3. 最新の機械学習技術の紹介
4. まとめと今後の展望

機械学習研究の現状と課題

- 現状の機械学習によって，画像理解，音声認識，言語翻訳などの知能の要素技術は，人間と同等以上の性能を達成できるようになってきた
  - そこそこ知的な業務はAIで代替可能？
- しかし，まだまだ技術的な課題はたくさんある：
  - 少ないデータからの学習
  - 追加学習による忘却
  - スケール不変性（cf.画像）
  - データの統計的独立性（cf.時系列）
  - チューニングの必要性
  - 要素技術を組み合わせた高度な知能の実現・・・

AI分野の現状

- あらゆる企業が「AI」を謳うようになり，
  世界的な研究開発競争，人材獲得競争が激化：
  - IT，金融，自動車，素材，教育，医療，電力，土木・・・
- サイエンス研究でもAIを活用：
  - 物理，宇宙，化学，材料，医学，生命，情報，制御・・・
- 機械学習技術の更なる高度化が進行：
  - 弱教師付き，長期学習，時系列，自動機械学習・・・
- AIの社会的影響・倫理に関する議論が活発化：
  - プライバシ，公平性，説明性，法律，経済・・・
- 人材不足が極めて深刻：
  - 研究開発，技術活用，AIリテラシー・・・

AI分野の今後：人材育成

- 国際的な人材獲得競争が激化の一途：
  - 大学院インターン生に高額給与
  - 大学付近に研究所を構えて人材を吸収
    （トロント，モントリオール，ロンドン，パリ，ベルリン・・・）
- 国内では，AI関連人材の供給が極めて限定的：
  - ほとんどの情報系学生は修士課程修了後に就職
  - 博士課程に進学する学生は少ない
- 日本政府のAI戦略：
  - 年間50万人の大学・高専生に対するAIリテラシー教育
  - 年間100万人の社会人に対するAIリカレント教育
- 専門家の育成も重要！

機械学習プロフェッショナルシリーズ（講談社，30＋巻）

- 機械学習のための連続最適化：
  金森敬文，鈴木大慈，竹内一郎，佐藤一誠
- オンライン予測：畑埜晃平，瀧本英二
- 関係データ学習：石黒 勝彦，林 浩平
- データ解析におけるプライバシー保護：佐久間　淳
- ウェブデータの機械学習：
  ダヌシカ ボレガラ，岡﨑直観，前原貴憲
- バンディット問題の理論とアルゴリズム：
  本多淳也，中村篤祥
- グラフィカルモデル：渡辺有祐
- ヒューマンコンピュテーションとクラウドソーシング：
  鹿島久嗣，小山聡，馬場雪乃
- ノンパラメトリックベイズ：佐藤一誠
- 変分ベイズ学習：中島伸一
- スパース性に基づく機械学習：冨岡亮太
- 生命情報処理における機械学習多重検定と
  推定量設計：瀬々潤，浜田道昭
- 劣モジュラ最適化と機械学習：河原吉伸，永野清仁
- 統計的学習理論：金森敬文
- 確率的最適化：鈴木大慈
- 異常検知と変化検知：井手剛，杉山将
- サポートベクトルマシン：竹内一郎，烏山昌幸
- 機械学習のための確率と統計：杉山将
- 深層学習：岡谷貴之
- オンライン機械学習：
  海野裕也，岡野原大輔，得居誠也，徳永拓之
- トピックモデル：岩田具治
- 統計的因果探索：清水昌平
- 画像認識：原田達也
- 深層学習による自然言語処理：
  坪井祐太，海野裕也，鈴木潤
- 音声認識：篠田浩一
- ガウス過程と機械学習：持橋大地，大羽成征
- 強化学習：森村哲郎
- ベイズ深層学習：須山敦志
- ロボット制御，音響処理，ソフトウェア工学，
  深層学習理論，転移学習．．．