IA048 - Aprendizado de Máquina: Prova 28/05/2024

Tiago Corrêa de Araújo de Amorim (RA: 100675)

1. Questão 1

As redes neurais generativas adversárias (GANs, generative adversarial networks) trouxeram uma abordagem inovadora para a área de aprendizado de máquina.

(a) (0,8) Explique por que as redes geradora e discriminadora são consideradas adversárias.
(b) (0,8) Tendo em vista os papeis desempenhados por cada rede, discorra sobre a função custo proposta por Goodfellow et al. (2014)[1] para o treinamento da GAN. Complementando essa análise, comente também sobre como a rede geradora consegue aprender as características típicas dos dados reais.

*1.1. Resposta **(a)***

As redes geradora e discriminadora são consideradas adversárias porque o treinamento dos seus pesos usam objetivos conflitantes. A função objetivo da rede discriminadora é maximizar o número de vezes em que classifica os dados reais como verdadeiros e os dados gerados pela rede geradora como falsos. Já a rede geradora tem como função objetivo maximizar o número de vezes em que a rede discriminadora classifica a saída da rede geradora como verdadeiros.

*1.2. Resposta **(b)***

A função custo proposta por Goodfellow segue o que foi discutido no item anterior. Os pesos da rede discriminadora são ajustados para maximizar a média do log das saídas da rede discriminadora[2]. Os pesos da rede geradora são ajustados para minimizar a média do log das saídas da rede discriminadora[3]. Como os objetidos são conflitantes, os autores propõe ajustar os pesos de cada rede de forma intercalada, ou seja, não são ajustados simultaneamente. Ademais, também comentam que existe um balanço delicado entre treinar *demais* a rede discriminadora a ponto de deixar a tarefa da rede geradora *muito difícil*.

Na proposta original a rede geradora recebe como entrada um vetor aleatório. O que se busca é que a rede geradora consiga mapear este vetor aleatório no espaço de distribuição dos dados reais. Uma rede geradora competente consegue aproximar o espaço de distribuição dos dados reais de forma a se tornar indistinguível do espaço real. Ao conseguir se tornar uma rede competente, a rede geradora estará efetivamente utilizando o vetor de entrada como uma *representação* das principais características dos dados reais.

2. Questão 2

(1,2) Explique os conceitos de mapa de características (feature map), neurônio, campo receptivo e compartilhamento de pesos no contexto de uma camada convolucional de uma CNN (convolutional neural network).

[1] Goodfellow, I. J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., Bengio, Y., Generative Adversarial Networks, Proceedings of the 27th International Conference on Neural Information Processing Systems (NIPS), pp.2672-2680, 2014.

[2] A saída da discriminadora deve ter valores altos para dados reais e baixos para dados gerados.

[3] Ou seja, busca *enganar* a rede discriminadora para que gere valores altos para os dados gerados.

2.1. Resposta

- **Mapa de características**:
- **Neurônio**:
- **Campo receptivo**:
- **Compartilhamento de pesos**:

3. Questão 3

Tendo em mente a teoria subjacente às máquinas de vetores-suporte (SVMs, do inglês support-vector machines):

(a) (0,5) Defina margem de classificação no contexto de um problema linearmente separável e explique por que a maximização da margem é, intuitivamente, uma abordagem segura de projeto.
(b) (0,5) Por que a formulação matemática relacionada à obtenção do classificador de máxima margem possui similaridades com as ideias de regularização (e.g. Tikhonov / ridge regression) vistas no curso?

*3.1. Resposta **(a)***

*3.2. Resposta **(b)***

4. Questão 4

(1,2) Numa importante conferência da área de inteligência computacional, foi lançada uma competição no âmbito de um problema de classificação de imagens. Duas jovens pesquisadoras decidiram, então, empregar uma CNN já consolidada na literatura (e.g. uma ResNet) para resolver a tarefa. Partindo de uma inicialização aleatória para os pesos da rede escolhida, e utilizando apenas os dados disponíveis na competição, elas, ao final do treinamento, observaram um nível de acurácia bastante adequado. No entanto, quando exposta a novos padrões de entrada (conjunto de teste), esta rede não atingiu um bom desempenho, tendo ficado muito abaixo das expectativas iniciais de projeto. Recomende (com argumentos bem fundamentados) duas estratégias para amenizar este problema.

4.1. Resposta

Uma possibilidade é que a base de dados utilizada pelas pesquisadoras não tem tramanho adequado para o treinamento de uma rede muito profunda. Redes como a ResNet são muito profundas, com um número significativo de pesos a serem ajustados. Estas redes funcionam bem porque foram ajustadas com um número **muito** grande de dados. Uma forma de buscar contornar o problema do limitado número de dados é utilizar *data augmentation*, gerandos amostras adicionais a partir dos próprio dados (rotação, translação, ...). É uma estratégia um pouco limitada, pois depende muito da quantidade de dados disponível, que pode ainda ser insuficiente. Uma estratégia mais interessante é fazer *transfer learning*, ou seja, utilizar os pesos da rede já treinados e adaptar a estrutura da rede para o problema específico. Em diferentes publicações foi explorada a estrutura destas redes *famosas*, verificando que as camadas vão se especializando em elementos cada vez mais complexo à medida que a informação segue pela rede. As primeiras camadas se especializam em formas simples (semi-círculo, linha vertical, ...), e camadas profundas em elementos mais complexos (olho, boca, ...). Boa parte destas atividades podem ser úteis para outros problemas de classificação. Assim é possível utilizar boa parte das primeiras camadas da rede existente, incluir algumas novas camadas e fazer o treinamento dos pesos apenas das novas camadas que foram adicionadas ao final.

5. Questão 5

(1,4) Considere o problema de identificação de tumores cerebrais a partir de um conjunto de 1500 imagens de ressonância magnética (MRI) do crânio, de dimensão 200 Œ 200, em tons de cinza (veja um exemplo na Figura 1). As possíveis classes do problema são: (0) glioma; (1) meningioma; (2) pituitário; (3) saudável (normal). Descreva detalhadamente como uma rede MLP (multilayer perceptron), com uma única camada intermediária, poderia ser aplicada a este problema, indicando aspectos referentes à arquitetura da rede, bem como à metodologia como um todo (e.g. tratamento dos dados, treinamento do modelo etc.).

5.1. Resposta

6. Questão 6

Ao realizar um processo de PCA sobre uma base de dados, um pesquisador obteve os seguintes autovalores para a matriz de autocorrelação:

$$\lambda = \begin{bmatrix} 0,2 \\ 2,3 \\ 1,5 \\ 3 \\ 0,05 \\ 0,15 \\ 0,5 \\ 0,3 \end{bmatrix} \tag{6.1}$$

(a) (0,3) Qual é a dimensão do espaço original dos dados?
(b) (0,7) Caso se busque uma preservação de ao menos 90% do conteúdo energético dos dados, qual é o menor número possível de componentes principais empregadas? Justifique.

*6.1. Resposta **(a)***
*6.2. Resposta **(b)***

7. Questão 7

Considere que uma CNN tenha sido aplicada à classificação de imagens de retina em três classes: normal, glaucoma e catarata. Na etapa de teste, a seguinte matriz de confusão foi obtida:

	Classe estimada		
Classe real	**Normal**	**Glaucoma**	**Catarata**
Normal	410	15	25
Glaucoma	10	100	40
Catarata	55	25	100

(a) (0,4) Considerando a classe **Glaucoma** como positiva, obtenha as quantidades de verdadeiros positivos (TP), falsos positivos (FP), verdadeiros negativos (TN) e falsos negativos (FN).
(b) (0,6) Determine o valor da acurácia balanceada atingida pela CNN, mostrando explicitamente os valores das métricas intermediárias necessárias para o cálculo.

*7.1. Resposta **(a)***
*7.2. Resposta **(b)***

8. Questão 8

(a) (1,0) Explique como funciona o mecanismo de auto-atenção de um transformer.
(b) (0,6) De que maneira um transformer consegue aproveitar possíveis interdependências de curto e longo prazo em uma sequência de entrada apesar de não ter recorrência?