به نام خدا

دانشکده مهندسی کامپیوتر

امنیت و حریم خصوصی در یادگیری ماشین
(۴۰۸۱۶)(نیم‌سال دوم سال تحصیلی ۱۴۰۱-۱۴۰۲)
استاد درس: دکتر امیرمهدی صادق‌زاده
دستیاران آموزشی: مهدی غزنوی، زینب گلگونی، الهه فرشادفر، محمدرضا کاظمی، حمید دشتبانی

تمرین دوم

مهلت تحویل: ساعت ۲۳:۵۹ یک‌شنبه ۱۸ فروردین ۱۴۰۲

نکات و قواعد

۱. سوالات خود را زیر پیام مربوطه در Quera مطرح نمایید.

۲. محل بارگذاری تمرین تا یک هفته پس از مهلت ارسال باز خواهد بود. در طول ترم، در مجموع می‌توانید از ۲۱ روز تاخیر مجاز به صورت ساعتی استفاده کنید و پس از آن به ازای هر روز ۲۰ درصد جریمه بر روی نمره‌ی کسب شده اعمال خواهد شد.

۳. لطفا مطابق تاکید پیشین، حتما آداب‌نامه‌ی انجام تمرین‌های درسی را رعایت نمایید. در صورت تخطی از آیین‌نامه، در بهترین حالت مجبور به حذف درس خواهید شد.

۴. در صورتی که پاسخ‌های سوالات نظری را به صورت دست‌نویس آماده کرده‌اید، لطفا تصاویر واضحی از پاسخ‌های خود ارسال کنید. در صورت ناخوانا بودن پاسخ ارسالی، نمره‌ای به پاسخ ارسال شده تعلق نمی‌گیرد.

۵. همه‌ی فایل‌های مربوط به پاسخ خود را در یک فایل فشرده و با نام **SPML_HW۲_StdNum_FirstName_LastName** ذخیره کرده و ارسال نمائید.

سوال ۱ بهینه‌سازی (۱۵ نمره)

در روند آموزش و بهینه‌سازی مدل‌های یادگیری ماشین، از روش‌های مختلفی برای بهبود سرعت و کارایی استفاده می‌شود. در این مورد به سوالات زیر پاسخ دهید.

(الف) (۳ نمره) نقش Momentum و نرخ یادگیری[۱] در بهینه‌ساز را توضیح دهید.

(ب) (۳ نمره) نقش برنامه‌ریز نرخ یادگیری[۲] چیست؟

(ج) (۳ نمره) در مورد عملکرد یک نمونه از برنامه‌ریزهایی که نرخ یادگیری را به صورت یکنواخت کاهش می‌دهند توضیح دهید.

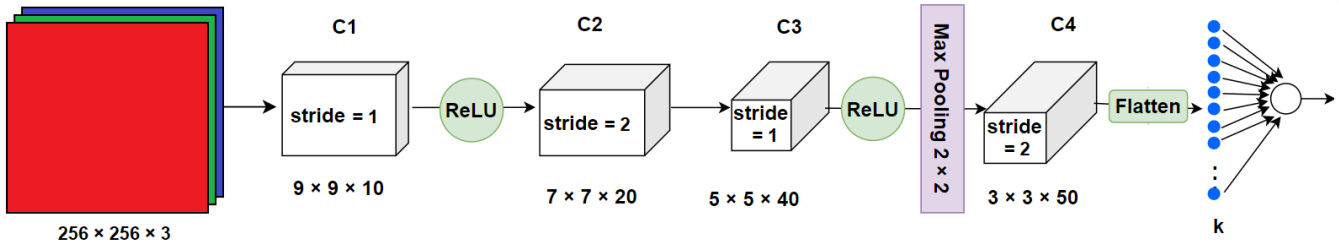
(د) (۳ نمره) در مورد یک برنامه‌ریز دیگر که در میانه‌ی آموزش، نرخ یادگیری را گاها افزایش می‌دهد توضیح دهید.

(هـ) (۳ نمره) تفاوت بین بهینه‌ساز Adam و Stochastic Gradient Descent را توضیح دهید (نوشتن جزئیات ریاضی لازم نیست و ذکر کلیات کافی است).

سوال ۲ (۱۰ نمره)

شبکه‌ی عصبی پیچشی شکل ۱ را در نظر بگیرید. در این شکل، ورودی در سمت چپ تصویر قرار دارد که از چهار لایه پیچشی C_1 تا C_4 عبور کرده و خروجی نهایی این لایه‌ها به یک شبکه تمام متصل داده می‌شود. ابعاد لایه‌گذاری[۳] را برای همه‌ی لایه‌ها برابر صفر در نظر بگیرید. اعداد نوشته شده در پایین هر لایه پیچشی به ترتیب از چپ به راست طول فیلتر، عرض فیلتر و تعداد فیلترها در آن لایه را مشخص می‌کند. گام لایه Max Pooling را نیز ۲ در نظر بگیرید.

[۱] Learning Rate
[۲] Learning Rate Scheduler
[۳] Padding



شکل ۱: شبکه پیچشی

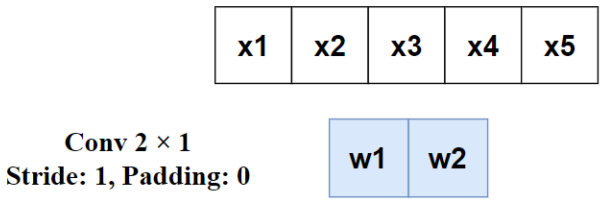
(الف) (۸ نمره) با توجه به توضیحات فوق و معماری رسم شده، مطابق جدول زیر، ابعاد خروجی C_1 تا C_4 (به همراه خروجی لایه مسطح‌ساز) را محاسبه کنید. همچنین تعداد کل پارامترهای شبکه (وزن‌ها و اریبی‌ها) را محاسبه کنید و مقدار k در شکل ۱ را مشخص کنید.

نام لایه	مشخصات لایه				ابعاد ورودی		ابعاد خروجی		پارامترهای لایه		هزینه پردازش (مگافلاپس)
	فیلترها	ابعاد فیلتر	لایه‌گذاری	گام	کانال‌ها	طول و عرض	کانال‌ها	طول و عرض	وزن‌ها	اریبی‌ها	
C_1	۱۰	۹ × ۹	۰	۱ × ۱	۳	۲۵۶ × ۲۵۶					
ReLU	–	–	–	–							
C_2	۲۰	۷ × ۷	۰	۲ × ۲							
C_3	۴۰	۵ × ۵	۰	۱ × ۱							
ReLU	–	–	–	–							
Max Pooling	–	۲ × ۲	۰	۲ × ۲							
C_4	۵۰	۳ × ۳	۰	۲ × ۲							
Flatten	–	–	–	–							
FC	–	–	–	–							

(ب) (۲ نمره) آیا عدم استفاده از تابع فعالساز بعد از لایه‌ی پیچشی C_2 روی قدرت مدل تاثیری دارد؟ چرا؟ در مورد C_4 چطور؟

سوال ۳ (۱۰ نمره)

یک لایه پیچشی تک بعدی همانند شکل ۲ را در نظر بگیرید که روی یک ورودی $x \in \mathbb{R}^{5\times 1}$ اعمال می‌شود. فرض کنید می‌خواهیم وزن‌های این



شکل ۲: یک لایه پیچشی تک بعدی

لایه را در یک ماتریس W نمایش دهیم.

(الف) (۳ نمره) عملیات پیچش را به صورت ضرب W در x بازنویسی کنید. به این منظور، ابعاد ماتریس وزن‌ها را به محاسبه کرده و سپس اعضای این ماتریس را مشخص کنید.

(ب) (۴ نمره) یکی از خواص شبکه‌های عصبی پیچشی، تنک[۴] بودن ماتریس وزن‌های لایه‌های پیچشی آن است. آیا این خاصیت در ماتریس به دست آمده در قسمت (الف) وجود دارد؟ توضیح دهید این خاصیت چه مزیت‌هایی برای مدل دارد.

(ج) (۳ نمره) محاسبات قسمت (الف) را برای یک فیلتر ۱×۴ با اندازه‌گام ۱ و لایه‌گذاری برابر ۰ دوباره تکرار کنید و در مورد تغییر وضعیت ماتریس W اظهار نظر کنید.

سوال ۴ (۱۲ نمره)

یکی از عملیاتی که در شبکه‌های عصبی پیچشی برای بهبود روند آموزش مدل به کار گرفته می‌شود، استفاده از نرمال‌سازی دسته‌ای[۵] است. در این مورد به سوالات زیر پاسخ دهید.

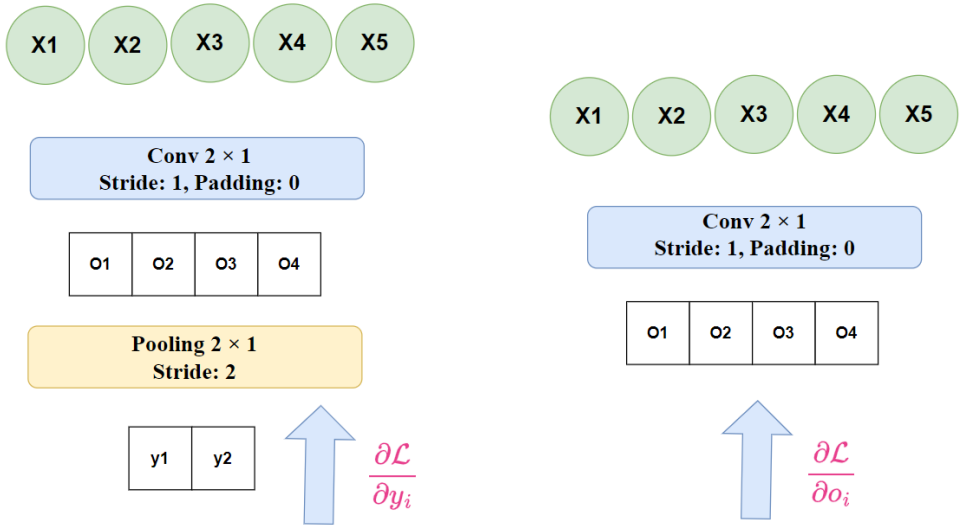
(الف) (۴ نمره) توضیح دهید که نرمال‌سازی دسته‌ای چگونه و چه کمکی به روند آموزش مدل کمک می‌کند؟

(ب) (۸ نمره) با در نظر گرفتن یک دسته داده به اندازه‌ی n که میانگین و واریانس آن به ترتیب برابر با μ و σ^2 است و با فرض اینکه مقدار گرادیان $\frac{\partial \mathcal{L}}{\partial y_i}$ را داریم، گرادیان تابع هزینه نسبت به β، γ و x_i را محاسبه کنید.

$$\mu \leftarrow \frac{1}{n}\sum_{i=1}^{n} x_i$$
$$\sigma^2 \leftarrow \frac{1}{n}\sum_{i=1}^{n} (x_i - \mu)^2$$
$$\widehat{x}_i \leftarrow \frac{x_i - \mu}{\sqrt{\sigma^2 + \epsilon}}$$
$$y_i \leftarrow \gamma \widehat{x}_i + \beta$$

سوال ۵ (۱۳ نمره)

در شبکه‌های عصبی پیچشی به طور رایج از دو عملیات Max Pooling و Average Pooling استفاده می‌شود. در این سوال می‌خواهیم نحوه عبور گرادیان از این دو لایه را بررسی کنیم. فرض کنید یک شبکه مانند شکل (۳الف) داریم. در این شبکه، یک ورودی $x \in \mathbb{R}^{5\times 1}$ داریم که از یک لایه



(ب) شبکه با لایه Pooling (الف) شبکه بدون لایه Pooling

شکل ۳: دو معماری متفاوت برای یک لایه

پیچشی تک‌بعدی عبور می‌کند و خروجی $[o_1\ o_2\ o_3\ o_4]^T$ را تولید می‌کند. وزن‌های این لایه را w_1 و w_2 در نظر بگیرید.

[۴] Sparse
[۵] Batch Normalization

(الف) (۳ نمره) ابتدا برای معماری شکل (۳الف)، با فرض این که مقادیر $\frac{\partial \mathcal{L}}{\partial o_1}$ تا $\frac{\partial \mathcal{L}}{\partial o_4}$ را داریم، مقادیر $\frac{\partial \mathcal{L}}{\partial w_1}$ و $\frac{\partial \mathcal{L}}{\partial w_2}$ را محاسبه کنید.

(ب) (۶ نمره) این بار فرض کنید مطابق معماری شکل (۳ب)، یک لایه Average Pooling بعد از لایه پیچشی داریم که خروجی $[y_1\ y_2]^T$ را تولید می‌کند. با فرض داشتن مقادیر $\frac{\partial \mathcal{L}}{\partial y_1}$ و $\frac{\partial \mathcal{L}}{\partial y_2}$ محاسبات قسمت (الف) را تکرار کنید و مقادیر به دست آمده را با مقادیر قسمت (الف) مقایسه کنید.

(ج) (۴ نمره) به جای Average Pooling عملیات Max Pooling را در نظر بگیرید و محاسبات قسمت (ب) را تکرار کنید (در محاسبات خود فرض کنید $o_1 < o_2$ و $o_3 > o_4$).

سوال ۶ عملی (۲۵ نمره)

در این سوال به کمک کتابخانه‌ی PyTorch به پیاده‌سازی شبکه‌های عصبی پیچشی خواهید پرداخت. برای حل این سوال به فایل CNN.ipynb مراجعه کنید.

سوال ۷ عملی (۲۵ نمره)

در این سوال به پیاده‌سازی دسته‌ای از خودکدگذارها به نام خودکدگذارهای حذف‌کننده نویز خواهید پرداخت. برای حل این سوال به فایل DAE.ipynb مراجعه کنید.

موفق باشید