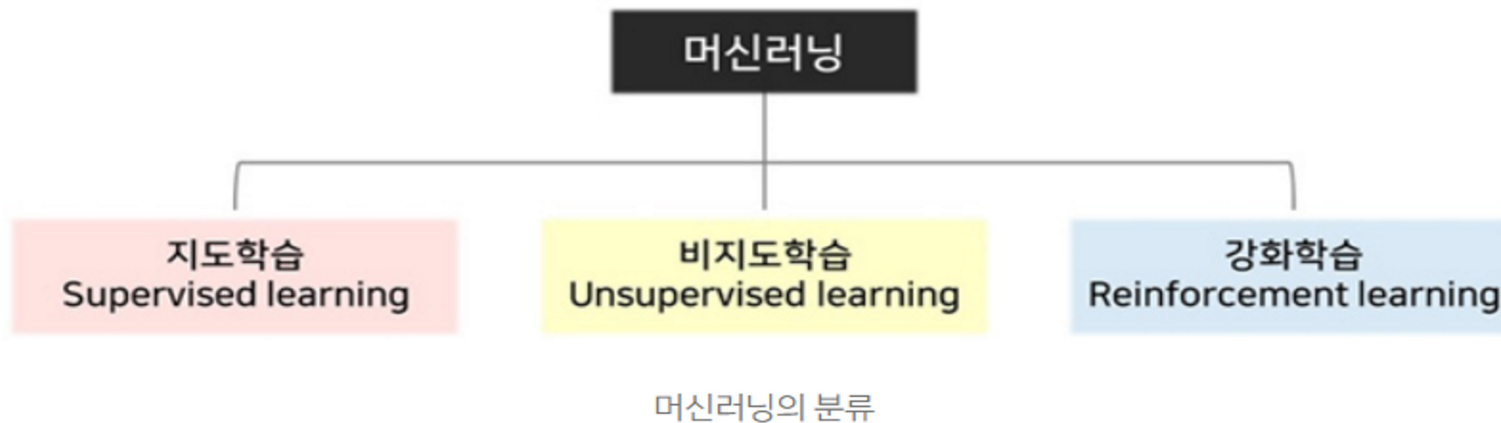


GAN(생산적 적대 신경망)

2019년 4월 19일 금요일 오전 10:12

- 인공지능을 소프트웨어적으로 구현하는 **머신러닝(Machine learning)**은 컴퓨터가 **데이터**를 **학습**하고 스스로 **패턴**을 찾아내 적절한 작업을 수행하도록 학습하는 알고리즘입니다.
- 머신러닝은 크게 **지도학습 (Supervised learning)**, **비지도학습 (Unsupervised learning)**, **강화학습 (Reinforcement learning)**등으로 분류됩니다.



1. **지도학습** : 정답이 주어진 상태에서 학습하는 알고리즘
 - a. 분류(classification)
 - 이진 분류(binary classification)
 - 다중 분류(multiclass classification)
 - b. 회귀(regression)

- 데이터의 특징을 기반으로 연속적인 숫자(벡터)를 예측
2. 비지도학습 : 정답이 주어지지 않은 상태에서 학습하는 알고리즘
- a. 군집화(clustering)
 - 데이터의 특징을 파악
 - Generative adversarial network (GAN) : 생산적 적대 신경망



GAN : 생산적 적대 신경망

- 원 데이터가 가지고 있는 확률분포를 추정하도록 하고, 인공지능망이 그 분포를 만들어 낼 수 있도록 한다
- GAN에서 다루고자 하는 모든 데이터는 확률분포를 가지고 는 랜덤변수(Random Variable)이다.
- 때문에 GAN과 같은 비지도학습이 가능한 머신러닝 알고리즘으로 데이터에 대한 확률분포를 모델링 할 수 있게 되면, 원 데이터와 확률분포를 정확히 공유하는 무한히 많은 새로운 데이터를 새로 생성할 수 있음을 의미합니다.
- GAN은 2014년 NIPS에서 Ian Goodfellow가 발표한 회귀생성 모델
- 분류를 담당하는 모델(판별자 D)과 회귀생성을 담당하는 두 개의 모델(생성자 G)로 구성되어 있습니다. 두 모델은 GAN이란 이름에서 쉽게

알 수 있듯이, **생성자 G와 판별자 D가 서로의 성능을 개선해 적대적으로 경쟁해 나가는 모델**입니다.

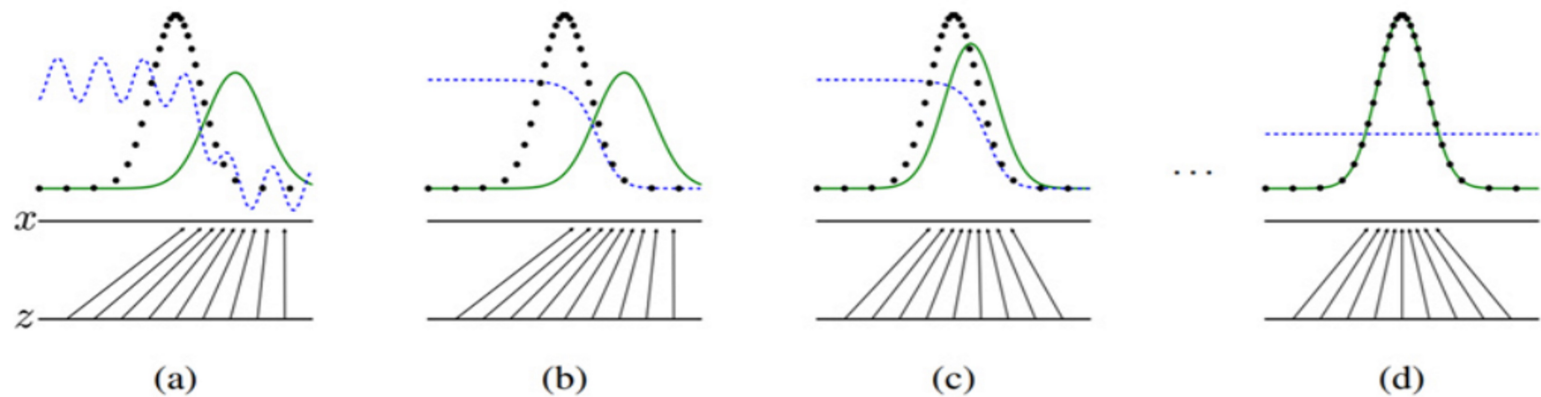
Example

쉽게 말해 경찰과 지폐 위조범의 대립과 같은 방식으로 이해할 수 있습니다.

지폐 위조범(생성자 G)은 경찰(분류자 D)을 최대한 열심히 속이려고 하고, 다른 한편에서는 경찰은 이렇게 위조된 지폐와 진짜 지폐를 두고 분류하기 위해 노력합니다.

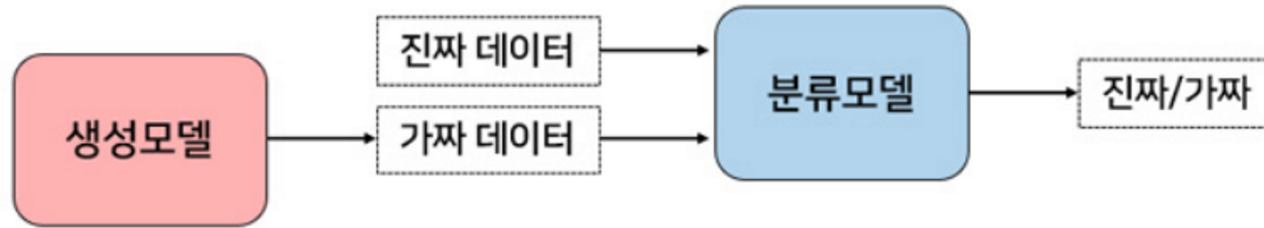
이러한 경쟁이 지속적으로 학습되면 결과적으로는 진짜 지폐와 위조지폐를 구별할 수 없을 정도의 상태가 되며, 진짜와 거의 차이가 없는 가짜 지폐를 만들어 낼 수 있습니다.

수학적으로 생성자 G는 앞에서 말한 원 데이터의 확률분포를 알아내려고 노력하며, 학습이 종료된 후에는 원 데이터의 확률분포를 따르는 새로운 데이터를 만들어 내게 됩니다.



※ 검은 점선: 원 데이터의 확률분포, 녹색 점선: GAN이 만들어 내는 확률분포, 파란 점선: 분류자의 확률분포

ALGORITHM :



- minmax problem :

$$\min_G \max_D V(D, G) = E_{x \sim p_{data}(x)} [\log D(x)] + E_{z \sim p_z(z)} [\log(1 - D(G(z)))]$$

$X \sim P_{data}(x)$: 실제 데이터에 대한 확률분포에서 샘플링한 데이터

$Z \sim P_z(z)$: 일반적으로 가우시안분포를 사용하는 임의의 노이즈에서 샘플링한 데이터를 의미

Z : 통상적으로 latent vector라고도 부르는데 차원이 줄어든 채로 데이터를 잘 설명할 수 있는 잠재 공간에서의 벡터를 의미

$D(x)$: 분류자, 진짜일 확률을 의미하는 0과 1사이의 값이라서, 데이터가 진짜이면 $D(x)$ 는 1, 가짜이면 0의 값..

$D(G(z))$: G가 만들어낸 데이터인 $G(z)$ 가 진짜라고 판단되면 1, 가짜라고 판단되면 0의 값

우선 **D가 V(D,G)를 최대화**하는 관점에서 생각해봅시다. 위의 수식을 최대화하기 위해서는 우변의 첫 번째 항과 두 번째 항 모두 최대가 되어야 하므로 $\log D(x)$ 와 $\log(1 - D(G(z)))$ 모두 최대가 되어야 합니다. 따라서, **$D(x)$ 는 1**이 되어야 하며 이는 **실제 데이터를 진짜라고 분류하도록 D를 학습하는 것을 의미합니다**. 마찬가지로 **$1 - D(G(z))$ 는 1**이 되어 $D(G(z))$ 는 따라서 0이어야 하며, 이는 **생성자가 만들어낸 가짜 데이터를 가짜라고 분류하도록 분류자를 학습하는 것을 의미합니다**. 다시 생각해보면 $V(D,G)$ 가 최대가 되도록 D를 학습하는 것은 판별자가 진짜 데이터를 진짜로, 가짜 데이터를 가짜로 분류하도록 학습하는 과정입니다.

다음으로 **생성자G가 V(D,G)를 어떻게 최소화**하도록 학습하는 지에 대한 관점에서 생각해봅시다. 위의 수식의 우변 첫 번째 항에는 G가 포함되어 있지 않으므로 생성자와 연관이 없어 생략이 가능합니다. 두 번째 항을 최소화하기 위해서는 **$\log(1 - D(G(z)))$ 가 최소**가 되어야 합니다. 따라서 **$\log(1 - D(G(z)))$ 는 0**이 되어야 하고 $D(G(z))$ 는 1이 되어야 합니다. 이는 **판별자가 진짜로 분류할 만큼 완벽한 가짜 데이터를 생성하도록 생성자를 학습시키는 것을 의미합니다**. 이처럼 $V(D,G)$ 를 최대화하는 방향으로 분류자 D를 학습하고, $V(D,G)$ 를 최소화하는 방향으로 생성자를 학습하는 것을 Minmax problem이라고 합니다.

- <https://www.samsungsds.com/global/ko/support/insights/Generative-adversarial-network-AI.html>
- <https://www.samsungsds.com/global/ko/support/insights/Generative-adversarial-network-AI-2.html>
- <https://www.samsungsds.com/global/ko/support/insights/Generative-adversarial-network-AI-3.html>