1_Empirical_Risk_Minimization

문제 정의

- 일반적으로 인공지능 모델의 학습과정에서는 **손실 함수를 정의하고 이를 최소화하는 매개변수를 구하는 것을 목표**로 한다. 이러한 매개변수를 추정하기 위해 여러 기법이 사용되는데, 대표적인 예시로는 **MLE(Maximum Likilihood Estimation), MAP(Maximum A Posterior)**가 있다. **Empirical Risk Minimization은 MLE를 일반화하여 표현한 식으로, 손실 함수가 어떤 형태이든 적용할 수 있는 방법**이다. ERM은 기본적으로 **N개의 입력 데이터에 해당하는 Y를 추정하여 얻은 Loss들의 평균값**을 말한다. 이를 **분류 문제에 적용하면 N개의 분류 문제 중 제대로 분류하지 못한 것의 비율(Misclassification Rate)을 경험적 위험(Empirical Risk)으로 계산하여 이를 최소화하는 방식**으로 작용하여 매개변수를 추정한다. ERM은 이처럼 **한정된 훈련 데이터에서 경험적으로 추정한 데이터 생성 분포를 기반으로 전체 데이터 생성 분포에 근접한 매개변수를 추정하기 위해 제안**되었다. 이를 통해 **학습되지 않은 새로운 데이터에 대해서도 일반화 성능을 향상시키는 것을 목표**로 한다.

해당 문제에 대한 일반적인 접근

- ERM의 경험적 위험은 훈련 Dataset N개에 대한 손실 함수의 평균으로 다음과 같은 수식으로 정의된다. $R_{emp}(\theta) = \frac{1}{N}\Sigma_{n=1}^{N} l(y_n, \theta; x_n)$. 일반적으로 매개변수를 추정하기 위해서는 경사하강법과 같은 최적화 알고리즘을 적용하여 매개변수를 업데이트 한다. 이 과정에서 **경험적 위험에 대한 정보를 반영하기 위해 그라디언트에 경험적 위험을 곱하여 이를 손실 함수에 다음과 같은 수식처럼 반영**한다. $\theta \leftarrow \theta - \eta \nabla \theta R_{emp}(\theta)$. 이 과정을 반복하며 별도의 검증 데이터셋을 사용하여 추정된 매개변수를 가진 모델의 성능을 평가한다.

일반적인 접근법의 제한 사항

- ERM은 한정된 훈련 데이터의 분포에 대해 정의된 손실 함수를 기반으로 하기에 **과적합** 문제가 발생할 가능성이 있다. 그리고 대부분의 경우 **경험적 데이터에 따른 분포는 실제 분포와 동일하지 않다.** 이로 인해 모델이 학습하지 않은 데이터에 대해 잘못 예측할 수 있는데 이는 **일반화 성능이 낮다**는 것을 의미한다. 또한, 대부분의 최적화 기법이 경사 하강법을 기반으로 하기에 **손실 함수의 기울기가 0이거나 미분이 불가능하다면 이를 사용할 수 없다.** 대표적인 예로 **0-1 Loss**가 있다. 이는 모델의 출력이 실제값과 같으면 0, 다르면 1을 출력하는데 이러한 손실 함수는 대부분의 점에서 기울기가 0이기 때문에, **훈련하는 모델의 성능을 평가할 수는 있어도 어느 방향으로 가중치를 수정해야 경험적 위험을 줄일 수 있는지는 알기 어렵다.**

제한 사항에 대한 해결 방안

- 과적합의 경우, **정규화**를 통해 해결할 수 있다. 먼저 모델의 **복잡도에 대한 페널티를 손실 함수에 추가하는 방법**이 있다. 그 방식으로는 매개변수 벡터의 절대값의 합에 비례하는 페널티를 추가하여 일부 매개변수의 값을 작게 만들어 모델의 복잡성을 낮추는 **L1 정규화**, 그리고 매개변수 벡터의 제곱의 합에 비례하는 페널티를 추가하여 모델의 매개변수 값이 상대적으로 작게 유지되도록 하는 **L2 정규화**가 있다. 또다른 방식으로는 **검증 데이터셋**을 사용하는 방법이 있다. 그 중에서 **교차 검증 기법**의 경우, 모델을 학습하는 과정에서 **데이터를 여러 개로 나누고 이 중 일부를 훈련에 그리고 나머지를 검증으로 사용**하는 것이다. 이를 통해 각기 **다른 모델들을 여러 개 학습하여 평균, 최솟값 등의 기법으로 검증 데이터에 가장 높은 성능을 보이는 모델을 선택**한다. 학습 과정에서는 **이른 학습 중단 기법(Early Stopping)**을 통해 정규화를 할 수 있다. 이는 **훈련 과정에서 검증 데이터셋의 성능이 더 이상 개선되지 않을 때, 훈련을 멈추는 기법으로, 너무 많은 훈련 Epoch로 발생할 수 있는 과적합을 방지**하는데 도움이 될 수 있다. 마지막으로 학습 데이터에 무작위성의 변화를 추가하는 **데이터 증강 기법**을 이용하여 데이터의 수를 늘려 정규화할 수 있는 방법이 있다. 이처럼 모델의 매개변수를 줄이거나 데이터의 수를 늘리면 효과적으로 정규화를 할 수 있다.
- 손실 함수의 기울기가 0이 되는 문제의 경우 **대체 손실 함수 기법(Surrogate Loss)**을 통해 해결할 수 있다. 이는 0-1 Loss 처럼 Gradient가 0이 되는 부분이 많은 경우, 이를 **대신할 수 있는 손실 함수를 정의하여 이를**

대신 최소값으로 최적화시키는 기법이다. 이러한 대체 손실 함수의 예시로는 실제 레이블과 예측 확률 간의 차이를 로그 함수로 측정하는 **Logistic Loss**, SVM에서 마진 오류를 최소화하는 역할을 하는 **Hinge Loss** 등을 사용한다.