프라이버시 보장 기계학습을 위한 시그모이드 함수의 다항 근사에 관한 비교 분석

안선웅, 김용준*
포항공과대학교

{asw3148, yongjune}@postech.ac.kr

An Analysis of Polynomial Approximation of Sigmoid function for Privacy-Preserving Machine Learning

Sunwoong Ahn, Yongjune Kim*
Pohang University of Science and Technology (POSTECH)

요 약

시그모이드 활성함수(sigmoid activation function)는 기계학습에서 널리 사용되는 대표적인 비선형 함수로, 프라이버시 보장 기계학습(privacy-preserving machine learning; PPML)에서도 그 중요성이 점점 부각되고 있다. 그러나 동형암호 기반 프라이버시 보장 기계학습에서는 지원되는 연산이 덧셈과 곱셈에 국한되기 때문에, 시그모이드 함수에 포함된 지수 함수와 나눗셈 연산을 직접 적용하기 어렵다. 이에 따라, 시그모이드 함수를 덧셈 및 곱셈 연산만으로 표현 가능한 다항식으로 근사하는 과정이 필수적이다. 본 논문에서는 시그모이드에 대한 다양한 다항 근사 기법들을 소개하고, 각 방법의 특성과 근사 성능을 분석하고자 한다.

Ⅰ. 서론

최근 민감한 데이터를 보호하면서도 효율적인 학습과 추론을 가능하게 하는 프라이버시 보장 기계학습에 대한 관심이 높아지고 있다. 특히 연산 중에도 데이터를 암호화된 상태로 유지할 수 있는 동형암호 기반 기계학습은 높은 수준의 보안을 유지할 수 있는 기술로 주목받고 있다.

기계학습에서 활용되는 시그모이드 (sigmoid) 함수는 입력값을 0 과 1 사이의 값으로 대응시키는 활성함수로 다음과 같이 정의된다:

$$\sigma(x) = \frac{1}{1+\exp(-x)}$$

그러나 동형암호 환경에서는 덧셈과 곱셈만 허용되는 제약이 존재하므로, 지수 함수와 나눗셈 연산을 포함하는 시그모이드 함수를 직접 계산하기 어렵다. 따라서, 덧셈과 곱셈만으로 구성된 다항식으로의 근사가 필수적이다.

본 논문에서는 대표적인 다항 근사 기법인 최소제곱법 (least squares method), Remez 알고리즘, 그리고 Taylor 근사 기법을 통해 시그모이드 함수를 다항 근사하고, 비교 분석을 통해 목적 및 제약 조건에 따라 어떤 근사 기법이 적절한지 판단할 수 있는 기준을 제시하고자 한다.

Ⅱ. 본론

최소제곱법은 주어진 데이터 점들에서 함수와 근사 다항식 간의 오차 제곱합을 최소화하는 다항식을 구하는 방법이다. 주어진 입력-출력 데이터 쌍 (a_i, b_i) 에 대해 a_i 로부터 구성한 Vandermonde 행렬을 $\mathbf{A}$, b_i 에 대한 벡터를 $\mathbf{b}$, 다항식 계수 벡터를 $\mathbf{x}$라고 할 때, 최소제곱 문제는 다음의 목적 함수를 최소화하는 해를 구하는 것으로 정의된다:

$$\min_{\mathbf{x}} \|\mathbf{A}\mathbf{x} - \mathbf{b}\|^2$$

이 문제의 해는 정규 방정식(normal equation)을 통해 다음과 같은 해석적 해(analytical solution)로 주어진다 [1]:

$$\mathbf{x} = (\mathbf{A}^{\mathrm{T}}\mathbf{A})^{-1}\mathbf{A}^{\mathrm{T}}\mathbf{b}$$

Remez 알고리즘은 근사 구간 내에서 최대 절댓값 오차를 최소화하는 minimax 최적화 기법에 기반하며, 다음의 문제를 푼다:

$$\min_{p_n} \max_{x} |\sigma(x) - p_n(x)|$$

최적 다항식은 $n+2$ 개의 교대 지점에서 오차가 동일한 절댓값을 가지며 부호가 교차한다는 Remez 교환 정리에 따라 반복적으로 갱신된다. 이로 인해 비교적 낮은 차수의 다항식으로도 균일한 정확도를 확보할 수 있다 [2].

* Corresponding author

	n	Least Squares		Remez		Taylor	
		[-3, 3]	[-6, 6]	[-3, 3]	[-6, 6]	[-3, 3]	[-6, 6]
Uniform	3	4.17e-05	1.45e-03	4.89e-05	1.59e-03	7.64e-03	1.55
	5	1.07e-06	1.88e-04	1.23e-06	2.04e-04	2.45e-03	3.15e-02
	7	2.81e-07	2.50e-05	3.17e-08	2.70e-05	2.78e-03	2.12e-01
	9	7.54e-10	3.42e-05	8.14e-10	3.65e-06	2.77e-03	1.44e-01
	11	1.92e-11	4.62e-07	2.02e-11	4.83e-07	2.77e-03	1.52e-01
	13	5.48e-13	6.71e-08	5.68e-13	6.96e-08	2.77e-03	1.51e-01
	15	1.38e-14	8.73e-09	1.41e-14	8.81e-09	2.77e-03	1.51e-01
Gaussian $(\mu = 0, \sigma^2 = 1)$	3	3.74e-05	1.64e-03	4.73e-05	1.49e-03	7.21e-04	7.67e-04
	5	1.02e-06	2.45e-04	1.23e-06	2.03e-04	2.45e-04	2.54e-04
	7	2.71e-08	3.41e-05	3.23e-08	2.73e-05	2.74e-04	2.87e-04
	9	7.10e-10	4.64e-06	8.27e-10	3.64e-06	2.73e-04	2.85e-04
	11	1.87e-11	6.31e-07	2.14e-11	4.93e-07	2.73e-04	2.85e-04
	13	4.53e-13	8.63e-08	5.20e-13	6.73e-08	2.73e-04	2.85e-04
	15	1.17e-14	1.17e-08	1.35e-14	9.12e-09	2.73e-04	2.85e-04

Table 1 시그모이드 다항 근사기법들에 대한 비교

Taylor 근사는 주어진 점 근방에서 미분 가능한 함수에 대해, 해당 점에서의 함수값과 도함수 정보를 활용해 다항식 형태로 근사하는 방법이다. 근사 중심점 근처에서는 높은 정확도를 보이는 장점이 있지만, 근사 구간이 넓어질수록 성능이 저하될 수 있는 한계가 존재한다. 비교 분석에서는 0 에 대한 Taylor 전개식을 사용하였고 $\tilde{\sigma}$ 를 시그모이드에 대한 Taylor 전개를 이용한 다항 근사식이라고 하면 아래와 같이 표현될 수 있다 [3]:

$$\tilde{\sigma}(x) = \sum_{k=0}^{n} \frac{\sigma^{(n)}(0)}{k!} x^k$$

Ⅲ. 실험 결과

Table. 1 은 Uniform 분포 및 Gaussian 분포에서 샘플링된 입력값에 대해 각 다항 근사 기법의 성능을 비교한 결과를 나타낸다. n 은 근사 다항식의 차수를 의미하며, 좁은 구간([-3, 3])과 넓은 구간([-6, 6])에서 분석하였다. 평가 성능을 위한 오차로 대표적인 평균 제곱 오차(mean squared error)를 활용하였다.

최소제곱법은 샘플링 점들에 대한 오차를 최소화하기에 입력 분포가 학습 샘플과 유사할수록 오차가 작아진다. 주어진 구간을 균등 간격으로 분할하여 샘플 포인트를 생성하였기에 Uniform 분포 입력과 Gaussian 분포 입력에 대해서 Remez 알고리즘과 유사하거나 작은 오차를 발생시켰음을 확인할 수 있었다.

Remez 알고리즘은 최대 절댓값 오차를 최소화함으로써, 주어진 근사 구간 전반에 걸쳐 균형 잡힌 오차 분포와 높은 근사 정확도를 유지하였다. 본 실험에서는 Uniform 및 Gaussian 입력 분포 모두에 대해 최소제곱법과 유사하거나 그 이상의 성능을 보이는 것으로 확인되었다.

Taylor 근사는 특정 지점(예: 0) 근방에서는 높은 정확도를 보이나, 구간이 넓어질수록 오차가 급격히 증가하여서 전역적인 근사에는 부적합하였다.

따라서 좁은 구간에서는 테일러 근사가, Uniform 분포 입력 및 Gaussian 분포 입력에 대해서는 Remez 알고리즘 또는 최소제곱법이 효과적이었다.

Ⅳ. 결론

본 논문에서는 시그모이드 활성함수에 대한 근사기법들을 소개하고 실험을 통해 비교 분석하였다. 본 연구는 프라이버시 보장 기계학습 환경에서 주어진 제약 조건과 목적에 따라 적절한 다항 근사 기법을 선택하는 데 실질적인 기준을 제공할 수 있다.

ACKNOWLEDGMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No. 2024-00399401, 양자안전 보안인프라 전환 및 대양자 복합 안정성 검증기술 개발).

참 고 문 헌

[1] S. H. Friedberg, A. J. Insel, and L. E. Spence, “Linear Algebra,” Englewood Cliffs, NJ: Prentice Hall, 1989.

[2] E. Cheney, “Introduction to approximation theory,” New York: McGraw−Hill, 1966.

[3] R. L. Burden and J. D. Faires, “Numerical Analysis,” Boston, MA: Brooks/Cole, 2011.