2020.02.21. HCAI Open Seminar

Open Set Recognition In Deep Networks

김상훈



CONTENTS

- ◆ 이해를 돕기 위한 배경지식 설명
 - (1) 기계학습의 분류
 - (2) 심층신경망에서의 분류모델
- ◆ 심층신경망 분류모델의 한계
- ◆ Open Set Recognition의 개념
- ◆ OpenMax : 실제 알고리즘을 통해 심층신경망에서의 거리기반 Open Set Recognition

 N_2

 N_n

(1) 기계학습의 분류

훈련 데이터의 형태에 따라

비지도학습

X ₁	X_2	 X_{P}

지도학습

	X ₁	X ₂	 X _P		Y
N_1			 		
N_2			 	$\xrightarrow{Function}$	
			 	Y = F(X)	
N_n			 		

지도학습 내에서도 Ү변수의 형태에 따라

회귀모델

예시)

• 기상 데이터로 주가를 예측 하는 문제

・분류모델

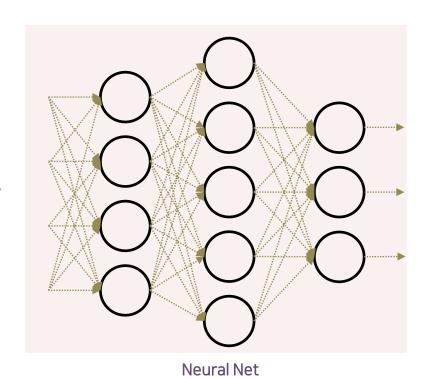
예시)

• 이미지 데이터로 고양이, 강아지를 분류하는 문제

(2) 심층신경망에서의 분류모델

Input X





Output Y

 Y

 강아지

 토끼

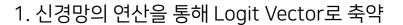
 강아지

 ···

 토끼

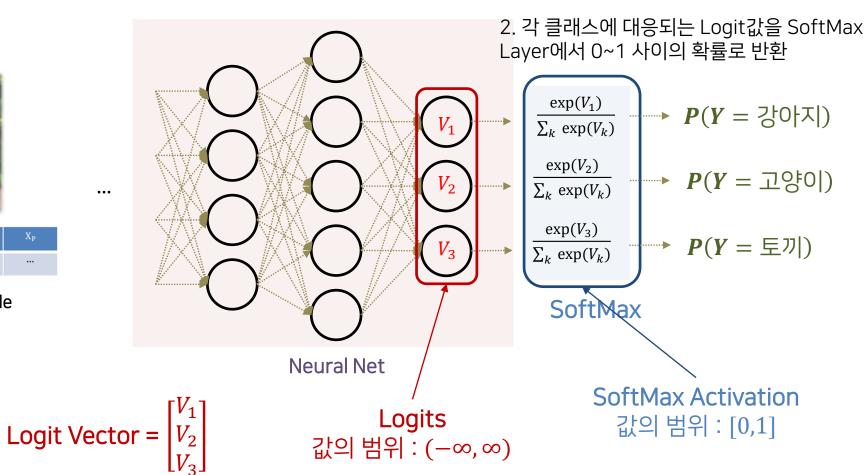
 고양이

고양이

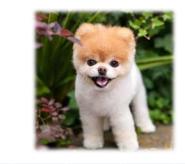




Pixel by pixel variable

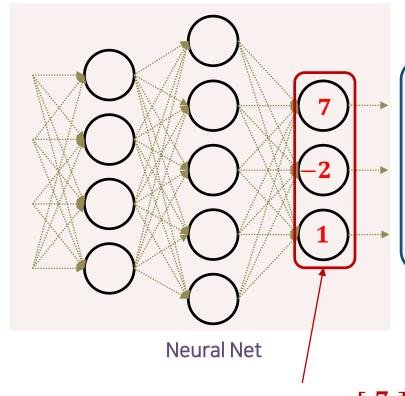


(2) 심층신경망에서의 분류모델

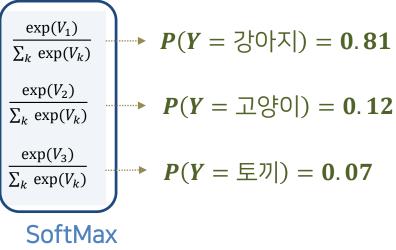


	X ₁	X_2	 Х _Р
N_1			

Pixel by pixel variable

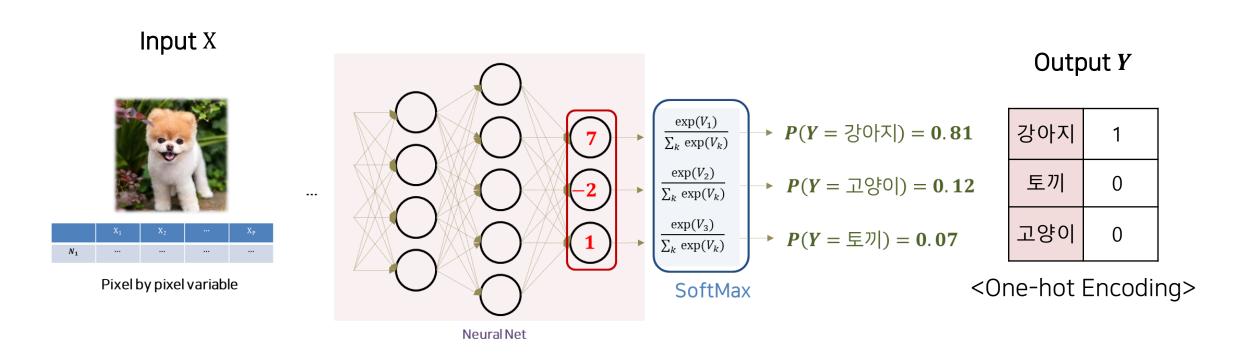


Logit 값이 클수록, 더 큰 확률을 가짐 (Logit 값은 각 클래스의 확률에 대응하는 값)



$$Logit Vector = \begin{bmatrix} 7 \\ -2 \\ 1 \end{bmatrix}$$

(2) 심층신경망에서의 분류모델



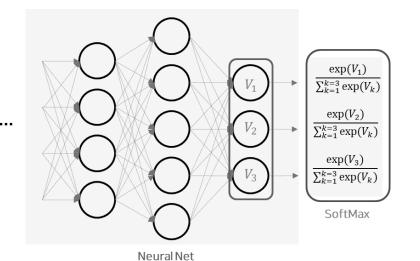
Output 값과 신경망이 출력하는 확률 중 가장 큰 확률을 가지는 클래스가 일치하도록 학습을 진행

(2) 심층신경망에서의 분류모델

Input X



	X ₁	X ₂	 X _P
N_1			 ***
N_2			
N_n			



모든 학습 데이터로 학습진행

Output Y

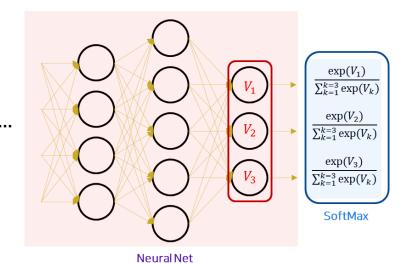
obs	강아지	고양이	토끼
N_1	1	0	0
N_2	0	1	0
•••	•••	•••	•••
N_n	0	0	1

(2) 심층신경망에서의 분류모델

Input X



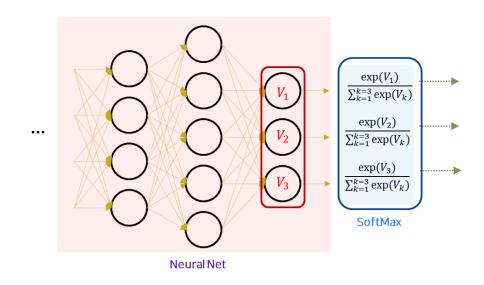
	X ₁	X ₂	 X _P
N_1			 ***
N_2			
N_n			



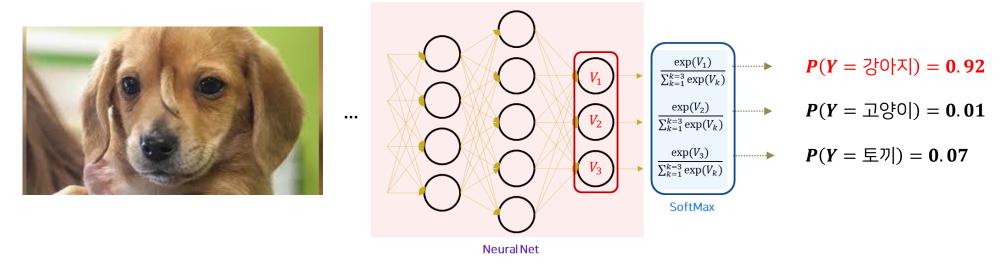
모든 학습 데이터로 학습완료

Output Y

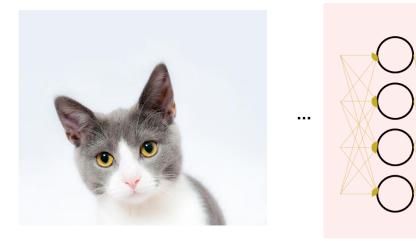
obs	강아지	고양이	토끼
N_1	1	0	0
N_2	0	1	0
***	***	***	
N_n	0	0	1

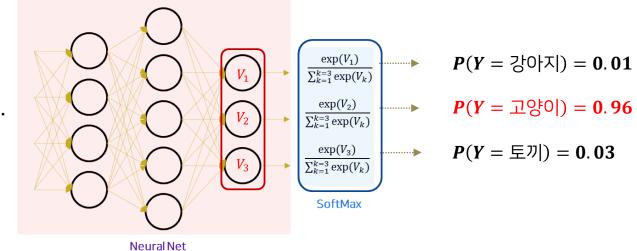


분류기(Classifier) 생성

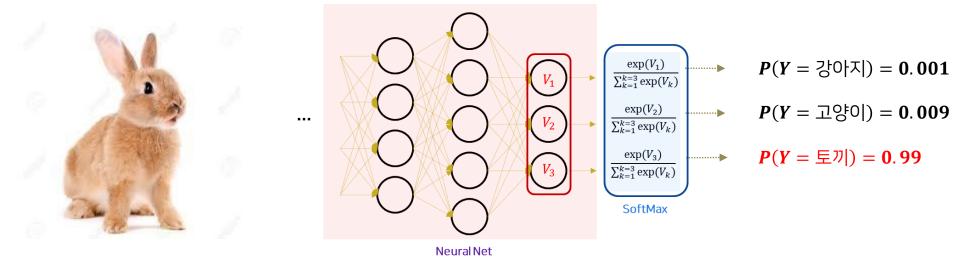


강아지/고양이/토끼 분류기





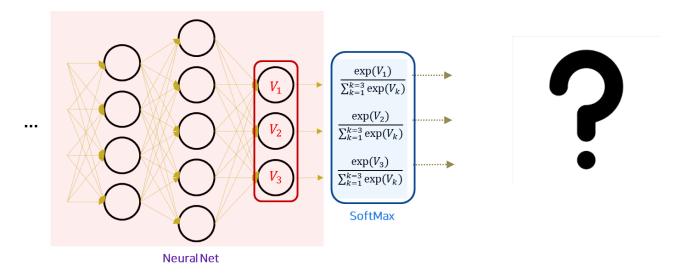
강아지/고양이/토끼 분류기



강아지/고양이/토끼 분류기

학습 단계에서 학습하지 않은 클래스의 데이터가 들어온다면?

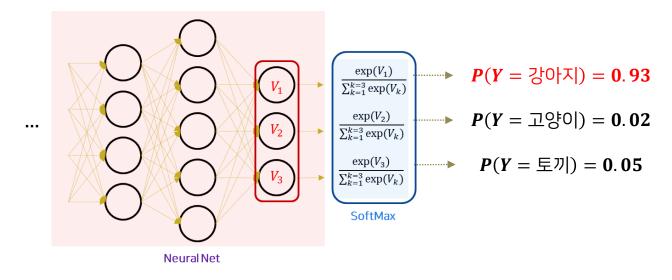




강아지/고양이/토끼 분류기

학습 단계에서 학습하지 않은 클래스의 데이터가 들어온다면?





강아지/고양이/토끼 분류기

분류기는 학습한 클래스에 대한 확률만 출력할 수 있다.

- Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images
 - 2015년 CVPR(Computer Vision and Pattern Recognition)에서 발표된 논문
 - 2020년 2월 20일 기준 1,553회 인용

Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images

Anh Nguyen University of Wyoming

anguyen8@uwyo.edu

Jason Yosinski Cornell University

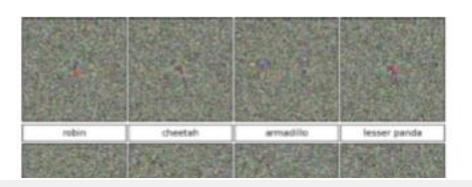
yosinski@cs.cornell.edu

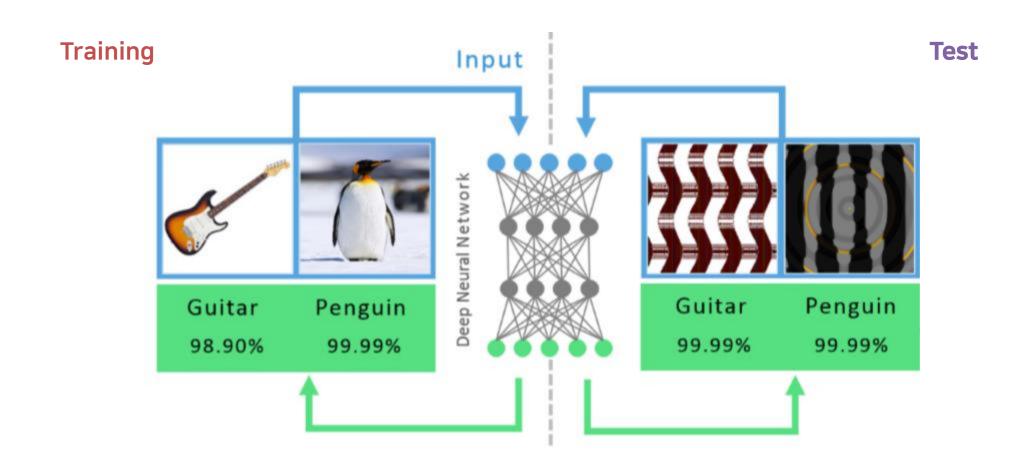
Jeff Clune University of Wyoming

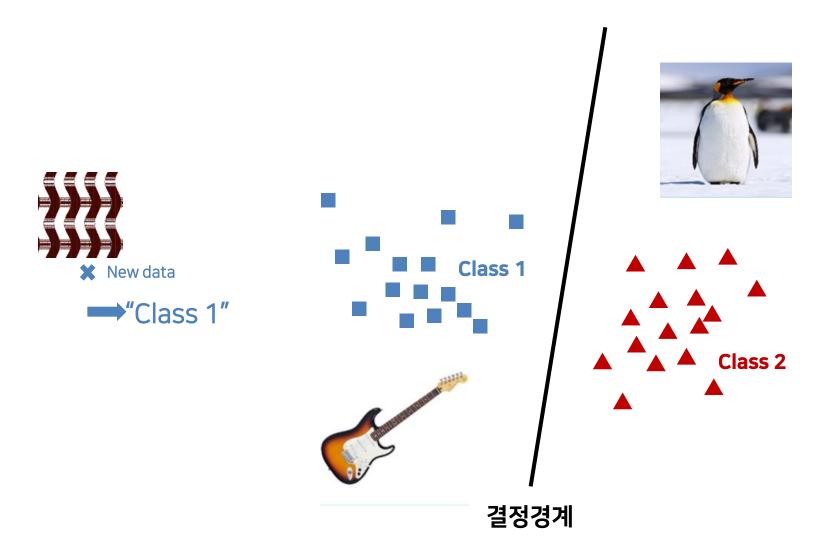
jeffclune@uwyo.edu

Abstract

Deep neural networks (DNNs) have recently been achieving state-of-the-art performance on a variety of pattern-recognition tasks, most notably visual classification problems. Given that DNNs are now able to classify objects in images with near-human-level performance, questions



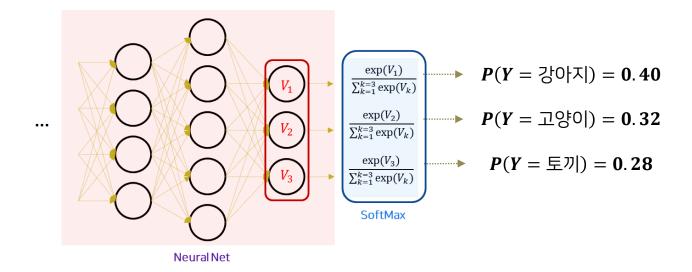






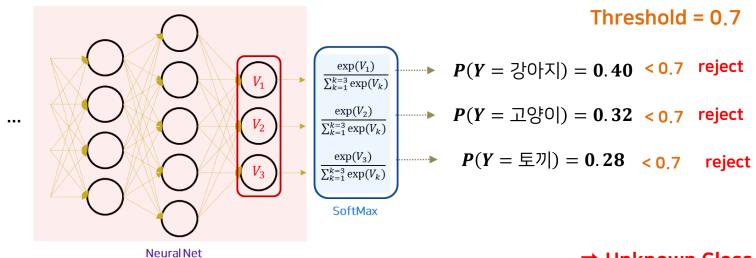
만약 SoftMax가 출력한 확률이 모두 낮다면?



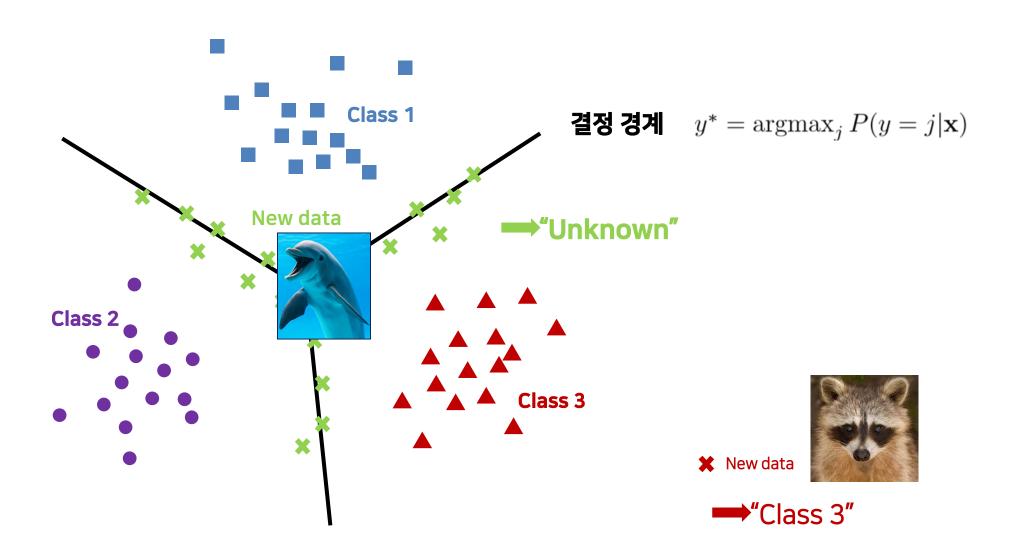


만약 SoftMax가 출력한 확률이 모두 낮다면?

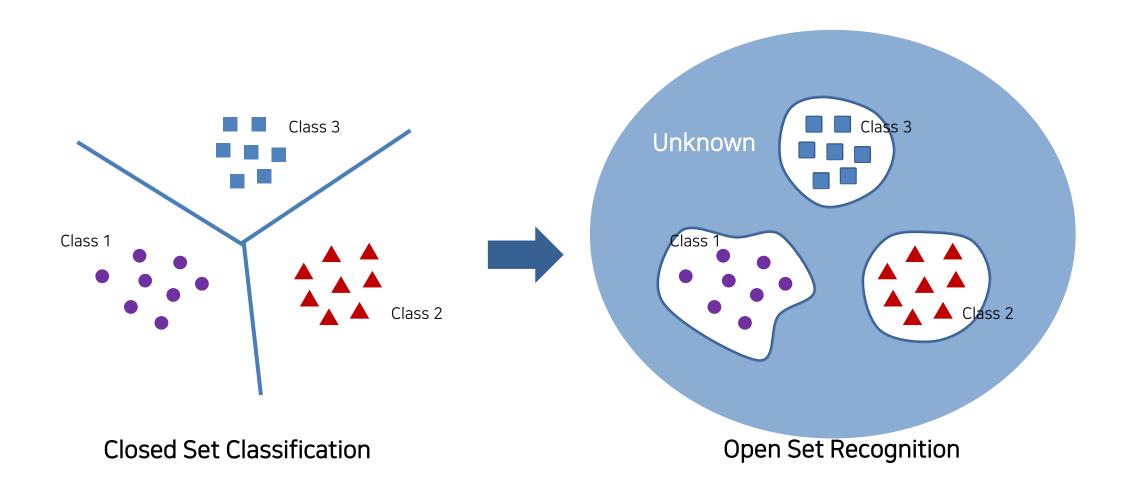




→ Unknown Class



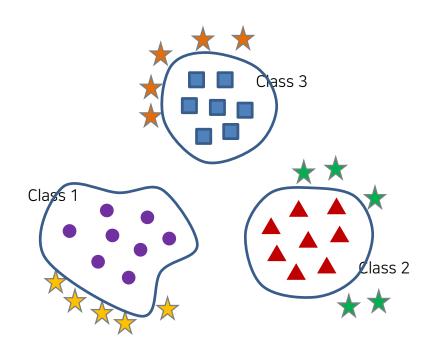
Open Set Recognition의 개념



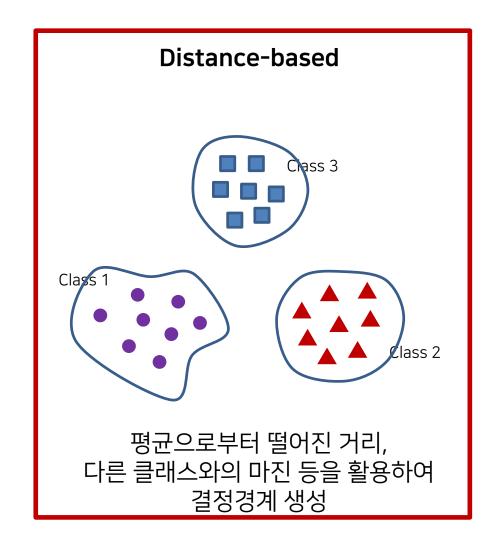
Open Set Recognition의 개념

❖ Open Set Recognition의 분류

Adversarial Learning-based



GAN 등의 생성모델을 통해 각 클래스와 비슷한 다른 이미지들을 생성하여 새로운 클래스로 추가하여 학습



Towards open set deep networks

- 2016년 CVPR(Computer Vision and Pattern Recognition)에서 발표된 논문
- 저자 Bendale A, Boult T
 - Toward Open Set Recognition, **Scheirer W J**, de Rezende Rocha A, Sapkota A, et al. (PAMI, 2013)에서 **Open Set Recognition을 처음 정의**
- Open Set Recognition을 심층신경망에 처음 적용한 연구
- 2020년 2월 20일 기준 218회 인용

Towards Open Set Deep Networks

Abhijit Bendale*, Terrance E. Boult University of Colorado at Colorado Springs

{abendale,tboult}@vast.uccs.edu

Abstract

Deep networks have produced significant gains for various visual recognition problems, leading to high impact academic and commercial applications. Recent work in deep networks highlighted that it is easy to generate images that humans would never classify as a particular object class, yet networks classify such images high confidence as that given class – deep network are easily fooled with images humans do not consider meaningful. The closed set nature of deep networks forces them to choose from one of the known classes leading to such artifacts. Recognition in

vision and learning. Recent research in deep networks has significantly improved many aspects of visual recognition [26, 3, 11]. Co-evolution of rich representations, scalable classification methods and large datasets have resulted in many commercial applications [5, 28, 16, 6]. However, a wide range of operational challenges occur while deploying recognition systems in the dynamic and ever-changing real world. A vast majority of recognition systems are designed for a static closed world, where the primary assumption is that all categories are known a priori. Deep networks, like many classic machine learning tools, are designed to perform closed set recognition.

❖ OpenMax 알고리즘

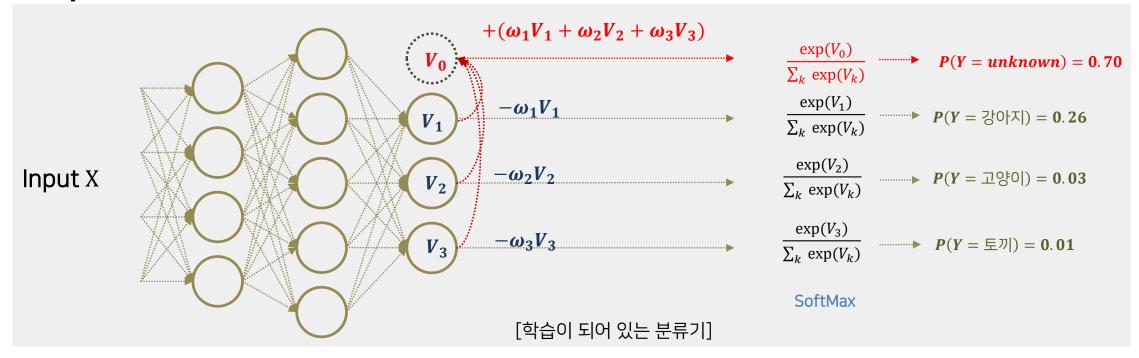


❖ OpenMax 알고리즘



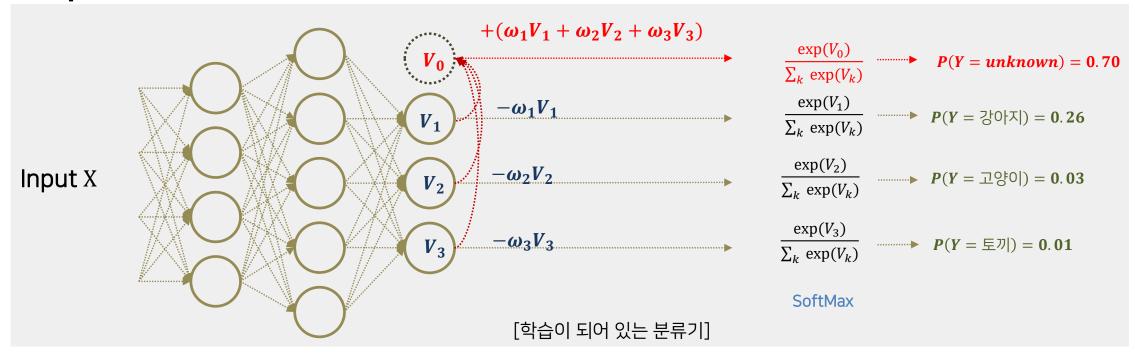
• $V_0 = unknown \ class$ 에 대응되는 Logit 값

❖ OpenMax 알고리즘



- $V_0 = unknown \ class$ 에 대응되는 Logit 값
- $\omega_k = 분류기가 k class로 잘못 분류했을 확률에 대응하는 가중치$

❖ OpenMax 알고리즘



ω_k 를 어떻게 정의할 수 있을까?

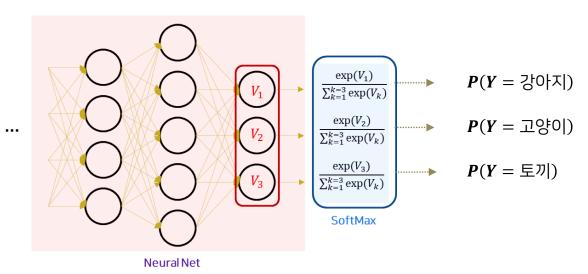
보 논문에서는 Extreme Value Theorem에 기반하여 각 클래스 별 평균 Logit Vector로부터의 거리에 대한 국단값(이상치)의 분포를 통해 ω_k 를 정의한다.

STEP1. 학습 데이터 중 분류기가 정확하게 분류한 데이터를 선별

Input X in Training data

	<i>X</i> ₁	X_2		X_P
N_1	•••			
N_2	•••	•••	•••	
	•••	•••	•••	•••
N_{n}				





강아지/고양이/토끼 분류기

STEP2. STEP1에서 선별된 데이터의 X데이터를 클래스별로 데이터를 분리

	X_1	X_2	 X_{P}
<i>N</i> ₁₁			
N_{12}			
N_{1a}			

	X_1	X_2	 X_P
N_{21}			
N ₂₂			
N_{2b}			

<강아지 클래스 데이터>

<고양이 클래스 데이터>

	X_1	X_2	 X_{P}
N ₃₁			
N_{32}			
N _{3c}			

<토끼 클래스 데이터>

STEP3. 각 클래스 별로 선별된 데이터를 이용하여 Logit Vector 계산

	<i>X</i> ₁	X_2	 X_P
N_1			
N_2			
N_a			

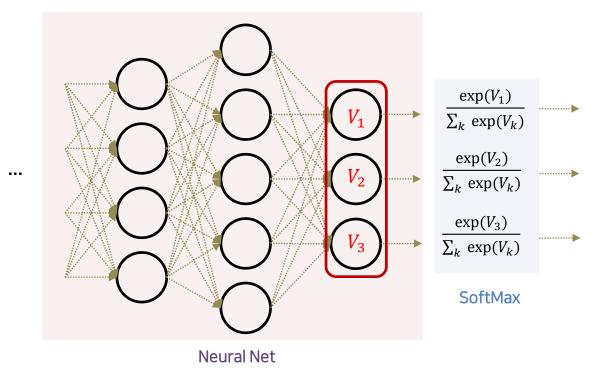
선별된 강아지 클래스 데이터

	X_1	X_2	 X_P
N ₂₁			
N ₂₂			
N_{2b}			

선별된 고양이 클래스 데이터

	X_1	X_2	 X_P
N ₃₁			
N ₃₂			
N _{3c}			

선별된 토끼 클래스 데이터



강아지/고양이/토끼 분류기

STEP3. 각 클래스 별로 선별된 데이터를 이용하여 Logit Vector 계산

Obs.	V_1	V_2	V_3
N ₁₁	9.87	-2.13	-6.23
N_{12}	18.5	3.18	4.98
N_{1a}	4.89	-3.91	1.01

<강아지 클래스 Logit Vector Matrix>

Obs.	V_1	V_2	V_3
<i>N</i> ₃₁	-3.23	-1.23	6.98
N ₃₂	1.52	1.52	9.78
N _{3c}	5.72	3.12	11.2

<토끼 클래스 Logit Vector Matrix>

Obs.	V_1	V_2	V_3
N ₂₁	2.17	8.29	-1.32
N ₂₂	1.89	9.13	2.11
N_{2b}	-3.14	5.42	1.35

<고양이 클래스 Logit Vector Matrix>

STEP4. 각 클래스 별 Logit Vector의 평균 계산

Obs.	V_1	V_2	V_3
N ₁₁	9.87	-2.13	-6.23
N_{12}	18.5	3.18	4.98
N_{1a}	4.89	-3.91	1.01

$$\overline{V_1} = 5.12$$
 $\overline{V_2} = -1.12$ $\overline{V_3} = 0.12$

<강아지 클래스 Logit Vector Matrix>

$$\mu_{rabit} = \begin{bmatrix} 1.32 \\ -2.35 \\ 9.32 \end{bmatrix}$$

<토끼 클래스 평균 Logit Vector>

$$\mu_{cat} = \begin{bmatrix} 0.12 \\ 11.27 \\ -3.53 \end{bmatrix}$$

<고양이 클래스 평균 Logit Vector>

$$\mu_{dog} = \begin{bmatrix} 5.12 \\ -1.12 \\ 0.12 \end{bmatrix}$$

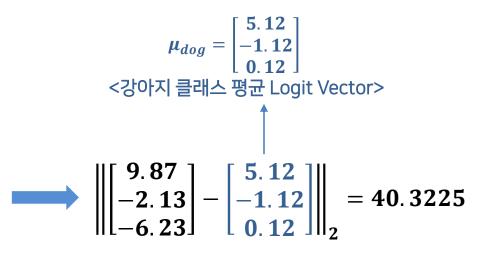
<강아지 클래스 평균 Logit Vector>

STEP5. 각 클래스 별 평균 Logit Vector와의 거리 계산

Obs.	V_1	V_2	V_3
N ₁₁	9.87	-2.13	-6.23
N_{12}	18.5	3.18	4.98
N_{1a}	4.89	-3.91	1.01

$$\overline{V_1} = 5.12$$
 $\overline{V_2} = -1.12$ $\overline{V_3} = 0.12$

<강아지 클래스 Logit Vector Matrix>

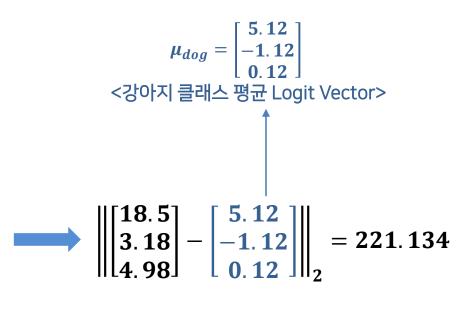


STEP5. 각 클래스 별 평균 Logit Vector와의 거리 계산

Obs.	V_1	V_2	V_3
N ₁₁	9.87	-2.13	-6.23
N_{12}	18.5	3.18	4.98
N_{1a}	4.89	-3.91	1.01

$$\overline{V_1} = 5.12$$
 $\overline{V_2} = -1.12$ $\overline{V_3} = 0.12$

<강아지 클래스 Logit Vector Matrix>



STEP5. 각 클래스 별 평균 Logit Vector와의 거리 계산

Obs.	V_1	V_2	V_3
N ₁₁	9.87	-2.13	-6.23
N_{12}	18.5	3.18	4.98
N_{1a}	4.89	-3.91	1.01

$$\overline{V_1} = 5.12$$
 $\overline{V_2} = -1.12$ $\overline{V_3} = 0.12$

<강아지 클래스 Logit Vector Matrix>

$$\mu_{dog} = \begin{bmatrix} 5.12 \\ -1.12 \\ 0.12 \end{bmatrix}$$
 <강아지 클래스 평균 Logit Vector>
$$\begin{bmatrix} 4.89 \\ -3.91 \\ 1.01 \end{bmatrix} - \begin{bmatrix} 5.12 \\ -1.12 \\ 0.12 \end{bmatrix} \Big|_2 = 8.6291$$

STEP5. 각 클래스 별 평균 Logit Vector와의 거리 계산

Obs.	평균 Logit Vector와의 거리
N ₁₁	221. 134
N ₁₂	217. 532
N_{1a}	0.014

Obs.	평균 Logit Vector와의 거리
N_{21}	195.312
N_{22}	194.904
N_{2b}	0.082

Obs.	평균 Logit Vector와의 거리
N ₃₁	139.641
N_{32}	121.896

N _{3c}	0.167

평균 Logit Vector와의 거리 내림차순 정렬

STEP6. 평균 Logit Vector와의 거리 중 가장 큰 η (=20)개 Sample 각 클래스 별로 추출

Obs.	평균 Logit Vector와의 거리	
N ₁₁	221.134	- 평균 Logit Vector와의 거리 중
<i>N</i> ₁₂	217.532	가장 큰 η (=20)개 Sample 추출
N_{1a}	0.014	
		[221.134,217.532, ··· ,197.423]

Extreme Value Theorem (the Fisher-Tippet Theorem)

Let $X_1,X_2\ldots,X_n\ldots$ be a sequence of independent and identically-distributed random variables, and $M_n=\max\{X_1,\ldots,X_n\}$. If a sequence of pairs of real numbers (a_n,b_n) exists such that each $a_n>0$ and $\lim_{n\to\infty}P\left(\frac{M_n-b_n}{a_n}\leq x\right)=F(x)$, where F is a non-degenerate

distribution function, then the limit distribution F belongs to either the Gumbel, the Fréchet or the Weibull family^[4]. These can be grouped into the generalized extreme value distribution.



동일분포에서 독립적으로 추출한 변수의 샘플 중 가장 큰 값을 뽑으면, <mark>가장 큰 값보다 클 확률</mark>은 Weibull 분포, Frechet 분포, Gumbel 분포의 형태로 만들 수 있다.



· 극단값의 분포, 이상치의 분포 추정

$$F(x;\mu,\sigma,0)=e^{-e^{-(x-\mu)/\sigma}} \quad ext{for} \;\; x \in \mathbb{R}.$$
Gumbel 분포

$$F(x;\mu,\sigma,\xi) = egin{cases} e^{-y^{-lpha}} & y>0 \ 0 & y\leq 0. \end{cases}$$

Frechet 분포

$$F(x;\mu,\sigma,\xi) = egin{cases} e^{-(-y)^lpha} & y < 0 \ 1 & y \geq 0 \end{cases}$$

Weibull 분포

- Fisher, R. A. (1930). The Genetical Theory of Natural Selection. Oxford: Oxford University Press.
- de Haan, Laurens; Ferreira, Ana (2006). Extreme Value Theory: An Introduction. New York: Springer. pp. 6–12. ISBN 0-387-34471-3.

Extreme Value Theorem (the Fisher-Tippet Theorem)

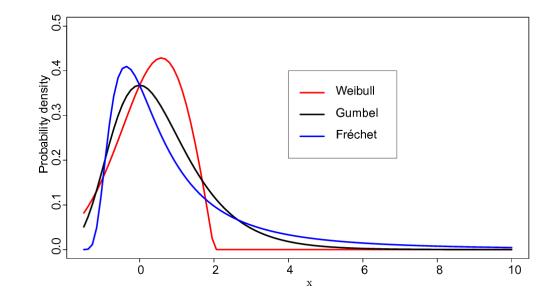
Let $X_1, X_2 \ldots, X_n \ldots$ be a sequence of independent and identically-distributed random variables, and $M_n = \max\{X_1, \ldots, X_n\}$. If a sequence of pairs of real numbers (a_n, b_n) exists such that each $a_n > 0$ and $\lim_{n \to \infty} P\left(\frac{M_n - b_n}{a_n} \le x\right) = F(x)$, where F is a non-degenerate distribution function, then the limit distribution F belongs to either the Gumbel, the Fréchet or the Weibull family^[4]. These can be grouped into the generalized extreme value distribution.

 \longrightarrow

동일분포에서 독립적으로 추출한 변수의 샘플 중 가장 큰 값을 뽑으면, 가장 큰 값보다 클 확률은 Weibull 분포, Frechet 분포, Gumbel 분포의 형태로 만들 수 있다.



극단값의 분포, 이상치의 분포 추정



- Fisher, R. A. (1930). The Genetical Theory of Natural Selection. Oxford: Oxford University Press.
- de Haan, Laurens; Ferreira, Ana (2006). Extreme Value Theory: An Introduction. New York: Springer. pp. 6–12. ISBN 0-387-34471-3.

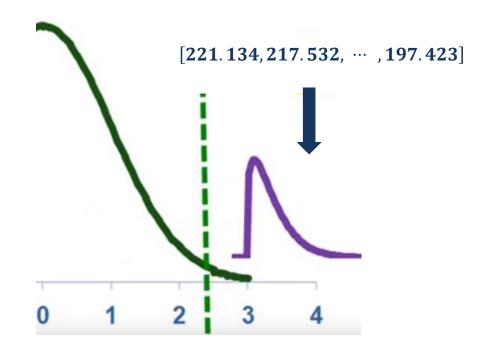
Extreme Value Theorem (the Fisher-Tippet Theorem)

Let $X_1, X_2 \ldots, X_n \ldots$ be a sequence of independent and identically-distributed random variables, and $M_n = \max\{X_1, \ldots, X_n\}$. If a sequence of pairs of real numbers (a_n, b_n) exists such that each $a_n > 0$ and $\lim_{n \to \infty} P\left(\frac{M_n - b_n}{a_n} \le x\right) = F(x)$, where F is a non-degenerate

distribution function, then the limit distribution F belongs to either the Gumbel, the Fréchet or the Weibull family^[4]. These can be grouped into the generalized extreme value distribution.

동일분포에서 독립적으로 추출한 변수의 샘플 중 가장 큰 값을 뽑으면, 가장 큰 값보다 클 확률은 Weibull 분포, Frechet 분포, Gumbel 분포의 형태로 만들 수 있다.

➡➡ 극단값의 분포, 이상치의 분포 추정



가장 큰 η (=20)개 Sample로 최대 가능도 추정을 통해 분포의 파라미터를 추정.

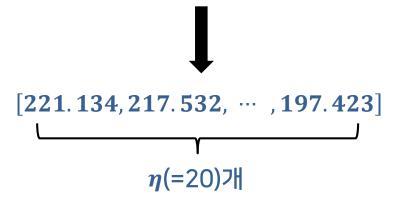
- Fisher, R. A. (1930). The Genetical Theory of Natural Selection. Oxford: Oxford University Press.
- de Haan, Laurens; Ferreira, Ana (2006). Extreme Value Theory: An Introduction. New York: Springer. pp. 6–12. ISBN 0-387-34471-3.

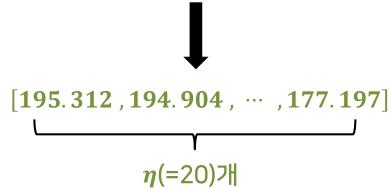
STEP7. **각 클래스별로 평균** Logit Vector**와의 거리 중 가장 큰 η개로** Weibull **분포(극단치 분포) 생성**

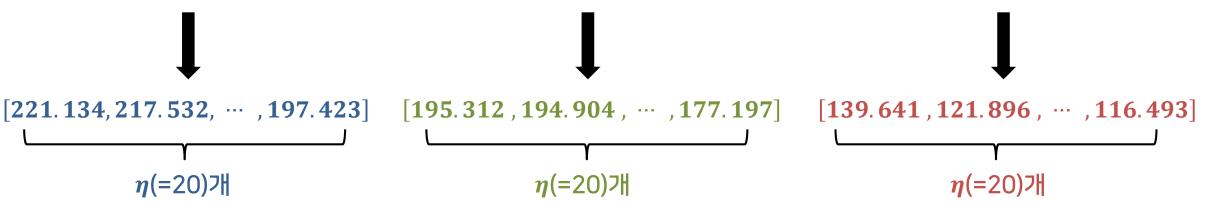
Obs.	평균 Logit Vector와의 거리
N_{11}	221.134
N_{12}	217.532
N_{1a}	0.014

Obs.	평균 Logit Vector와의 거리
N ₂₁	195.312
N ₂₂	194.904
•••	
N_{2b}	0.082

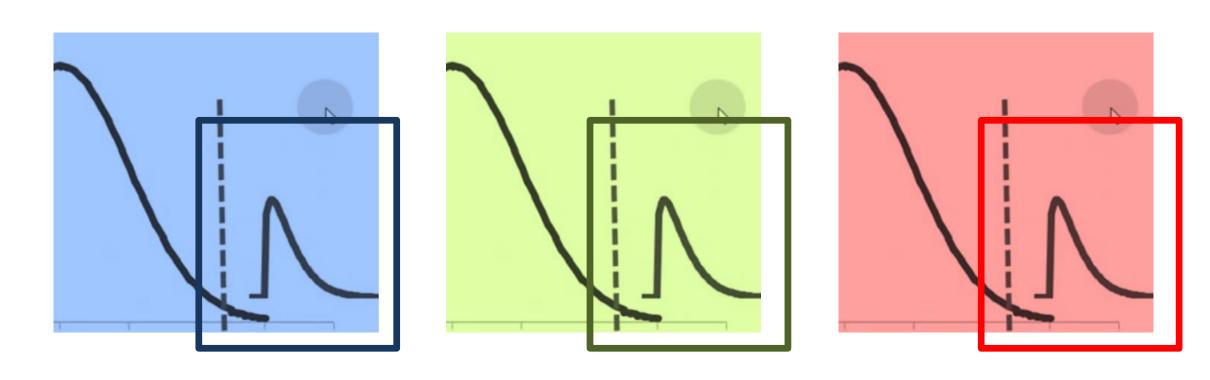
Obs.	평균 Logit Vector와의 거리	
N ₃₁	139.641	
N_{32}	121.896	
N _{3c}	0.167	







STEP7. 각 클래스별로 평균 Logit Vector와의 거리 중 가장 큰 η 개로 Weibull 분포(극단치 분포) 생성

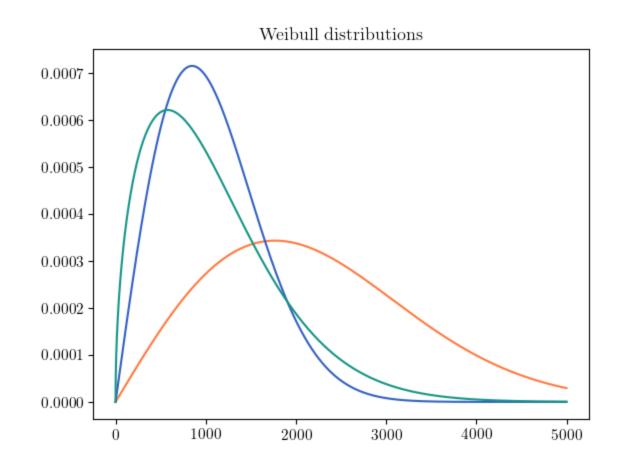


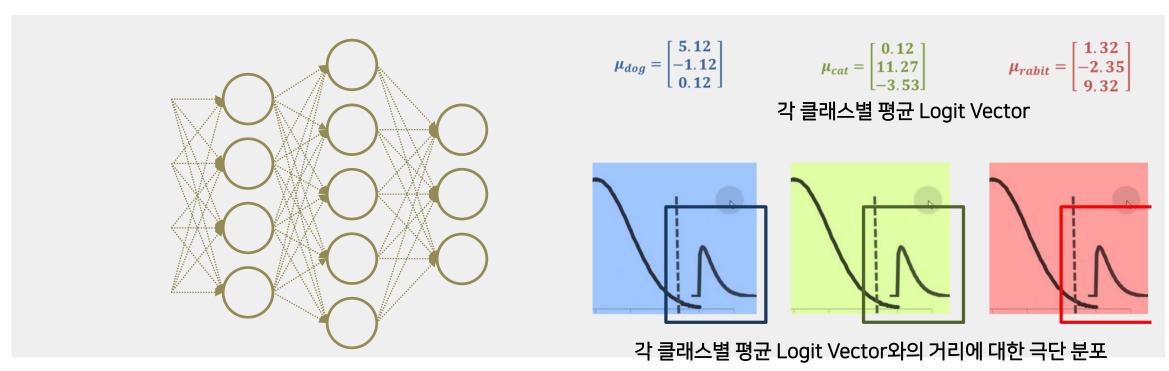
각 클래스별 평균 Logit Vector와의 거리의 극단 분포

※ 주의. 각 분포는 모두 scale과 shape이 다른 분포



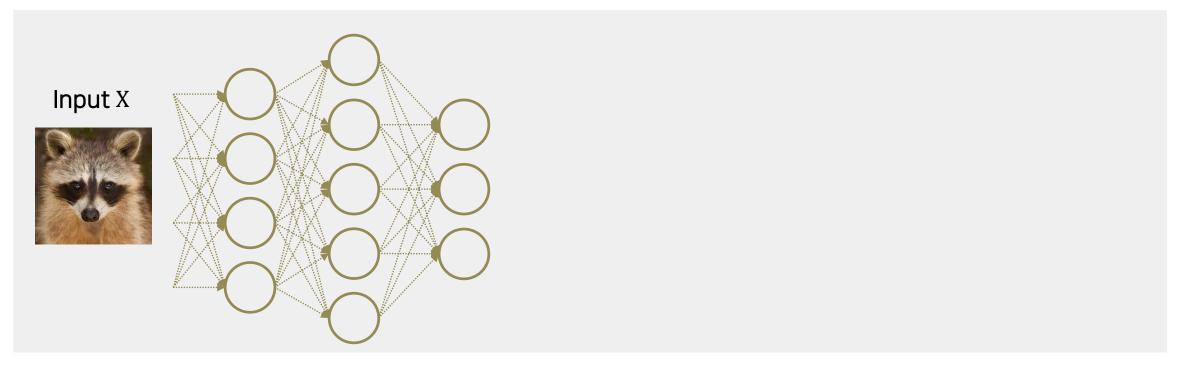
STEP7. 각 클래스별로 평균 Logit Vector와의 거리 중 가장 큰 η 개로 Weibull 분포(극단값의 분포) 생성





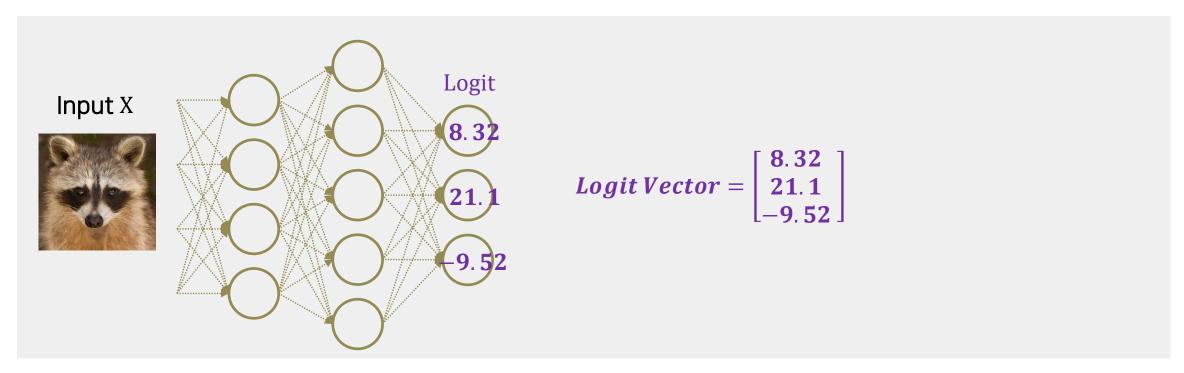
강아지/고양이/토끼 분류기

STEP1. 구축된 신경망에 테스트 데이터를 입력



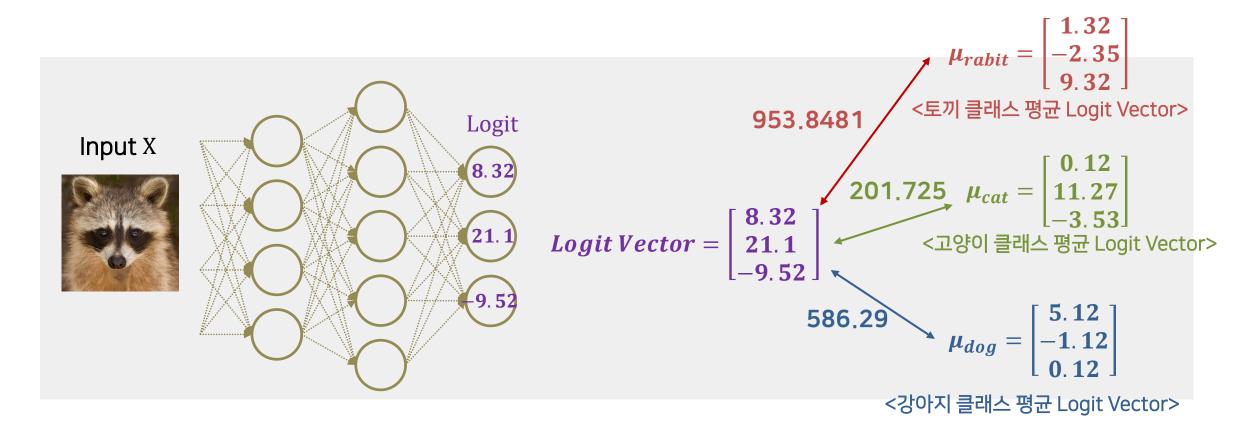
강아지/고양이/토끼 분류기

STEP2. 입력 데이터의 Logit Vector 계산 후 각 클래스별 평균 Logit Vector와의 거리 각각 계산



강아지/고양이/토끼 분류기

STEP2. 입력 데이터의 Logit Vector 계산 후 각 클래스별 평균 Logit Vector와의 거리 각각 계산

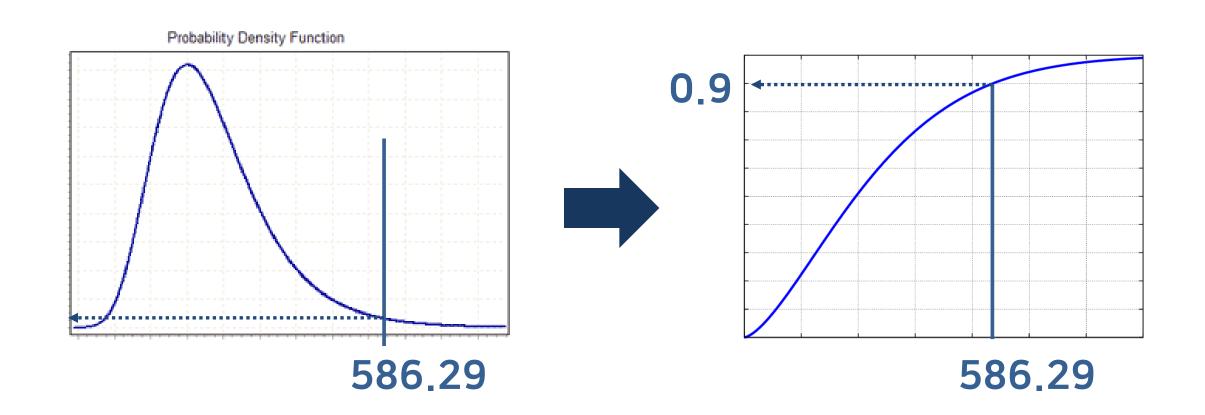


STEP3. 각각의 극단 분포의 CDF를 통해 각 클래스 평균 Logit Vector와의 거리의 극단 확률 계산



※ 주의. 각 분포는 모두 scale과 shape이 다른 분포

STEP3. 각각의 극단 분포의 CDF를 통해 각 클래스 평균 Logit Vector와의 거리의 극단 확률 계산

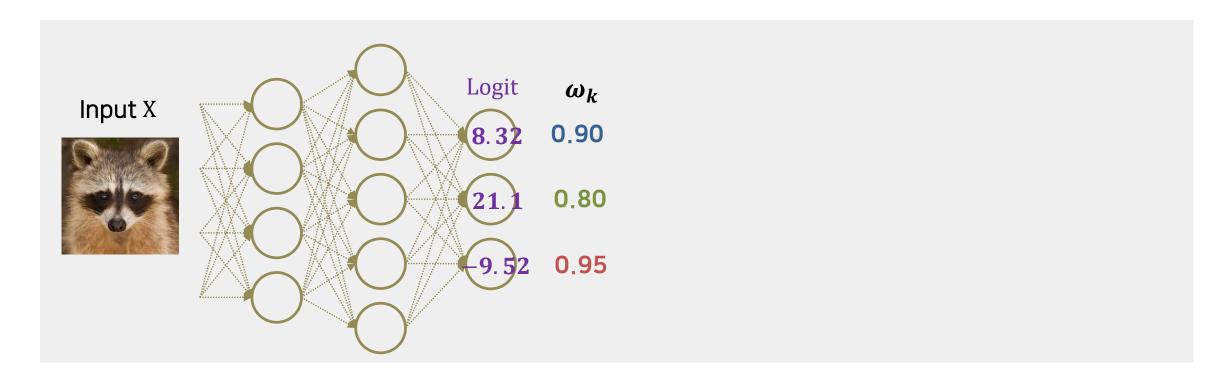


STEP3. 각각의 극단 분포의 CDF를 통해 각 클래스 평균 Logit Vector와의 거리의 극단 확률 계산

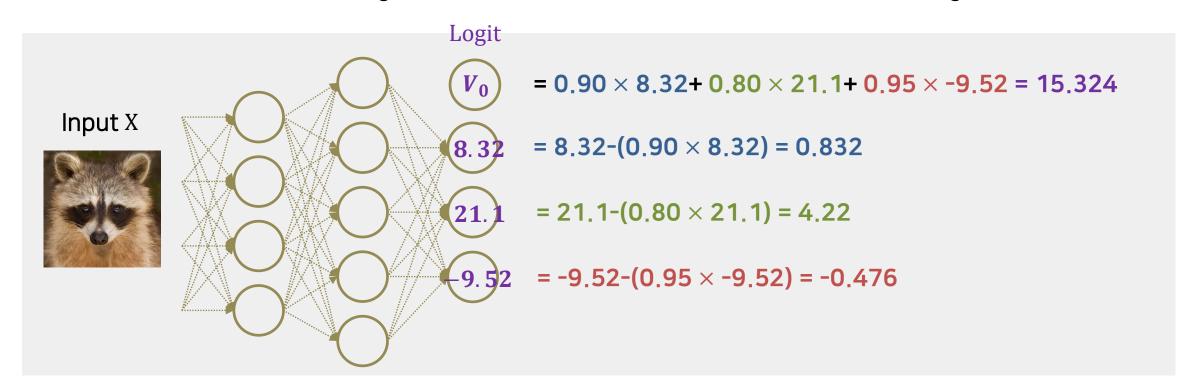


※ 주의. 각 분포는 모두 scale과 shape이 다른 분포

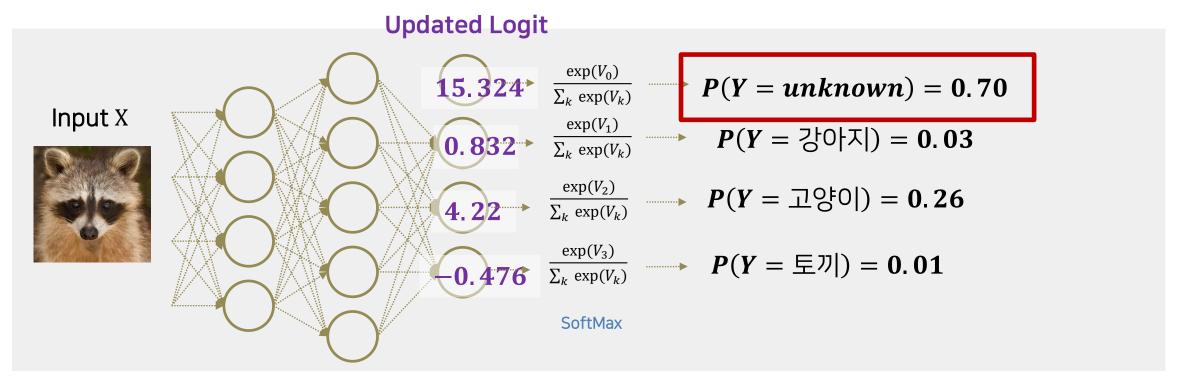
STEP4. 극단분포의 CDF 값(Logit Vector가 해당 클래스가 아닐 확률)을 ωk로 두어 Logit Vector 업데이트



STEP4. **극단분포의** CDF **값**(Logit Vector**가 해당 클래스가 아닐 확률)을** ω_k로 두**어** Logit Vector **업데이**트

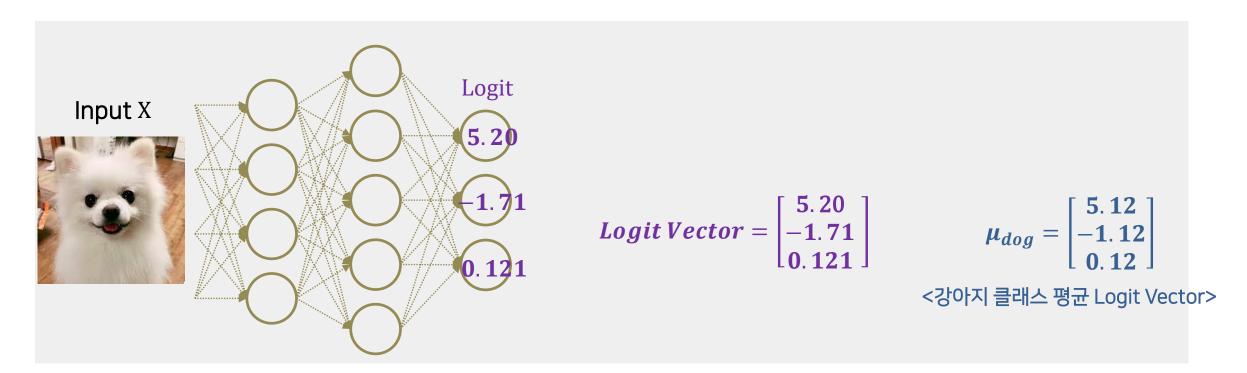


STEP5. 업데이트 된 Logit Vector를 SoftMax Layer에 통과 시켜 결과 도출

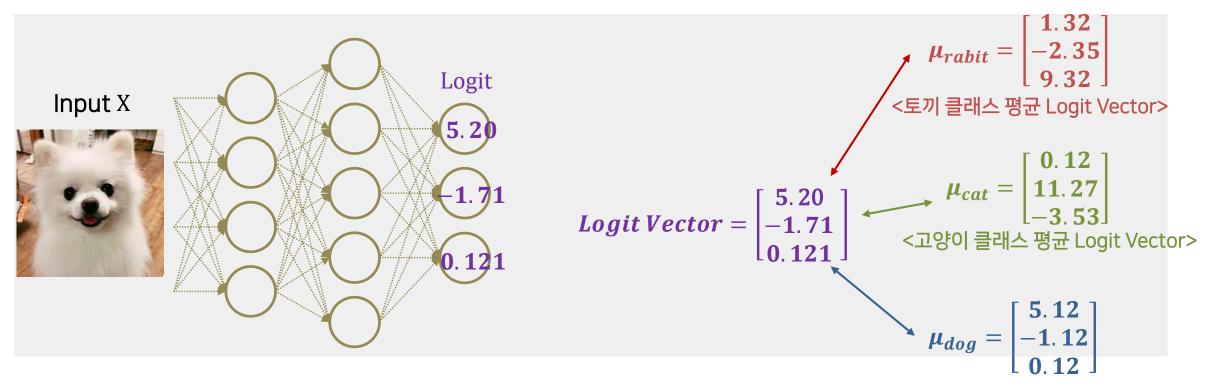


→Unknown Class

STEP4. **극단분포의** CDF **값**(Logit Vector**가 해당 클래스가 아닐 확률)을 ω**k로 두**어** Logit Vector **업데이**트

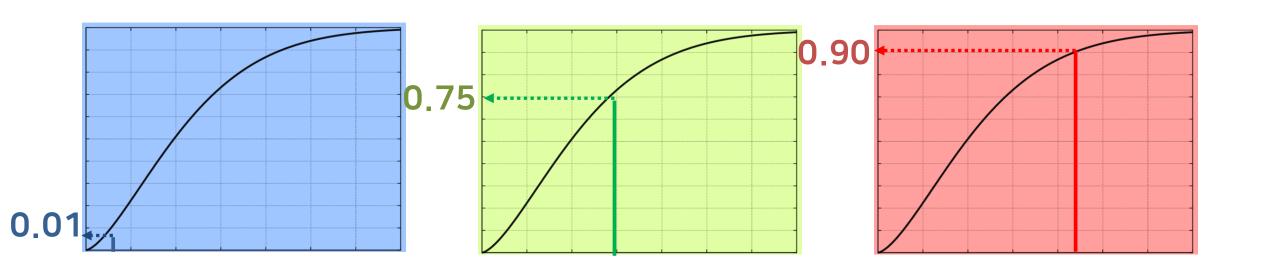


STEP4. 국단분포의 CDF 값(Logit Vector가 해당 클래스가 아닐 확률)을 ω_k 로 두어 Logit Vector 업데이트



<강아지 클래스 평균 Logit Vector>

STEP3. 각각의 극단 분포의 CDF를 통해 각 클래스 평균 Logit Vector와의 거리의 극단 확률 계산



강아지 클래스

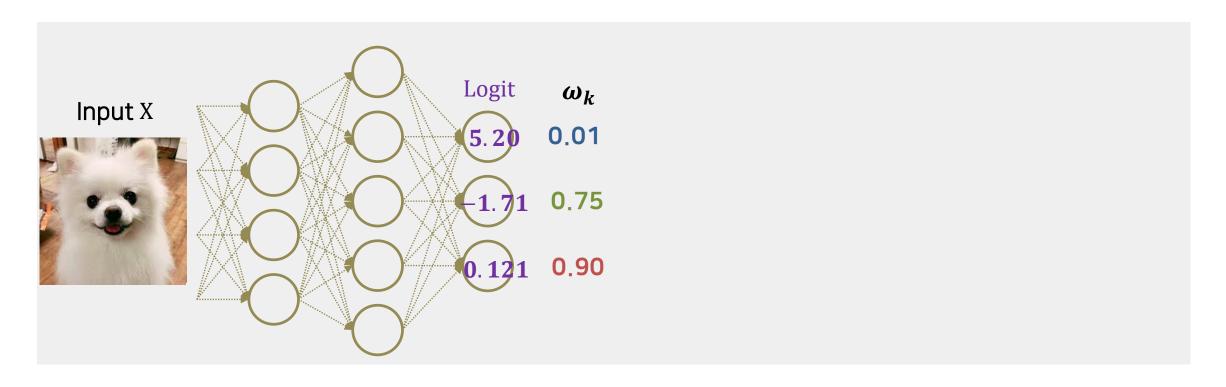
고양이 클래스

토끼 클래스

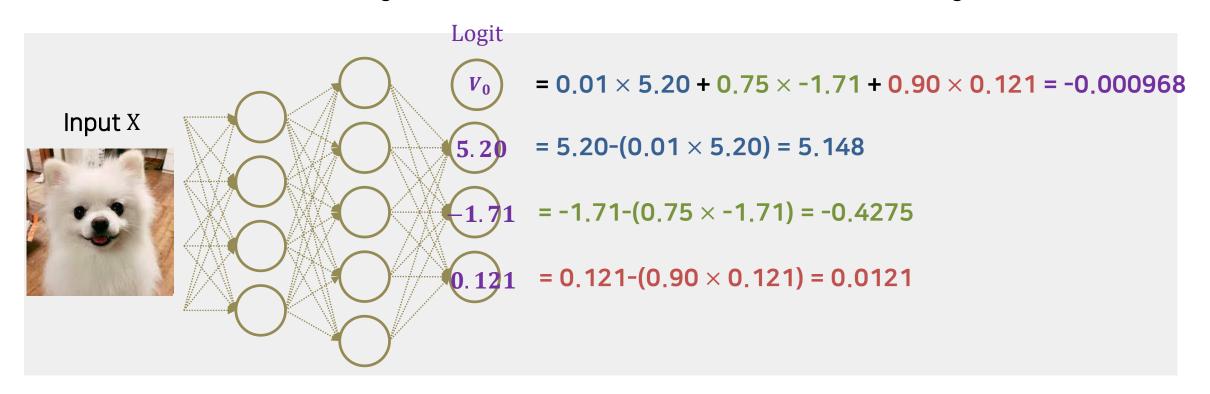
※ 주의. 각 분포는 모두 scale과 shape이 다른 분포



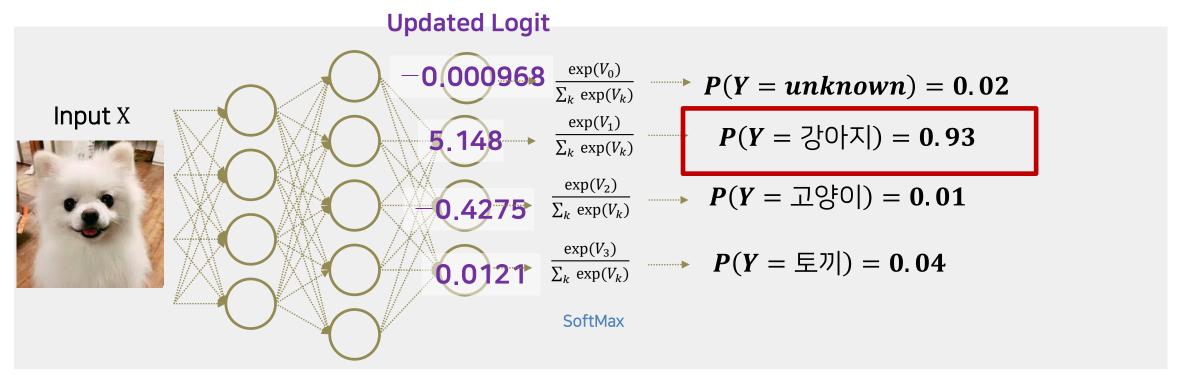
STEP4. **극단분포의** CDF **값**(Logit Vector**가 해당 클래스가 아닐 확률)을 ω**k로 두**어** Logit Vector **업데이트**



STEP4. **극단분포의** CDF **값**(Logit Vector**가 해당 클래스가 아닐 확률)을** ω_k로 두**어** Logit Vector **업데이**트



STEP5. 업데이트 된 Logit Vector를 SoftMax Layer에 통과 시켜 결과 도출





OpenMax: 실험결과

Baseball



Hammerhead



SoftMax

0.94

0.57

OpenMax

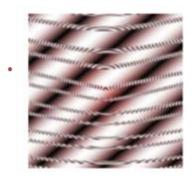
0.94

0.58

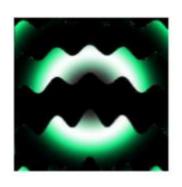
학습 데이터에 포함된 클래스

훈련데이터에 포함된 클래스에 대한 분류 성능은 OpenMax와 SoftMax 간의 큰 차이가 없다

Baseball



Hammerhead



1.0

0.98

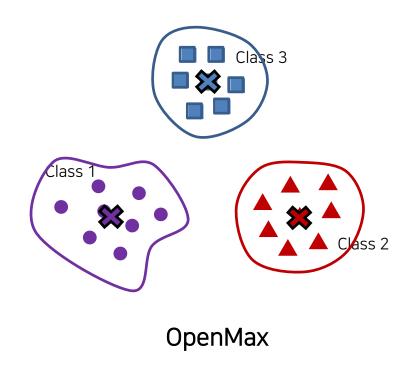
0.00

0.00

Unknown 클래스

훈련데이터에 포함되지 않은 클래스에 대한 분류 성능은 SoftMax의 경우 높은 확신으로 오분류한 데이터에 대해 OpenMax는 우수한 성능으로 거부 한다.

OpenMax : এণ







- 각 클래스 별 평균으로부터의 거리에 대한 극단분포를 이용하여 결정경계 제한
- Unknown Class에 대한 Logit 을 정의하고,
 기존의 Logit Update

Q&A