Deep Learning

Sem 02 - Aula 02

Renato Assunção - DCC - UFMG

Funções de ativação precisam ser não-lineares

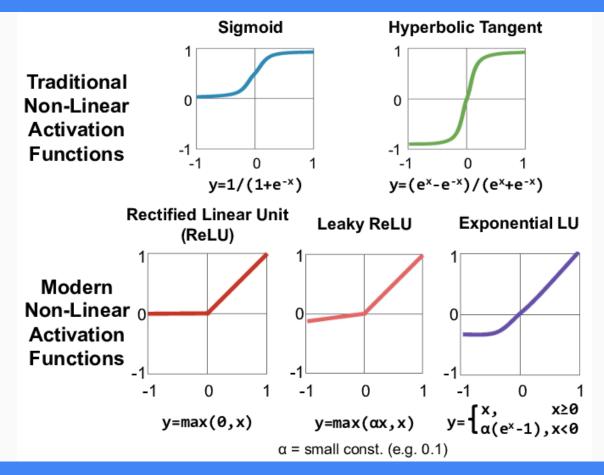
- Em redes neurais, é essencial ter uma função de ativação não-linear
- Função linear de entradas x₁, x₂, x₃, x₄:
 - Qualquer função da forma f(x₁, x₂, x₃, x₄) = w₀ + w₁*x₁ + w₂*x₂ + w₃*x₃ + w₄*x₄
 - ou da forma f(x) = Wx + w₀ onde w₀ e W são matrizes de constantes e x é
 vetor-coluna
- O que acontece se as funções de ativação numa rede neural são lineares?

E se forem lineares?

- Considere uma rede neural com L camadas sucessivas
- Se as funções de ativação em cada camada forem todas lineares:
 - o as L camadas podem ser reduzidas a uma única camada
 - a relação entre os inputs e a saída será uma função linear
 - a rede vai representar bem apenas funções aproximadamente lineares

$$\begin{split} z^{[2]} &= W^{[2]} a^{[1]} & (2.8) \\ &= W^{[2]} g(z^{[1]}) & \text{by definition} & (2.9) \\ &= W^{[2]} z^{[1]} & \text{since } g(z) = z & (2.10) \\ &= W^{[2]} W^{[1]} x & \text{from Equation } (2.4) & (2.11) \\ &= \tilde{W} x & \text{where } \tilde{W} = W^{[2]} W^{[1]} & (2.12) \end{split}$$

Funções de ativação



Vanishing gradients

- Uma descoberta importante recente:
 - sigmóides e tangente hiperbólica não são boas funções de ativação quando temos muitas camadas na rede.
 - Em geral, usamos sigmóide ou tangente hiperbólica na última camada (na saída) quando o problema é de classificação
 - Em outras camadas mais internas costumamos usar outras funções de ativação como a ReLU ou outras mais especializadas para imagens (mais tarde, em redes convolucionais)
- Qual o problema com sigmóides e tangentes hiperbólicas?

Gradientes em funções compostas

- Rede neural é uma grande sequência de composição de funções.
- Alternamos combinações lineares das saídas do passo anterior com uma função de ativação.
- Fazemos isto diversas vezes.
- Na regra da cadeia vai aparecer a DERIVADA da função de ativação várias vezes, como fatores multiplicativos.
- Suponha que todas as funções de ativação sejam sigmóides.
- No backpropagation, teremos derivadas de funções lineares vezes a derivada da logística VÁRIAS VEZES (= número de camadas)

Composição e o produto de derivadas da função logística

Função de custo ou de perda é uma composição de camadas (funções):

$$egin{aligned} \mathcal{L}(w_1,w_2,w_3,w_4,\ldots) &= \sum_{i=1}^m \mathcal{L}^{(i)} \ &= \sum_{i=1}^m \left(\sigma_1 \circ T_1 \circ \sigma_2 \circ T_2 \circ \sigma_3 \circ T_3
ight) \left(x^{(i)},w_1,w_2,w_3,w_4,\ldots
ight) \end{aligned}$$

Derivada parcial com respeito a w₂:

$$egin{aligned} rac{\partial}{\partial w_2} \mathcal{L}(w_1, w_2, w_3, w_4, \ldots) &= \sum_{i=1}^m rac{\partial}{\partial w_2} \mathcal{L}^{(i)} \ &= \sum_{i=1}^m rac{\partial}{\partial w_2} (\sigma_1 \circ T_1 \circ \sigma_2 \circ T_2 \circ \sigma_3 \circ T_3) \left(x^{(i)}, w_1, w_2, w_3, w_4, \ldots
ight) \ &= \sum_{i=1}^m \sigma_1' imes \partial T_1 imes \sigma_2' imes \partial T_2 imes \sigma_3' imes \partial T_3 \end{aligned}$$

Composição e o produto de derivadas da função logística

Função de custo ou de perda é uma composição de camadas (funções):

$$egin{aligned} \mathcal{L}(w_1, w_2, w_3, w_4, \ldots) &= \sum_{i=1}^m \mathcal{L}^{(i)} \ &= \sum_{i=1}^m \left(\sigma_1 \circ T_1 \circ \sigma_2 \circ T_2 \circ \sigma_3 \circ T_3
ight) (x^{(i)}, w_1, w_2, w_3, w_4, \ldots) \end{aligned}$$

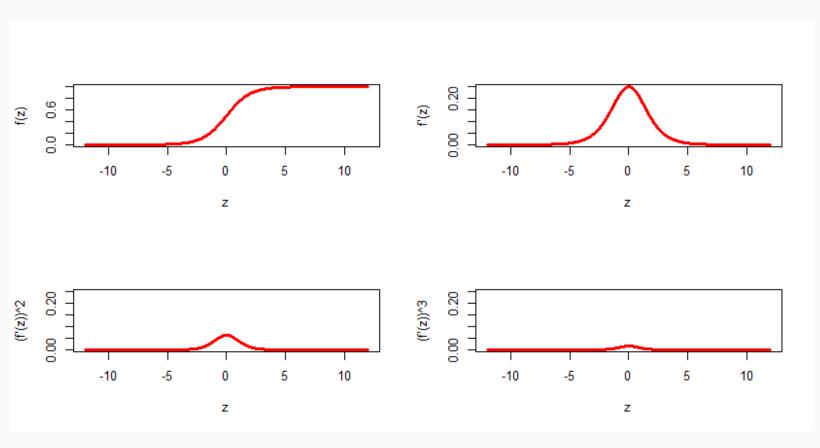
Derivada parcial com respeito a w₂:

$$\frac{\partial}{\partial w_2}\mathcal{L}(w_1,w_2,w_3,w_4,\ldots) = \sum_{i=1}^m \frac{\partial}{\partial w_2}\mathcal{L}^{(i)}$$
 sigmóide avaliadas em diferentes pontos
$$= \sum_{i=1}^m \frac{\partial}{\partial w_2} (\sigma_1 \circ T_1 \circ \sigma_2 \circ T_2 \circ \sigma_3 \circ T_3) \left(x^{(i)},w_1,w_2,w_3,w_4,\ldots\right)$$

$$= \sum_{i=1}^m \sigma_1' \times \partial T_1 \times \sigma_2' \times \partial T_2 \times \sigma_3' \times \partial T_3$$

produto de derivadas da

Sigmóide: vanishing gradients



Produto das derivadas da sigmóide <u>no</u> <u>mesmo ponto</u>

Melhor caso:
ponto 0, o
máximo:
dissolve
rapidamente
(vanishes
quickly)

E a ReLU?

- Função f(x) = max{0, x}
- Derivada f'(x) = 0 ou 1 dependendo de x < 0 ou x > 0
- Derivadas no backprop:
 - além dos termos de derivadas de funções lineares,
 teremos produtos de derivadas de ReLU.



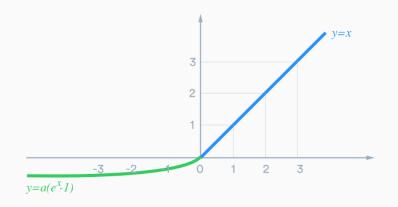
- Elas podem zerar a derivada parcial se uma delas for zero
- Mas o produto das derivadas não necessariamente → 0, como nas sigmóides
- Leaky ReLU: criada para evitar a derivada ZERO da ReLU ("dying ReLU")
- Parametrized ReLU: PReLU
 - o introduz um parâmetro a

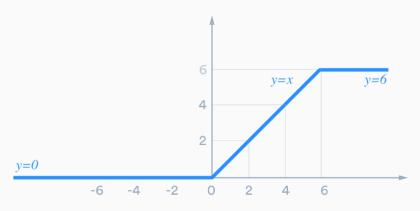
Renato Assunção - DCC - UFMG

Alternativas a ReLU

Exponential ReLU: ELU

ReLU-6



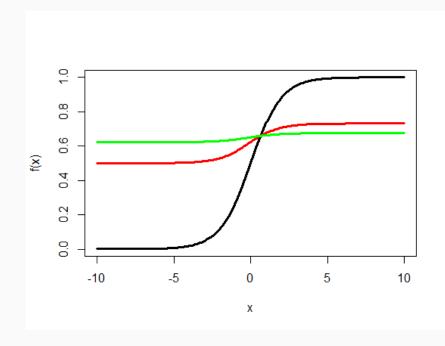


ReLU é idempotente

- Uma coisa importante a salientar é que ReLU é uma função idempotente.
- Def: Uma função f(x) é chamada de idempotente se f(f(x)) = f(x)
- Exemplo:
 - \circ f(x) = x
 - \circ f(x) = |x|
 - \circ f(x) = max(0, x) = ReLU
- Veja que $f(f(x)) = f^2(x) = (f \circ f)(x)$
- Funções que não são idempotentes:
 - o $f(x) = x^2$ ou $f(x) = 1/(1+e^{-x}) = logística$

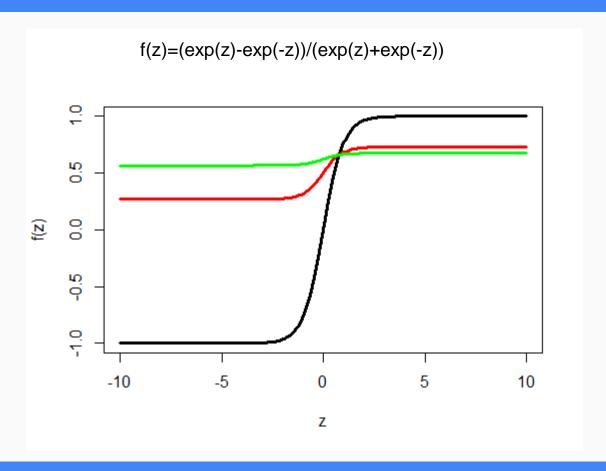
Outra maneira de ver o vanishing gradient

- Se f é idempotente então f∘f∘f∘ ··· ∘f = f
- Essa propriedade é importante para redes neurais profundas, porque cada camada na rede aplica uma nãolinearidade.
- Agora, vamos aplicar duas funções da família sigmóide à mesma entrada repetidamente 1, 2, 3 vezes

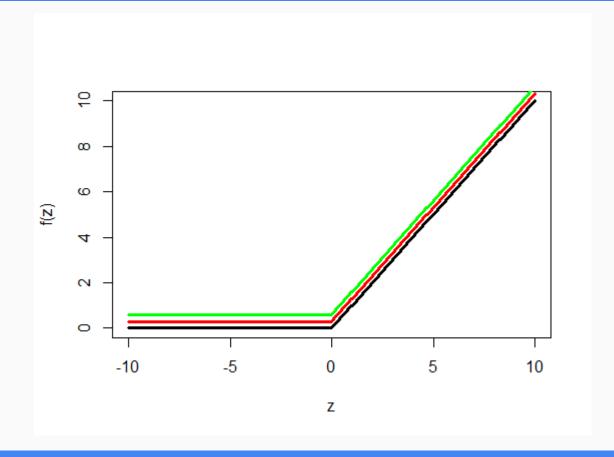


 A função sigmóide composta "esmaga" sua entrada, resultando no problema do vanishing gradient: as derivadas vão para zero com no. de composições

Tangente hiperbólica composta 3 vezes



ReLU composta 3 vezes (jittered para visualizar)



ReLU e variantes estão nos principais frameworks

```
import tensorflow as tf

conv_layer = tf.layers.conv2d(
   inputs=input_layer,
   filters=32,
   kernel_size=[5, 5],
   padding='same',
   activation=tf.nn.relu,
)
```

```
from keras.layers import Activation, Dense
model.add(Dense(64, activation='relu'))
```

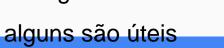
```
from torch.nn import RNN

model = nn.Sequential(
    nn.Conv2d(1, 20, 5),
    nn.ReLU(),
    nn.Conv2d(20, 64, 5),
    nn.ReLU()
)
```

Entendendo a necessidade de regularização

- Aprendemos os parâmetros W's e b's minimizando a função de perda
- Como a função de perda = -logverossimilhança, estamos maximizando log-verossimilhança
- Fisher mostrou que o MLE é o melhor estimador possível de um parâmetro.
- Então... nada mais a fazer, certo?
- George Box: todos os modelos são falsos;





MLE em modelos verdadeiros

- O modelo é verdadeiro: dados observados foram, de fato, gerados de acordo com o modelo probabilístico sob análise.
- ullet Existe um verdadeiro valor do parâmetro heta que gera os dados observados
- Quando a amostra não é pequena, o MLE é:
 - \circ converge para heta quando a amostra cresce
 - aprox não-viciado para estimar
 - um estimador não viciado possui variância >= Informação de Fisher^{-1}
 - o erro de estimação do MLE tem variância → inverso da informação de Fisher
 - MLE aprox gaussiano

Exemplo muito simples

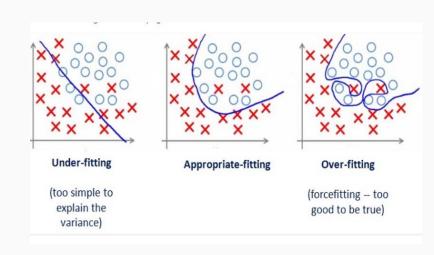
- Caso gaussiano i.i.d. $Y_1, Y_2, \ldots, Y_n \sim N(\mu, \sigma^2)$
- Como estimar $\mu_?$ Média aritmética? Mediana? Média dos extremos? Combinação desses estimadores?
- Suponha que $\hat{\mu}_{}$ seja <u>qualq</u>uer estimador de $\mu_{}$
- Um estimador é não-viciado se ele não subestima ou superestima sistematicamente:
- ado $MSE(\hat{\mu})=\mathbb{E}\left[(\hat{\mu}-\mu)^2
 ight]$ os, $MSE(\hat{\mu})\geq \sigma^2/n$, menor valor possível MSE = Erro de estimação ao quadrado
- Para estimadores aprox não-viciados,
- O MLE tem seu MSE $_{f i}$ gual a $^{\sigma^2/n}$ inverso da informação de Fisher
- Nada pode ser melhor

MLE em modelos falsos

- ullet Em princípio, podemos ter uma estimador viciado para μ com variância menor que σ^2/n
- E quando o modelo verdadeiro n\u00e3o for normal?
- Usamos o MLE no modelo falso.
 - O MLE converge? Para onde?
 - Tem variância mínima?
 - O MLE converge para o modelo "falso" mais próximo (sentido de distância de Kullback-Leibler) do modelo verdadeiro desconhecido
 - White (1982). Econometrica,

OK, e daí? Especificação incorreta em redes neurais

- Sem esperanças de especificar um "modelo verdadeiro" em redes neurais
- Em que direção erramos na especificação?
- Costumamos colocar muita redundância de features ou parâmetros.
- Em DL, #parâmetros cresce com #dados
- Risco de overfitting na fase de treinamento (controlado pelo erro no conjunto de teste).



de aulas de Andrew Ng, coursera

Overfitting em regressão linear

Regressão linear simples → para entender bem o núcleo do problema

- vetor Y com as respostas (tamanho = 1500 exemplos)
- Imagine predizendo resposta Y com base em n+1 features

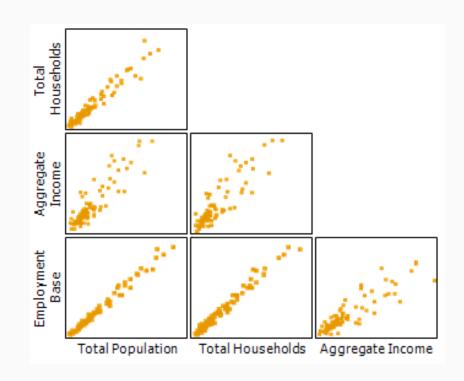
- Preditor é uma combinação linear dos n vetores 1, x₁, x₂, ..., x_n
- n +1 colunas de tamanho 1500 cada uma delas.
- Preditor é uma combinação linear desses vetores.
- Imagine que a predição é muito boa, pouco erro de predição.

Muitas features → redundância

Colocamos muitas features no modelo

- Várias medem coisas similares
- → altamente correlacionadas entre si

- Veja exemplo ao lado
- Dados de setores censitários



Outro exemplo simples

All Greens Franchise

The data (X1, X2, X3, X4, X5, X6) are for each franchise store.

X1 = annual net sales/\$1000

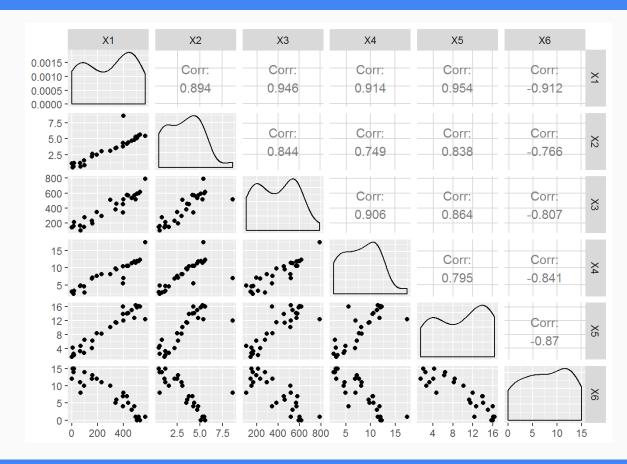
X2 = number sq. ft./1000

X3 = inventory/\$1000

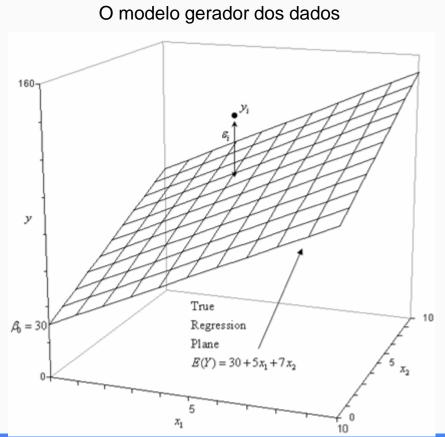
X4 = amount spent on advertising/\$1000

X5 = size of sales district/1000 families

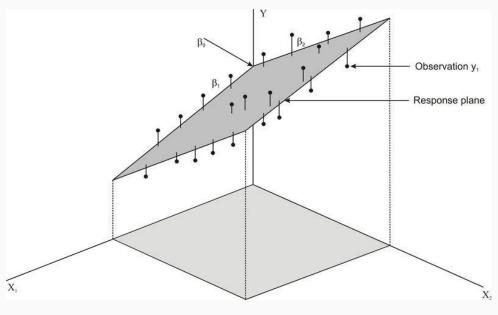
X6 = number of competing stores in district



A regressão múltipla mais simples: duas features



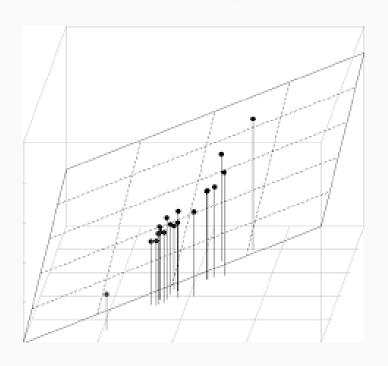
O modelo e os dados gerados

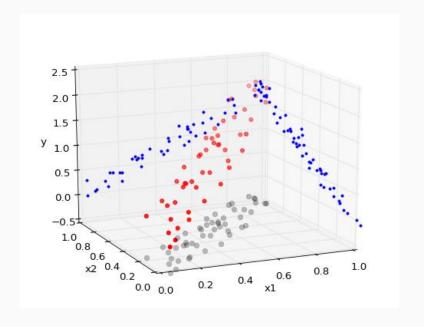


Renato Assunção - DCC - UFMG

Duas features quase colineares

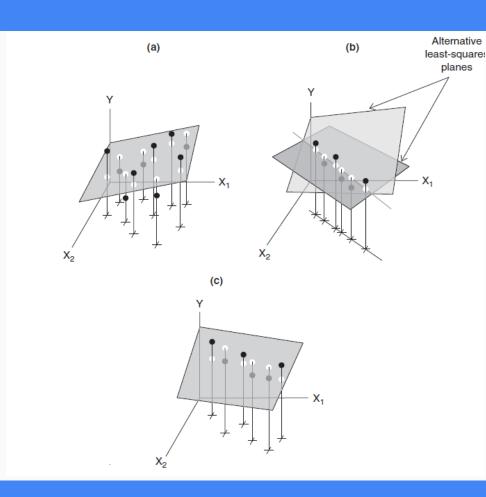
https://www.youtube.com/watch?v=gAIVp3mt8Bw





Instabilidade dos coeficientes

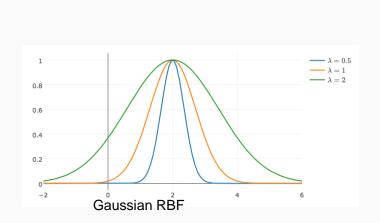
- Predição: OK, quase não muda
- Coeficientes da regressão:
 - altamente instáveis
 - Quer dizer: alta variância
 - Pequena mudança nos dados, e teremos coeficientes
 completamente diferentes (mas quase as mesmas predições)
- Modelo pode omitir certas features sem prejuízo da predição

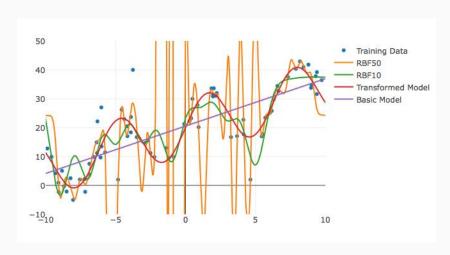


Outra maneira (mais usual) de ver a necessidade de regularização

- Generic Features: increase model expressivity
 - Gaussian Radial Basis Functions:

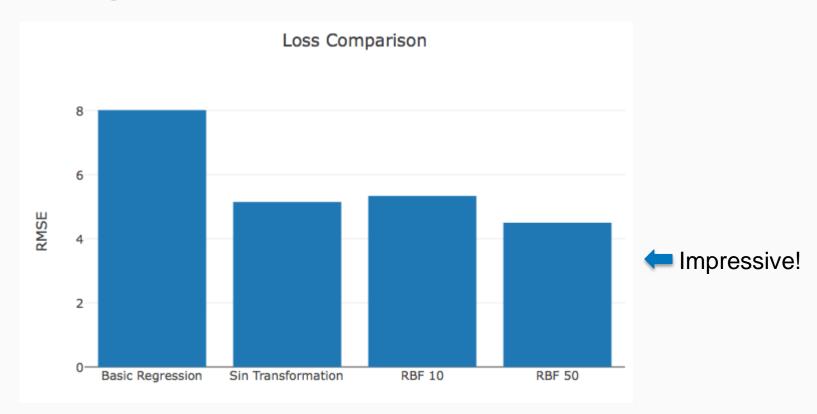
$$\phi_{\lambda_i,\mu_i}(x) = \exp\left(-\frac{||x - \mu_i||_2^2}{\lambda_i}\right)$$



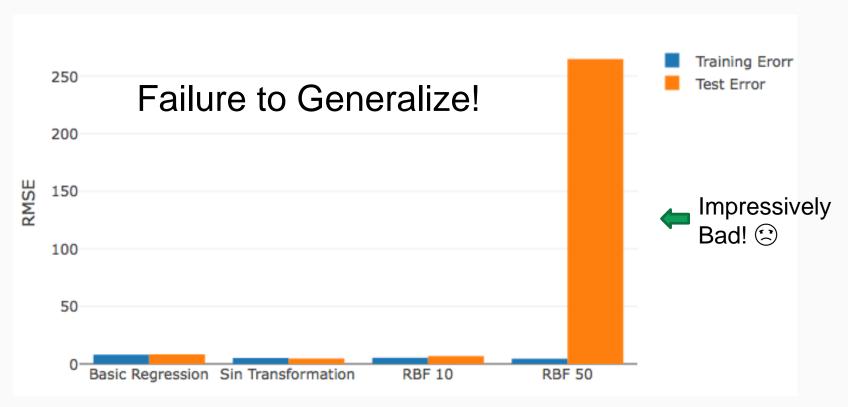


Este e os próximos 7 slides vieram de aula preparada por Joseph E. Gonzalez jegonzal@cs.berkeley.edu Fernando Perez fernando.perez@berkeley.edu

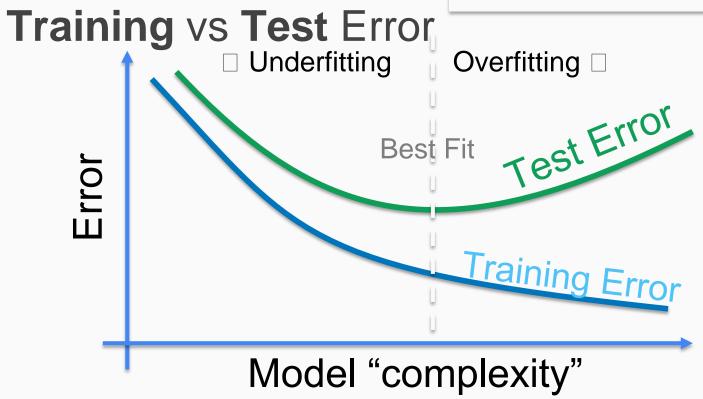
Training Error



Training vs Test Error



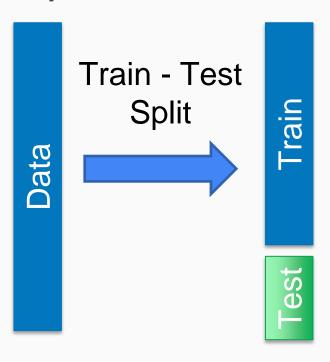
Training error typically *under estimates* **test error**.



(e.g., number of features)

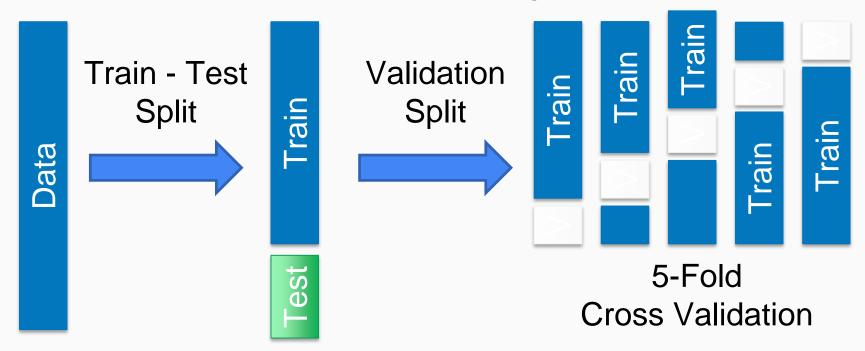
Generalization: The Train-Test Split

- Training Data: used to fit model
- Test Data: check generalization error
- How to split?
 - o Randomly, Temporally, Geo...
 - Depends on application (usually randomly)
- What size? (90%-10%)
 - Larger training set □ more complex models
 - Larger test set □ better estimate of generalization error
 - Typically between 75%-25% and 90%-10%



You can only use the test dataset once after deciding on the model

Generalization: Validation Split



Cross validation simulates multiple train test-splits on the training data.

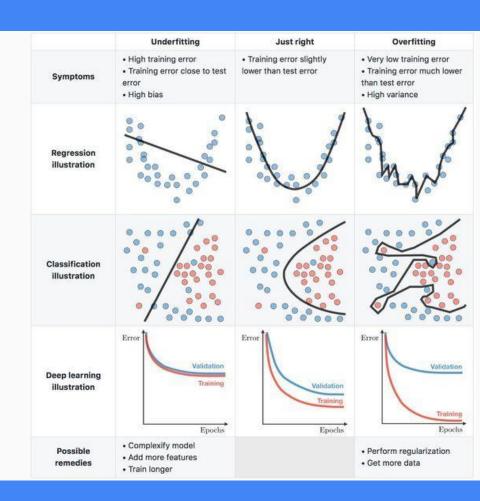
Recipe for Successful Generalization

- 1. Split your data into training and test sets (90%, 10%)
- 2. Use only the training data when designing, training, and tuning the model
 - > Use **cross validation** to test *generalization* during this phase
 - Do not look at the test data
- 3. Commit to your final model and train once more using **only the training** data.
- 4. Test the final model using the **test data**. If accuracy is not acceptable return to (2). (*Get more test data if possible*.)
- 5. Train on all available data and ship it!



Bias/variância

- Ideia de bias/variância são fáceis de entender, mas difíceis de dominar.
 - Se o seu modelo underfit
 (regressão logística com dados não lineares) ele tem um "alto viés"
 - Se o seu modelo overfit, então ele tem uma "alta variância"
 - Seu modelo ficará bem se você equilibrar o bias/variância



Bias/variance trade-off

- Se o seu algoritmo tem bias alto:
 - Tente uma RN maior (> hidden layers, > no de unidades)
 - o Tente um modelo diferente que seja mais adequado para seus dados.
 - Tente rodar por mais tempo.
 - Tente algoritmos de otimização diferentes.
- Se seu algoritmo tiver uma high variance:
 - Obtenha mais dados.
 - Tente regularização.
 - Tente um modelo diferente que seja mais adequado para seus dados.

Problema é mais abstrato em redes neurais

- Em regressão linear, conseguimos visualizar o problema
- Em redes neurais, não é possível ver as coisas de maneira tão simples
- Mas a mesma coisa ocorre: alta variação dos coeficientes
- Solução é chamada de regularização
- Abordagens para regularização:
 - penalização L2
 - penalização L1
 - drop-out
 - data augmentation
 - early stopping

Regularização via penalização

- Evitar a aparição de coeficientes com coeficientes extremamente altos ou extremamente baixos.
- Estes coeficientes são um sinal de redundância das features ou complexidade de explicação/predição

- ullet Considere o vetor $heta = (W^{[1]}, W^{[2]}, \dots, W^{[L]})$
- Tornamos as matrizes de pesos num longo vetor
- Observe que ele não possui os termos b's de bias

Normas para Regularização

- ullet Seja $heta=(heta_1, heta_2,\dots, heta_M)=(W^{[1]},W^{[2]},\dots,W^{[L]})$
- ullet Ao invés de controlar cada coeficiente $heta_i$ separadamente, usamos uma medida global dos seus "tamanhos"
- Duas normas:

$$_{\circ}$$
 Norma $\mathbb{L}_{2}=|| heta||_{2}^{2}= heta^{T}\cdot heta=\sum_{i} heta_{i}^{2}$

$$_{\circ}$$
 Norma $\mathbb{L}_{1}=|| heta||_{1}=\sum_{||} heta_{i}||_{1}$

 O objetivo da regularização é que a norma do vetor de pesos estimado não seja grande demais

Regularização via penalização

• A função de custo/perda que queremos minimizar é $J(\theta,b^{[1]},b^{[2]},\dots,b^{[L]}) = \sum_i \mathcal{L}(y^{(i)},\hat{y}^{(i)})$ $= \sum_i (y^{(i)} - \hat{y}^{(i)})^2 \quad \text{regressao}$ $= \sum_i \left(y^{(i)}\log(\hat{y}^{(i)}) + (1-y^{(i)})\log(1-\hat{y}^{(i)})\right) \quad \text{2-classificacao}$ $= \sum_i \sum_i \left(I[y^{(i)} = k]\log(\hat{y}^{(i)}_k)\right) \quad \text{K-classificacao}$

- A função regularizada é
- ullet Caso L1: $J(heta, b^{[1]}, b^{[2]}, \ldots, b^{[L]}) + \lambda || heta||_1$

Regularização LASSO (Least Absolute shrinkage and selection operator)

$$ullet$$
 Caso L2: $J(heta,b^{[1]},b^{[2]},\ldots,b^{[L]})+\lambda|| heta||_2^2$ Regularização RIDGE

Parâmetro lambda

- Ao invés de minimizar a -log-verossimilhança, nós minimizamos a -logverosimilhança mais um termo de penalização
- Penalizamos vetores de pesos "grandes demais"
- O parâmetro lambda controle a importância do termo de penalização
- É chamado de (um dos) hiper-parâmetro do modelo
- Papel de lambda: Na prática, ele penaliza grandes pesos e limita efetivamente a liberdade de escolher pesos em nossos modelos.

$$J(heta, b^{[1]}, b^{[2]}, \dots, b^{[L]}) + \lambda || heta||_2^2$$

Parâmetro lambda

$$J(heta, b^{[1]}, b^{[2]}, \dots, b^{[L]}) + \lambda || heta||_2^2$$

- Se $\lambda=0$, temos a situação anterior, sem penalização, talvez levando a overfitting, com pesos grandes demais
- ullet Se $^{\lambda}>>0$, teremos uma penalização excessiva.
- O segundo termo vai dominar a soma: na prática, vamos minimizar apenas o tamanho do vetor de pesos levando a um vetor muito próximo de zero.
- Acabaremos induzindo um alto bias no nossos modelos ao forçar a maioria dos pesos a ser muito próxima de zero
- Se lambda for OK, ele reduzirá apenas alguns pesos que levam a overfit da

Backpropagation com penalização

- Backpropagation não muda muito
- Por exemplo, com L2

$$egin{aligned} heta_j^{t+1} &= heta_j^t - lpha \left \lfloor rac{\partial J}{\partial heta_j} \mid_{ heta_j^t} + 2\lambda heta_j^t
ight
floor \end{aligned}$$

Com L1:

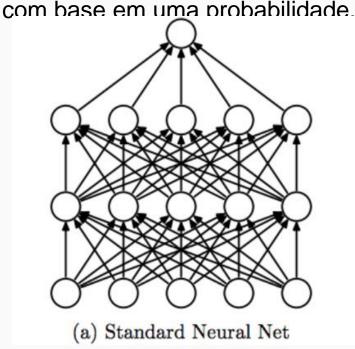
$$heta_j^{t+1} = heta_j^t - lpha \left[rac{\partial J}{\partial heta_i} + \lambda \left(I[heta_j^t > 0] - I[heta_j^t < 0]
ight)
ight]$$

Como escolher λ

- Escala logarítmica:
- Escolha 12 valores para λ □ 0, 0.01, 0.02, 0.04, 0.08, 0.16, 0.32, 0.64, 1.28,
 2.56, 5.12, 10
- Rode o conjunto de treinamento para cada lambda
- Calcule a função de custo com o conjunto de validação para checar a qualidade do resultado
- Escolha o valor de lambda que seja o melhor.

Regularização via dropout

A regularização via dropout elimina alguns neurônios/pesos em cada iteração



(b) After applying dropout.

Extraído de

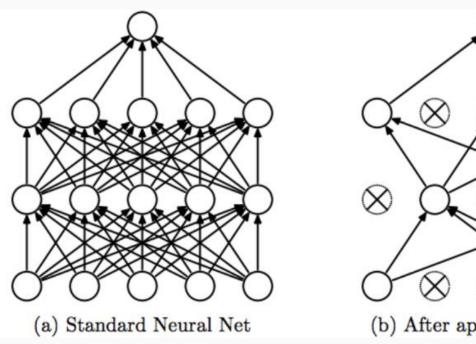
Srivastava, Hinton, Krizhevsky, Sutskever, Salakhutdinov.

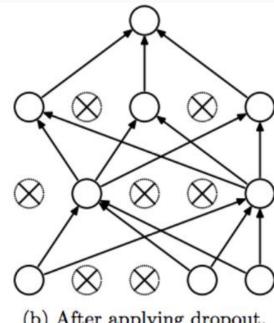
Dropout: a simple way to prevent neural networks from overfitting.

JMLR 2014

Dropout aleatoriamente em cada ciclo de iterações

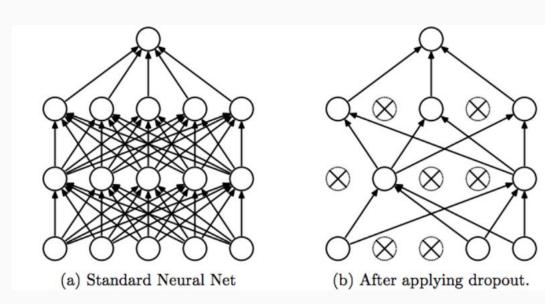
Ao descartar um neurônio, removemos a unidade temporariamente da rede, juntamente com todas as suas conexões de entrada e de saída.





Qual a probabilidade usada para descartar unidades?

- Do paper/patente: use
 probabilidade p= ½ para reter um
 neurônio interno (escondido) de
 camadas com muitas unidades.
- Use p aprox 1 para reter neurônios das camadas finais com muito poucos neurônios
- Use probab p=0.8 para reter features da camada visível. (Ng recomenda p=1.0)



Como implementar? Dropout invertido

- Fase de Treinamento:
 - Para cada camada oculta, para cada amostra de treinamento, para cada iteração, ignore (zero out) uma fração aleatória, p, de nós (e as ativações correspondentes).
 - Use "Dropout invertido" para compensar: multiplique os valores das ativações que sobram pelo fator de dropout inverso 1/p.
- Suponha p=0.8 e uma camada com 50 unidades → em média restarão 40
- Ao passar para a próxima camada, o valor z vai usar apenas 40
 neurônios/ativados → multiplique-os por 1/0.8 = 1.25 para manter o valor de z da
 próxima camada igual (em valor esperado) ao valor SEM dropout.

Como implementar? Dropout invertido

- Fase de teste:
 - Use todos os neurônios, não delete nenhum.
 - E os pesos a serem usados?
 - Use o valor mais recente obtido para cada peso quando ele n\u00e3o esteve deletado.
 - Não precisa compensar pela probabilidade p.
 - Isto foi feito na fase de treinamento.
- Paper original era um pouco mais complicado.

Slide de Andrew Ng

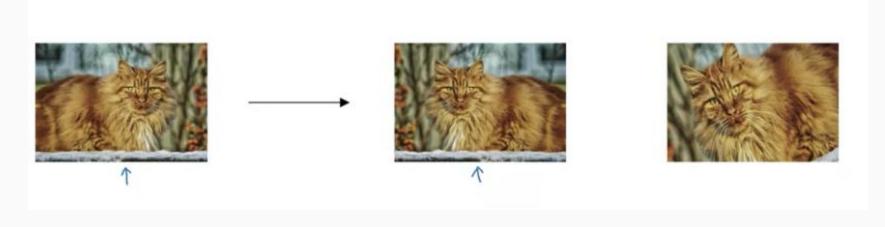
Implementing dropout ("Inverted dropout") Illustre with log R=3. beep-pub= 0.8 -> 83 = np rodon rod (a3 styre To), a3 styre To) < keep-prob = 10 multiply lad, d3) # a3 x = d3. = a3 /= 08 temp-pab = 50 units as 10 units shut off 2 th = 600 a (e) + 600 Test 1= 08

Andrew Ng

Regularização via dropout

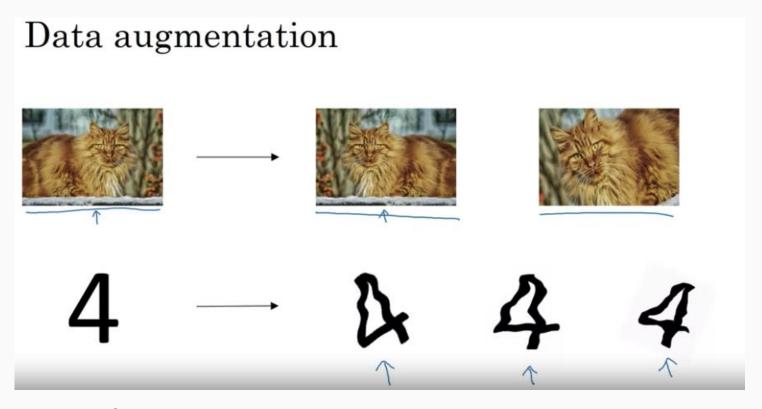
- O dropout força uma rede neural a aprender quais são os neurônios mais robustos.
- São aqueles neurônios que são importantes em muitos subconjuntos aleatórios diferentes de outros neurônios.
- O dropout praticamente dobra o número de iterações necessárias para convergir.
- No entanto, o tempo de treinamento para cada exemplo é menor pois a rede é mais simples.

Data augmentation



Slide de Andrew Ng

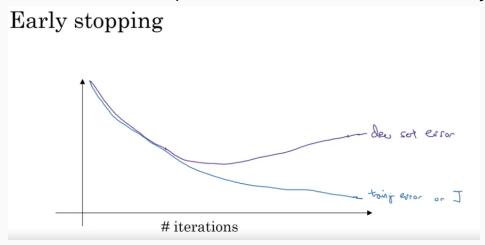
Outras maneiras de regularizar



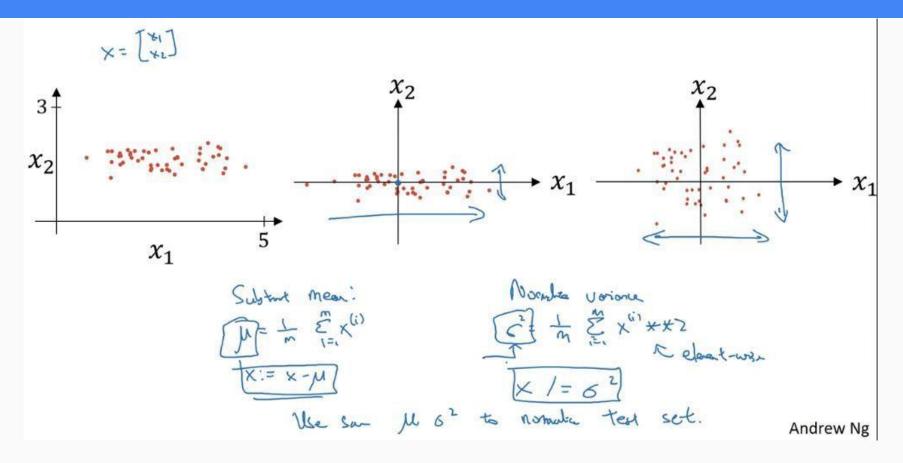
Slide de Andrew Ng

Outras maneiras de regularizar: early stopping

- Divida os dados de treinamento em um conjunto de treinamento e um conjunto de validação.
- Treinar apenas no conjunto de treinamento.
- Avaliar o erro no conjunto de validação de vez em quando (a cada 5 iterações, por exemplo)
- Pare o treinamento assim que o erro no conjunto de validação subir.
- Use os pesos que a rede tinha na etapa anterior como resultado da execução do treinamento.



Normalizando as entradas



Normalizar as entradas

