Robustness of Conditional GANs to Noisy Labels
Spotlight presentation, NeurIPS 2018

Kiran K. Thekumparampil¹  Ashish Khetan¹
Zinan Lin²  Sewoong Oh¹

¹University of Illinois at Urbana-Champaign
²Carnegie Mellon University

Poster #5, Tue, Dec 4 2018
Conditional GAN (cGAN) is vital for achieving high quality

- **Input**: Labeled real samples \((X, Y)\)
- **Output**: Fake samples for label \(Y\)

Visual quality: cGAN >>> GAN

[https://github.com/tensorflow/models/tree/master/research/gan]
Conditional GAN (cGAN) is vital for achieving high quality

- **Input**: Labeled real samples \((X, Y)\)
- **Output**: Fake samples for label \(Y\)

[Image: Dog, Landscape, Butterfly, Burger]

“Cat”  \(\rightarrow\) cGAN  \(\rightarrow\) Latent Code

[Brock et al. 2018]

Visual quality: cGAN \(>>\) GAN

[https://github.com/tensorflow/models/tree/master/research/gan]
Conditional GAN (cGAN) is vital for achieving high quality

- **Input**: Labeled real samples \((X, Y)\)
- **Output**: Fake samples for label \(Y\)

![Visual quality comparison]

```
[https://github.com/tensorflow/models/tree/master/research/gan]
```
Conditional GAN is sensitive to noise in labels

cGAN trained with noisy labels produces samples
- that are **biased**, generating examples from wrong classes, and,
- of **lower quality** (red boxes).

label

```
0 0 0 0 0 0 0 0 0 0
1 1 1 1 1 1 1 1 1 1
2 2 2 2 2 2 2 2 2 2
3 3 3 3 3 3 3 3 3 3
4 4 4 4 4 4 4 4 4 4
5 5 5 5 5 5 5 5 5 5
6 6 6 6 6 6 6 6 6 6
7 7 7 7 7 7 7 7 7 7
8 8 8 8 8 8 8 8 8 8
9 9 9 9 9 9 9 9 9 9
```

real data
Conditional GAN is sensitive to noise in labels

cGAN trained with noisy labels produces samples
  - that are **biased**, generating examples from wrong classes, and,
  - of **lower quality** (red boxes).

```
label
0  1  4  0  1  0  4  5  9  2  7
1  1  2  9  0  5  7  \\  5  1
2  8  2  2  0  1  4  5  5  2  1
3  3  3  1  1  6  2  3  9  3
4  4  6  5  4  4  1  4  4  4
5  2  5  5  7  2  5  8  4  3
6  3  6  5  1  4  7  7  9  3  6
7  0  7  6  2  7  1  3  7  7
8  6  8  2  0  8  8  9  8  8
9  0  9  9  5  9  0  9  4  3  4
```

noisy real data
Conditional GAN is sensitive to noise in labels

cGAN trained with noisy labels produces samples
  - that are **biased**, generating examples from wrong classes, and,
  - of **lower quality** (red boxes).

<table>
<thead>
<tr>
<th>label</th>
<th>noisy real data</th>
<th>standard cGAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1 4 0 1 0 4 5 9 2 7</td>
<td>8 3 0 0 0 3 0 4 0</td>
</tr>
<tr>
<td>1</td>
<td>1 1 2 9 0 5 7 1 5 1</td>
<td>1 3 / 1 6 3 4 1 1</td>
</tr>
<tr>
<td>2</td>
<td>8 2 0 1 4 5 5 2 1</td>
<td>7 7 0</td>
</tr>
<tr>
<td>3</td>
<td>3 3 3 1 1 6 2 3 9 3</td>
<td>3 2 6 0 6 3 2 8 1 3</td>
</tr>
<tr>
<td>4</td>
<td>7 6 5 4 4 1 4 4 4</td>
<td>4 4 4 9 4 2 3 1 4</td>
</tr>
<tr>
<td>5</td>
<td>8 5 5 7 2 5 8 / 4 3</td>
<td>4 5 0 3 7 5 5 7</td>
</tr>
<tr>
<td>6</td>
<td>3 6 5 1 4 7 4 3 6</td>
<td>6 2 2 0 8 6 5 6 2</td>
</tr>
<tr>
<td>7</td>
<td>0 1 6 2 7 1 3 7 7</td>
<td>7 2 / 7 4 0 9 9</td>
</tr>
<tr>
<td>8</td>
<td>6 8 2 0 6 / 8 9 8 8</td>
<td>5 8 8 8 9 4 9</td>
</tr>
<tr>
<td>9</td>
<td>0 9 9 5 9 0 9 4 3 4</td>
<td>9 7 3 9 2 4 9 9 8 6</td>
</tr>
</tbody>
</table>
Conditional GAN is sensitive to noise in labels

cGAN trained with noisy labels produces samples

- that are **biased**, generating examples from wrong classes, and,
- of **lower quality** (red boxes).

<table>
<thead>
<tr>
<th>label</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>8</td>
</tr>
<tr>
<td>9</td>
</tr>
</tbody>
</table>

noisy real data         standard cGAN         our RCGAN
Conditional GAN (cGAN)

\[ \min_Q \text{JS}(P \parallel Q) \]

\[ x_{\text{real}} \rightarrow G \rightarrow P \]

\[ y_{\text{real}} \rightarrow Q \]

\[ z \rightarrow G \rightarrow x \rightarrow D \rightarrow \text{adversarial loss} \]

\[ y \rightarrow y \rightarrow \text{EIGHT} \]

[Bora et al. 2018, Miyato et al. 2018, Sukhbaatar et al. 2015]
Conditional GAN under noisy labeled data

\[
\begin{align*}
\min_Q JS(\tilde{P} \parallel Q)
\end{align*}
\]

Thekumparampil (UIUC)  Robust Conditional GAN  NeurIPS 2018  5 / 14
Robust Conditional GAN (RCGAN) Architecture

\[ \min_Q \text{JS}(\tilde{P} \parallel \tilde{Q}) \]

[Bora et al. 2018, Miyato et al. 2018, Sukhbaatar et al. 2015]
Minimizing noisy divergence minimizes true divergence

Let $\tilde{P}$ & $\tilde{Q}$ be the noisy labeled versions of $P$ & $Q$.

**Theorem 1 (Population-level Analysis)**

\[
\begin{align*}
TV(\tilde{P}, \tilde{Q}) & \leq TV(P, Q) \leq M_C TV(\tilde{P}, \tilde{Q}) \\
JS(\tilde{P} \parallel \tilde{Q}) & \leq JS(P \parallel Q) \leq M_C \sqrt{8 \ JS(\tilde{P} \parallel \tilde{Q})}
\end{align*}
\]

\[\implies \tilde{Q} = \tilde{P} \implies Q = P\]

where $TV$: Total Variation, $JS$: Jensen-Shannon divergence and $M_C \triangleq \max_i \sum_j |(C^{-1})_{ij}|$. 

Neural Network Distance ($d_F$) w.r.t a class of parametric discriminator functions $F$ is known to generalize [Arora et al. 2017]
Minimizing noisy divergence minimizes true divergence

Let $\tilde{P}$ & $\tilde{Q}$ be the noisy labeled versions of $P$ & $Q$.

**Theorem 1 (Population-level Analysis)**

\[
\begin{align*}
\text{TV} \left( \tilde{P}, \tilde{Q} \right) & \leq \text{TV} \left( P, Q \right) \leq M_C \text{TV} \left( \tilde{P}, \tilde{Q} \right) \\
\text{JS} \left( \tilde{P} \parallel \tilde{Q} \right) & \leq \text{JS} \left( P \parallel Q \right) \leq M_C \sqrt{8 \text{JS} \left( \tilde{P} \parallel \tilde{Q} \right)} \end{align*}
\]

$\implies \tilde{Q} = \tilde{P} \implies Q = P$

where $\text{TV}$: Total Variation, $\text{JS}$: Jensen-Shannon divergence and $M_C \triangleq \max_i \sum_j \left| (C^{-1})_{ij} \right|$. 

**Neural Network Distance** $(d_F)$ w.r.t a class of parametric discriminator functions $\mathcal{F}$ is known to generalize [Arora et al. 2017]
Minimizing noisy divergence minimizes true divergence

Let $\tilde{P}_n$ & $\tilde{Q}_n$ be the empirical noisy real and generated distributions.

**Theorem 2 (Finite Sample Analysis)**

If $\mathcal{F}$ satisfies inclusion condition, then $\exists c > 0$ such that

$$d_{\mathcal{F}}(\tilde{P}_n, \tilde{Q}_n) - \epsilon \leq d_{\mathcal{F}}(P, Q) \leq M_C (d_{\mathcal{F}}(\tilde{P}_n, \tilde{Q}_n) + \epsilon)$$

with probability at least $1 - e^{-p}$ for any $\epsilon > 0$ and $n \geq cp \log \left(\frac{pL}{\epsilon}\right) / \epsilon^2$

when $\mathcal{F}$ is $L$-Lipschitz in $p$ parameters

**Projection Discriminator satisfies inclusion condition**
RCGAN generates correct class (MNIST)
RCGAN generates correct class (MNIST)

Thekumparampil (UIUC) Robust Conditional GAN NeurIPS 2018 10 / 14
RCGAN generates correct class (MNIST)
RCGAN improves quality of samples (CIFAR-10)

The diagram shows the Inception Score for different noise levels across three models: cGAN, RCGAN, and RCGAN-U. The Inception Score decreases as the noise level increases for all models, with RCGAN-U generally performing better than cGAN and RCGAN at lower noise levels.
RCGAN can correct noisy training labels (MNIST)

The graph shows the label recovery accuracy for different noise levels for RCGAN, RCGAN-U, and cGAN. The accuracy decreases as the noise level increases, with RCGAN-U performing slightly better than RCGAN and cGAN at higher noise levels.
Thank you

Poster #5, Tue, Dec 04
https://github.com/POLane16/Robust-Conditional-GAN