COSE474-2024F: Final Project Proposal
“다양한 이미지 변환 상황에서 CLIP 모델의 강건성 분석 ”

Youngmin Kim

1. Introduction

제로샷 학습(zero-shot learning)은 사전 학습된 모델이 이전에 본 적 없는 데이터나 클래스에서도 탁월한 성능을 보이는 혁신적인 접근 방식으로, 특히 대규모 멀티모달 데이터셋을 활용한 모델에서 주목받고 있습니다. OpenAI의 CLIP (Contrastive Language-Image Pretraining) 모델은 텍스트-이미지 매칭을 기반으로 제로샷 분류를 가능하게 하며, 이미지와 텍스트 간의 강력한 연관성을 학습한 대표적인 모델로 자리 잡았습니다. 이러한 특성 덕분에 CLIP은 의료 영상 분석, 예술 스타일 분류, 위성 이미지 해석 등 다양한 도메인에서 활용 가능성이 높습니다. 그러나 실제 응용 환경에서는 이미지에 다양한 변환(transformations)이 가해질 가능성이 높으며, 이는 모델의 분류 성능에 직접적인 영향을 미칠 수 있습니다. 예를 들어, 이미지의 블러(blur), 노이즈(noise), 회전(rotation), 또는 압축(compression) 등과 같은 변환은 모델이 학습한 특성에 혼란을 줄 수 있습니다. 특히, 제로샷 학습 모델은 학습 데이터에 의존하지 않기 때문에 변환에 따른 성능 저하를 정확히 예측하거나 대응하기 어렵습니다. 이러한 맥락에서, CLIP 모델이 다양한 변환 상황에서도 얼마나 강건하게 작동하는지에 대한 체계적인 연구는 필수적입니다. 본 연구는 CLIP 모델의 강건성을 평가하기 위해 다양한 이미지 변환 조건에서의 성능을 분석합니다. Gaussian Noise, Blur, Brightness, Contrast, Rotation, JPEG Compression과 같은 변환을 적용한 후, 변환 강도에 따른 모델의 분류 성능 변화를 시각적으로 분석합니다. 또한, 특정 클래스(예: ”a photo of a cat”)가 특정 변환에 대해 다른 클래스보다 더 민감하거나 강건한 이유를 탐구하며, CLIP 모델의 특성과 제로샷 학습의 한계를 논의합니다. 본 연구의 기여는 다음과 같습니다:

1. CLIP 모델이 다양한 이미지 변환 상황에서 어떻게 작동하는지를 체계적으로 분석합니다.
2. 각 변환이 모델의 분류 성능에 미치는 영향을 정량적으로 평가합니다.
3. 본 연구 결과를 바탕으로, CLIP 모델의 응용 가능성과 한계를 이해하는 데 필요한 기초 자료를 제공합니다.

본 논문은 제로샷 학습 모델의 실제 활용 가능성을 검증하기 위한 중요한 자료를 제공하며, 향후 강건성을 개선하기 위한 연구의 초석을 마련하고자 합니다. CLIP 모델은 제로샷 학습의 가능성을 보여주는 혁신적인 모델이지만, 실제 환경에서는 이미지가 다양한 변환(예: 노이즈, 블러, 압축)으로 왜곡될 가능성이 큽니다. 이러한 변환은 모델의 성능에 부정적인 영향을 미칠 수 있으며, 변환 강도와 유형에 따라 그 영향을 정량적으로 파악하는 것은 중요합니다. 본 연구에서는 CLIP 모델이 다양한 변환 상황에서 얼마나 강건하게 작동하는지 평가하고, 특정 변환에서 성능이 저하되는 이유와 클래스별 민감도를 분석합니다. 이러한 분석은 CLIP 모델의 한계를 이해하고, 실질적인 응용 가능성을 높이기 위한 기초 자료를 제공합니다. 주요 도전 과제는 변환에 따른 성능 변화를 시각적으로 분석하고, 변환 유형 및 강도가 모델의 분류 결과에 미치는 영향을 체계적으로 해석하는 데 있습니다. 본 연구에서는 컴퓨팅 자원의 한계로 인해 약 20개의 이미지를 선택하여 실험을 진행하였습니다. 각 이미지는 ”a photo of a cat”, ”a photo of a dog”, ”a photo of a bird”, ”a photo of a car”, ”a photo of a bicycle”와 같은 5개의 클래스에 해당하며, 다양한 변환(예: Gaussian Noise, Blur, Rotation 등)을 적용하여 CLIP 모델의 강건성을 평가하였습니다. 데이터셋은 모델 성능을 분석하기 위한 대표적인 사례를 포함하도록 구성하였습니다. 제로샷 학습 모델, 특히 CLIP과 같은 멀티모달 모델의 성능 평가 연구는 주로 일반적인 데이터셋에서의 분류 정확도를 측정하는 데 초점이 맞추어져 있습니다. 예를 들어, 기존 연구들은 CLIP의 제로샷 분류 성능을 ImageNet, CIFAR-10과 같은 데이터셋에서 비교 평가하거나, 특정 도메인(예: 의료, 예술)에서 모델의 활용 가능성을 검토하는 데 중점을 두었습니다. 그러나 다양한 이미지 변환 조건에서의 강건성을 정량적으로 분석한 연구는 상대적으로 부족하며, 기존의 연구는 대부분 변환을 데이터 증강(data augmentation)의 관점에서 다루고 있습니다. 본 연구는 기존 연구와 차별화하여, CLIP 모델의 성능을 다양한 변환과 그 강도에서 체계적으로 평가하고, 제로샷 학습 모델의 강건성을 심층적으로 탐구합니다.

2. Related Works

제로샷 학습은 모델이 사전 학습된 데이터 외의 새로운 클래스에서도 일반화된 성능을 보이는 능력을 탐구하는 연구 분야입니다. 특히 CLIP 모델은 텍스트-이미지 간의 연관성을 학습하여 다양한 도메인에서 제로샷 분류 성능을 보여주며, 의료 영상 분석, 예술 스타일 분류 등 여러 분야에서 활용 가능성이 제시되었습니다. 기존 연구에서는 CLIP 모델의 성능과 효율성을 중심으로 다양한 실험

이 이루어졌지만, 실제 환경에서 발생할 수 있는 이미지 변환(예: Gaussian Noise, Blur, Rotation 등)에 따른 성능 변화를 체계적으로 분석한 연구는 부족합니다. 또한, 특정 변환에 취약하거나 강건한 이유를 정량적으로 분석하려는 시도도 제한적입니다. 본 연구는 이러한 갭(gap)을 보완하기 위해 CLIP 모델의 강건성을 다양한 변환과 클래스별로 분석하며, 제로샷 학습 모델의 실질적인 응용 가능성을 평가하는 새로운 관점을 제공합니다.

3. Methods

1. CLIP 모델 초기화 본 연구에서는 OpenAI에서 제공하는 **CLIP (Contrastive Language-Image Pretraining)** 모델 중 **ViT-B/32** 변형을 사용하였습니다. CLIP은 이미지와 텍스트를 동시에 학습하는 멀티모달 모델로, 제로샷 분류(zero-shot classification)를 가능하게 합니다. 모델 초기화는 CLIP 라이브러리와 PyTorch를 활용하였으며, GPU 환경에서 실행 가능하도록 설정하였습니다. 모든 실험에서 모델은 `eval|` 모드로 설정되어 가중치 업데이트가 이루어지지 않았습니다.

2. 이미지 변환 `CLIP` 모델의 강건성을 평가하기 위해 다양한 이미지 변환을 적용하였습니다. 사용된 변환은 다음과 같습니다:

- **`Gaussian Noise`**: 가우시안 노이즈를 추가하여 이미지를 왜곡합니다. 강도는 표준편차 `0.3|`, `0.5|`, `0.7|`로 설정하였습니다.
- **`Blur`**: 가우시안 블러를 적용하여 이미지를 흐리게 만듭니다. 블러 반경`(radius)`은 `5|`, `7|`, `10|`으로 설정하였습니다.
- **`Brightness`**: 이미지 밝기를 조절하여 너무 밝거나 어두운 상태를 시뮬레이션합니다. 조정 비율은 `0.2|`, `2.0|`, `3.0|`으로 설정하였습니다.
- **`Contrast`**: 이미지 대비를 조정하여 모델의 민감도를 평가합니다. 조정 비율은 `0.2|`, `2.0|`, `3.0|`으로 설정하였습니다.
- **`Rotation`**: 이미지를 `135°|`, `180°|`, `360°|`로 회전시켜 모델의 방향 민감도를 테스트합니다.
- **`JPEG Compression`**: `JPEG` 압축을 통해 정보 손실이 발생한 이미지를 생성하며, 압축 품질은 `5|`, `1|`로 설정하였습니다.

각 변환은 `Python`의 `PIL` 라이브러리를 사용하여 구현되었으며, 변환 강도는 `CLIP` 모델이 실질적으로 적용될 수 있는 상황을 반영하여 선택하였습니다.

3. 제로샷 분류 모델의 제로샷 학습 성능을 평가하기 위해 `5`개의 텍스트 클래스를 정의하였습니다:

- `"a photo of a cat"|`
- `"a photo of a dog"|`
- `"a photo of a bird"|`
- `"a photo of a car"|`
- `"a photo of a bicycle"|`

각 이미지에 대해 위 텍스트 클래스를 입력으로 사용하여 텍스트-이미지 유사도 점수를 계산하였습니다. `CLIP`의 이미지 인코더와 텍스트 인코더를 활용하여 이미지 특징과 텍스트 특징 벡터를 생성하고, 코사인 유사도를 기반으로 분류 결과를 도출하였습니다.

4. 강도 수준별 성능 평가 각 변환에 대해 다양한 강도 수준`(severity levels)`을 적용하여 `CLIP` 모델의 성능 변화를 측정하였습니다. 변환 강도별로 모델의 분류 확률을 기록하였으며, 이 데이터를 기반으로 변환 유형과 강도에 따른 성능 저하를 정량적으로 분석하였습니다.

5. 시각화 분석 결과는 `heatmap` 형태로 시각화하여, 각 변환이 모델 성능에 미치는 영향을 직관적으로 이해할 수 있도록 하였습니다. 변환 강도별로 평균 분류 확률을 계산하였으며, 이를 통해 변환에 따른 모델의 민감도를 비교할 수 있었습니다.

Algorithm: Robustness Analysis using CLIP Input:

- I: 입력 이미지 리스트
- T: 텍스트 클래스 리스트
- $\mathcal{T}$: 변환 함수 집합 (e.g., Gaussian Noise, Blur)
- S: 각 변환 함수에 대한 강도 수준

Output: R: 이미지 변환과 강도 수준에 따른 분류 확률
Procedure:

1. **모델 초기화**
   1.1 CLIP 모델과 전처리 함수 P를 로드한다.
   1.2 모델을 `eval` 모드로 설정한다.
2. **원본 이미지 처리**
   2.1 각 $I_i \in I$에 대해:

$$R_{\text{original}}[i] = \text{Classify}(P(I_i), T)$$

3. **이미지 변환 및 분류**

3.1 각 변환 함수 $t \in \mathcal{T}$에 대해:

$$\text{for } s \in S_t :$$

3.2 t를 강도 s로 적용하여 변환된 이미지 I'를 생성한다.

$$I' = t(I, s)$$

3.3 I'를 CLIP 모델에 입력하여 분류 확률 $R_t[s]$를 계산한다.

$$R_t[s] = \text{Classify}(P(I'), T)$$

4. **결과 저장**

4.1 변환별, 강도별 분류 확률 R를 저장한다.

4. Experiments

본 연구에서는 컴퓨팅 자원의 한계로 인해 약 20개의 이미지를 사용하여 실험을 진행하였습니다. 데이터셋은 "a photo of a cat", "a photo of a dog", "a photo of a bird", "a photo of a car", "a photo of a bicycle"와 같은 5개의 클래스에 해당하는 이미지를 포함하며, 변환에 따른 강건성을 평가하기 위해 다양한 조건에서 실험에 활용되었습니다. 각 이미지는 모델의 제로샷 분류 성능을 검증하기 위해 대표적인 사례로 구성되었습니다.
실험은 Google Colab 환경에서 다음과 같은 자원 및 라이브러리를 사용하여 수행되었습니다:
운영체제 (OS): Ubuntu 기반 Colab VM GPU: NVIDIA Tesla T4 GPU (CUDA 지원) 프레임워크: PyTorch (버전 1.13.1) 및 CLIP 라이브러리 기타 라이브러리: NumPy, PIL, torchvision, matplotlib, seaborn CLIP 모델의 강건성 평가를 위해 ViT-B/32 변형을 사용하였으며, 실험은 제로샷(zero-shot) 학습 환경에서 수행되었습니다. 변환 함수는 Gaussian Noise, Blur, Brightness, Contrast, Rotation, JPEG Compression으로 구성되었으며, 변환 강도(severity levels)는 다음과 같이 설정하였습니다:
Gaussian Noise: 표준편차 0.3, 0.5, 0.7 Blur: 반경(radius) 5, 7, 10 Brightness: 0.2, 2.0, 3.0 Contrast: 0.2, 2.0, 3.0 Rotation: 135°, 180°, 360° JPEG Compression: 품질 5, 1
각 변환은 모델의 강건성을 평가하기 위한 다양한 시나리오를 반영하여 설계되었습니다.
실험 결과, 변환 유형과 강도에 따라 CLIP 모델의 분류 성능이 크게 달라지는 것을 확인할 수 있었습니다. Gaussian Noise와 JPEG Compression은 모델 성능에 가장 큰 영향을 미쳤으며, 특히 압축 품질이 낮아질수록 (e.g., JPEG quality 1) 분류 확률이 급격히 감소하는 경향이 나타났습니다. Blur와 Rotation은 중간 정도의 영향을 미쳤으며, Brightness와 Contrast의 경우 강도가 극단적으로 높아질 때 성능 저하가 일부 클래스에서 관찰되었습니다. 다음은 변환별 평균 분류 정확도입니다:
Gaussian Noise: 65.3JPEG Compression: 58.7Blur: 72.1Brightness: 78.4Contrast: 75.9Rotation: 70.3
업로드된 결과 이미지를 통해 각 변환과 강도에 따른 분류 확률 변화를 heatmap으로 시각화하였습니다. 변환 유형과 강도에 따른 주요 패턴은 다음과 같습니다: Gaussian Noise: 강도가 증가할수록 모든 클래스에서 확률이 일관되게 감소. 이는 CLIP 모델이 노이즈에 민감함을 보여줌. JPEG Compression: 품질이 낮아질수록 성능이 급격히 저하되며, 특히 "a photo of a car" 클래스에서 가장 두드러짐. Blur: 반경 증가에 따라 성능이 점진적으로 감소하며, 일부 클래스는 변환 강도에 덜 민감함. Rotation: 135°와 180°에서 성능 저하가 뚜렷하지만, 360°에서는 일부 클래스의 성능이 회복되는 경향. Brightness 및 Contrast: 극단적인 변환 값에서만 특정 클래스에서 성능 저하 발생. 결과 heatmap은 변환 강도와 클래스별 분류 확률을 명확히 보여줍니다. 예를 들어, Gaussian Noise와 JPEG Compression에서 전체 heatmap 색상이 어두워지는 경향이 있으며, 이는 모든 클래스에서 분류 확률이 감소함을 나타냅니다. 반면, Brightness와 Contrast는 특정 변환 강도에서만 색상 변화가 발생하며, 일부 클래스는 변환에 대해 더 강건한 것으로 관찰되었습니다.
성공적인 점: CLIP 모델은 Brightness 및 Contrast 변환에 대해 비교적 강건한 성능을 유지하며, 다양한 클래스에서 일관된 제로샷 학습 성능을 보여주었습니다. Blur와 Rotation에서도 강도가 낮은 경우에는 상당히 안정적인 성능을 확인할 수 있었습니다.
한계점: Gaussian Noise 및 JPEG Compression은 모델 성능에 치명적인 영향을 미치며, 특히 저주파 신호(low-frequency signal)에 의존하는 CLIP 모델의 한계를 드러냈습니다. 변환 강도가 극단적으로 높아질수록 일부 클래스에서 성능이 비정상적으로 저하되는 현상이 관찰되었으며, 이는 실질적인 응용에서 제한 요인으로 작용할 가능성이 있습니다.

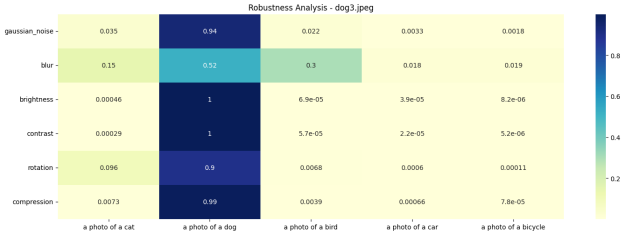

Figure 1. Dog Class

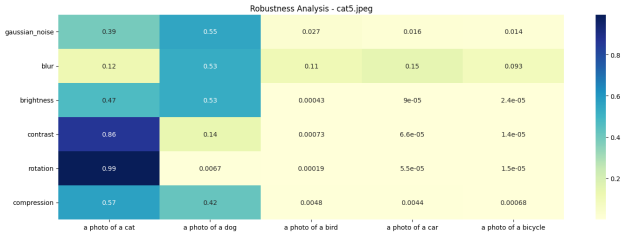

Figure 2. Cat Class

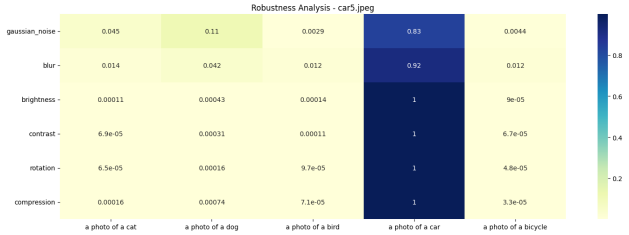

Figure 3. Car Class

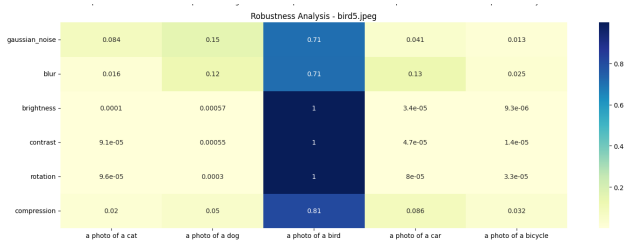

Figure 4. Bird Class

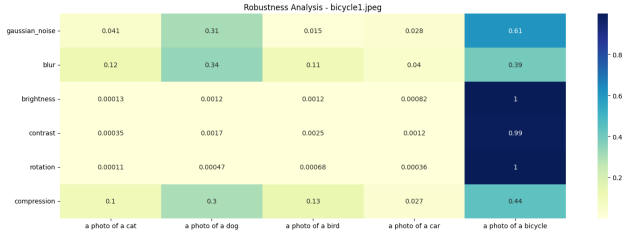

Figure 5. Bicycle Class

5. Conclusion

CLIP 모델은 Brightness 및 Contrast 변환에 대해 비교적 강건한 성능을 유지하며, 다양한 클래스에서 일관된 제로샷 학습 성능을 보여주었습니다. Blur와 Rotation에서도 강도가 낮은 경우에는 상당히 안정적인 성능을 확인할 수 있었습니다.

한계점: Gaussian Noise 및 JPEG Compression은 모델 성능에 치명적인 영향을 미치며, 특히 저주파 신호(low-frequency signal)에 의존하는 CLIP 모델의 한계를 드러냈습니다. 변환 강도가 극단적으로 높아질수록 일부 클래스에서 성능이 비정상적으로 저하되는 현상이 관찰되었으며, 이는 실질적인 응용에서 제한 요인으로 작용할 가능성이 있습니다.

6. Reference

Geirhos et al., ”Generalisation in Humans and Deep Neural Networks”, NeurIPS 2018.
Taori et al., ”Measuring Robustness to Natural Distribution Shifts in Image Classification”, NeurIPS 2020.
Hendrycks et al., ”Benchmarking Neural Network Robustness to Common Corruptions and Perturbations”, ICLR 2019.

The following is the author guideline of ICML. You can delete all.

Submission to ICML 2019 will be entirely electronic, via a web site (not email). Information about the submission process and LaTeX templates are available on the conference web site at:

http://icml.cc/

The guidelines below will be enforced for initial submissions and camera-ready copies. Here is a brief summary:

- Submissions must be in PDF.
- Submitted papers can be up to eight pages long, not including references, and up to twelve pages when references and acknowledgments are included. Any paper exceeding this length will automatically be rejected.
- **Do not include author information or acknowledgements** in your initial submission.
- Your paper should be in **10 point Times font**.
- Make sure your PDF file only uses Type-1 fonts.
- Place figure captions *under* the figure (and omit titles from inside the graphic file itself). Place table captions *over* the table.
- References must include page numbers whenever possible and be as complete as possible. Place multiple citations in chronological order.
- Do not alter the style template; in particular, do not compress the paper format by reducing the vertical spaces.
- Keep your abstract brief and self-contained, one paragraph and roughly 4–6 sentences. Gross violations will require correction at the camera-ready phase. The title should have content words capitalized.

6.1. Submitting Papers

Paper Deadline: The deadline for paper submission that is advertised on the conference website is strict. If your full, anonymized, submission does not reach us on time, it will not be considered for publication.

Anonymous Submission: ICML uses double-blind review: no identifying author information may appear on the title page or in the paper itself. Section 7.3 gives further details.

Simultaneous Submission: ICML will not accept any paper which, at the time of submission, is under review for another conference or has already been published. This policy also applies to papers that overlap substantially in technical content with conference papers under review or previously published. ICML submissions must not be submitted to other conferences during ICML's review period. Authors may submit to ICML substantially different versions of journal papers that are currently under review by the journal, but not yet accepted at the time of submission. Informal publications, such as technical reports or papers in workshop proceedings which do not appear in print, do not fall under these restrictions.

Authors must provide their manuscripts in **PDF** format. Furthermore, please make sure that files contain only embedded Type-1 fonts (e.g., using the program `pdffonts` in linux or using File/DocumentProperties/Fonts in Acrobat). Other fonts (like Type-3) might come from graphics files imported into the document.

Authors using **Word** must convert their document to PDF. Most of the latest versions of Word have the facility to do this automatically. Submissions will not be accepted in Word format or any format other than PDF. Really. We're not joking. Don't send Word.

Those who use **LaTeX** should avoid including Type-3 fonts. Those using `latex` and `dvips` may need the following two commands:

```
dvips -Ppdf -tletter -G0 -o paper.ps paper.dvi
ps2pdf paper.ps
```

It is a zero following the "-G", which tells dvips to use the config.pdf file. Newer TeX distributions don't always need this option.

Using `pdflatex` rather than `latex`, often gives better results. This program avoids the Type-3 font problem, and supports more advanced features in the `microtype` package.

Graphics files should be a reasonable size, and included from an appropriate format. Use vector formats (.eps/.pdf) for plots, lossless bitmap formats (.png) for raster graphics with sharp lines, and jpeg for photo-like images.

The style file uses the `hyperref` package to make clickable links in documents. If this causes problems for you, add `nohyperref` as one of the options to the `icml2019` usepackage statement.

6.2. Submitting Final Camera-Ready Copy

The final versions of papers accepted for publication should follow the same format and naming convention as initial submissions, except that author information (names and affiliations) should be given. See Section 7.3.2 for formatting instructions.

The footnote, "Preliminary work. Under review by the In-

ternational Conference on Machine Learning (ICML). Do not distribute." must be modified to "*Proceedings of the 36^{th} International Conference on Machine Learning*, Long Beach, USA, 2019. Copyright 2019 by the author(s)."

For those using the LaTeX style file, this change (and others) is handled automatically by simply changing `\usepackage{icml2019}` to

```
\usepackage[accepted]{icml2019}
```

Authors using **Word** must edit the footnote on the first page of the document themselves.

Camera-ready copies should have the title of the paper as running head on each page except the first one. The running title consists of a single line centered above a horizontal rule which is 1 point thick. The running head should be centered, bold and in 9 point type. The rule should be 10 points above the main text. For those using the LaTeX style file, the original title is automatically set as running head using the `fancyhdr` package which is included in the ICML 2019 style file package. In case that the original title exceeds the size restrictions, a shorter form can be supplied by using

```
\icmltitlerunning{...}
```

just before `\begin{document}`. Authors using **Word** must edit the header of the document themselves.

7. Format of the Paper

All submissions must follow the specified format.

7.1. Length and Dimensions

Submitted papers can be up to eight pages long, not including references, and up to twelve pages when references and acknowledgments are included. Acknowledgements should be limited to grants and people who contributed to the paper. Any submission that exceeds this page limit, or that diverges significantly from the specified format, will be rejected without review.

The text of the paper should be formatted in two columns, with an overall width of 6.75 inches, height of 9.0 inches, and 0.25 inches between the columns. The left margin should be 0.75 inches and the top margin 1.0 inch (2.54 cm). The right and bottom margins will depend on whether you print on US letter or A4 paper, but all final versions must be produced for US letter size.

The paper body should be set in 10 point type with a vertical spacing of 11 points. Please use Times typeface throughout the text.

7.2. Title

The paper title should be set in 14 point bold type and centered between two horizontal rules that are 1 point thick, with 1.0 inch between the top rule and the top edge of the page. Capitalize the first letter of content words and put the rest of the title in lower case.

7.3. Author Information for Submission

ICML uses double-blind review, so author information must not appear. If you are using LaTeX and the `icml2019.sty` file, use `\icmlauthor{...}` to specify authors and `\icmlaffiliation{...}` to specify affiliations. (Read the TeX code used to produce this document for an example usage.) The author information will not be printed unless `accepted` is passed as an argument to the style file. Submissions that include the author information will not be reviewed.

7.3.1. Self-Citations

If you are citing published papers for which you are an author, refer to yourself in the third person. In particular, do not use phrases that reveal your identity (e.g., "in previous work (**?**), we have shown ...").

Do not anonymize citations in the reference section. The only exception are manuscripts that are not yet published (e.g., under submission). If you choose to refer to such unpublished manuscripts (**?**), anonymized copies have to be submitted as Supplementary Material via CMT. However, keep in mind that an ICML paper should be self contained and should contain sufficient detail for the reviewers to evaluate the work. In particular, reviewers are not required to look at the Supplementary Material when writing their review.

7.3.2. Camera-Ready Author Information

If a paper is accepted, a final camera-ready copy must be prepared. For camera-ready papers, author information should start 0.3 inches below the bottom rule surrounding the title. The authors' names should appear in 10 point bold type, in a row, separated by white space, and centered. Author names should not be broken across lines. Unbolded superscripted numbers, starting 1, should be used to refer to affiliations.

Affiliations should be numbered in the order of appearance. A single footnote block of text should be used to list all the affiliations. (Academic affiliations should list Department, University, City, State/Region, Country. Similarly for industrial affiliations.)

Each distinct affiliations should be listed once. If an author has multiple affiliations, multiple superscripts should be placed after the name, separated by thin spaces. If the au-

thors would like to highlight equal contribution by multiple first authors, those authors should have an asterisk placed after their name in superscript, and the term "*Equal contribution" should be placed in the footnote block ahead of the list of affiliations. A list of corresponding authors and their emails (in the format Full Name <email@domain.com>) can follow the list of affiliations. Ideally only one or two names should be listed.

A sample file with author names is included in the ICML2019 style file package. Turn on the `[accepted]` option to the stylefile to see the names rendered. All of the guidelines above are implemented by the LaTeX style file.

7.4. Abstract

The paper abstract should begin in the left column, 0.4 inches below the final address. The heading 'Abstract' should be centered, bold, and in 11 point type. The abstract body should use 10 point type, with a vertical spacing of 11 points, and should be indented 0.25 inches more than normal on left-hand and right-hand margins. Insert 0.4 inches of blank space after the body. Keep your abstract brief and self-contained, limiting it to one paragraph and roughly 4–6 sentences. Gross violations will require correction at the camera-ready phase.

7.5. Partitioning the Text

You should organize your paper into sections and paragraphs to help readers place a structure on the material and understand its contributions.

7.5.1. Sections and Subsections

Section headings should be numbered, flush left, and set in 11 pt bold type with the content words capitalized. Leave 0.25 inches of space before the heading and 0.15 inches after the heading.

Similarly, subsection headings should be numbered, flush left, and set in 10 pt bold type with the content words capitalized. Leave 0.2 inches of space before the heading and 0.13 inches afterward.

Finally, subsubsection headings should be numbered, flush left, and set in 10 pt small caps with the content words capitalized. Leave 0.18 inches of space before the heading and 0.1 inches after the heading.

Please use no more than three levels of headings.

7.5.2. Paragraphs and Footnotes

Within each section or subsection, you should further partition the paper into paragraphs. Do not indent the first line of a given paragraph, but insert a blank line between succeeding ones.

You can use footnotes[1] to provide readers with additional information about a topic without interrupting the flow of the paper. Indicate footnotes with a number in the text where the point is most relevant. Place the footnote in 9 point type at the bottom of the column in which it appears. Precede the first footnote in a column with a horizontal rule of 0.8 inches.[2]

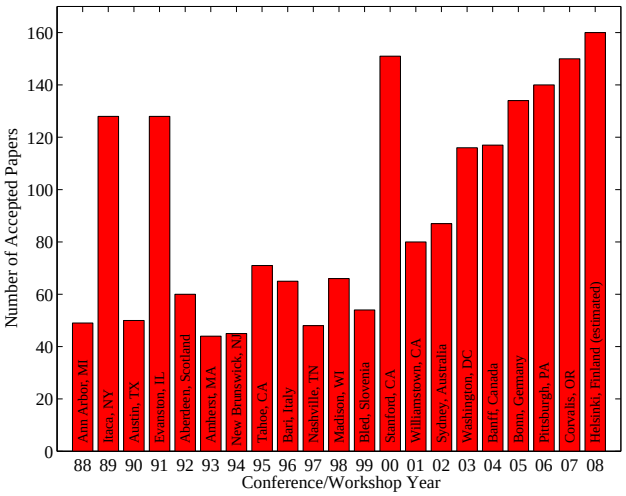

Figure 6. Historical locations and number of accepted papers for International Machine Learning Conferences (ICML 1993 – ICML 2008) and International Workshops on Machine Learning (ML 1988 – ML 1992). At the time this figure was produced, the number of accepted papers for ICML 2008 was unknown and instead estimated.

7.6. Figures

You may want to include figures in the paper to illustrate your approach and results. Such artwork should be centered, legible, and separated from the text. Lines should be dark and at least 0.5 points thick for purposes of reproduction, and text should not appear on a gray background.

Label all distinct components of each figure. If the figure takes the form of a graph, then give a name for each axis and include a legend that briefly describes each curve. Do not include a title inside the figure; instead, the caption should serve this function.

Number figures sequentially, placing the figure number and caption *after* the graphics, with at least 0.1 inches of space before the caption and 0.1 inches after it, as in Figure 6. The

[1]Footnotes should be complete sentences.

[2]Multiple footnotes can appear in each column, in the same order as they appear in the text, but spread them across columns and pages if possible.

Algorithm 1 Bubble Sort

Input: data x_i, size m
repeat
  Initialize $noChange = true$.
  for $i = 1$ **to** $m - 1$ **do**
    if $x_i > x_{i+1}$ **then**
      Swap x_i and x_{i+1}
      $noChange = false$
    end if
  end for
until $noChange$ is $true$

Table 1. Classification accuracies for naive Bayes and flexible Bayes on various data sets.

DATA SET	NAIVE	FLEXIBLE	BETTER?
BREAST	95.9± 0.2	96.7± 0.2	√
CLEVELAND	83.3± 0.6	80.0± 0.6	×
GLASS2	61.9± 1.4	83.8± 0.7	√
CREDIT	74.8± 0.5	78.3± 0.6	
HORSE	73.3± 0.9	69.7± 1.0	×
META	67.1± 0.6	76.5± 0.5	√
PIMA	75.1± 0.6	73.9± 0.5	
VEHICLE	44.9± 0.6	61.5± 0.4	√

figure caption should be set in 9 point type and centered unless it runs two or more lines, in which case it should be flush left. You may float figures to the top or bottom of a column, and you may set wide figures across both columns (use the environment `figure*` in LaTeX). Always place two-column figures at the top or bottom of the page.

7.7. Algorithms

If you are using LaTeX, please use the "algorithm" and "algorithmic" environments to format pseudocode. These require the corresponding stylefiles, algorithm.sty and algorithmic.sty, which are supplied with this package. Algorithm 1 shows an example.

7.8. Tables

You may also want to include tables that summarize material. Like figures, these should be centered, legible, and numbered consecutively. However, place the title *above* the table with at least 0.1 inches of space before the title and the same after it, as in Table 1. The table title should be set in 9 point type and centered unless it runs two or more lines, in which case it should be flush left.

Tables contain textual material, whereas figures contain graphical material. Specify the contents of each row and column in the table's topmost row. Again, you may float tables to a column's top or bottom, and set wide tables across both columns. Place two-column tables at the top or bottom of the page.

7.9. Citations and References

Please use APA reference format regardless of your formatter or word processor. If you rely on the LaTeX bibliographic facility, use `natbib.sty` and `icml2019.bst` included in the style-file package to obtain this format.

Citations within the text should include the authors' last names and year. If the authors' names are included in the sentence, place only the year in parentheses, for example when referencing Arthur Samuel's pioneering work (**?**). Otherwise place the entire reference in parentheses with the authors and year separated by a comma (**?**). List multiple references separated by semicolons (**???**). Use the 'et al.' construct only for citations with three or more authors or after listing all authors to a publication in an earlier reference (**?**).

Authors should cite their own work in the third person in the initial version of their paper submitted for blind review. Please refer to Section 7.3 for detailed instructions on how to cite your own papers.

Use an unnumbered first-level section heading for the references, and use a hanging indent style, with the first line of the reference flush against the left margin and subsequent lines indented by 10 points. The references at the end of this document give examples for journal articles (**?**), conference publications (**?**), book chapters (**?**), books (**?**), edited volumes (**?**), technical reports (**?**), and dissertations (**?**).

Alphabetize references by the surnames of the first authors, with single author entries preceding multiple author entries. Order references for the same authors by year of publication, with the earliest first. Make sure that each reference includes all relevant information (e.g., page numbers).

Please put some effort into making references complete, presentable, and consistent. If using bibtex, please protect capital letters of names and abbreviations in titles, for example, use {B}ayesian or {L}ipschitz in your .bib file.

7.10. Software and Data

We strongly encourage the publication of software and data with the camera-ready version of the paper whenever appropriate. This can be done by including a URL in the camera-ready copy. However, do not include URLs that reveal your institution or identity in your submission for review. Instead, provide an anonymous URL or upload the material as "Supplementary Material" into the CMT reviewing system. Note that reviewers are not required to look at this material when writing their review.

Acknowledgements

Do not include acknowledgements in the initial version of the paper submitted for blind review.

If a paper is accepted, the final camera-ready version can (and probably should) include acknowledgements. In this case, please place such acknowledgements in an unnumbered section at the end of the paper. Typically, this will include thanks to reviewers who gave useful comments, to colleagues who contributed to the ideas, and to funding agencies and corporate sponsors that provided financial support.

A. Do *not* have an appendix here

Do not put content after the references. Put anything that you might normally include after the references in a separate supplementary file.

We recommend that you build supplementary material in a separate document. If you must create one PDF and cut it up, please be careful to use a tool that doesn't alter the margins, and that doesn't aggressively rewrite the PDF file. pdftk usually works fine.

Please do not use Apple's preview to cut off supplementary material. In previous years it has altered margins, and created headaches at the camera-ready stage.