به نام خدا

امنیت و حریم خصوصی در یادگیری ماشین (۴۰۸۱۶)

نیم‌سال اول سال تحصیلی ۱۴۰۵-۱۴۰۴

استاد درس: دکتر امیرمهدی صادق‌زاده

طراحان: فیروزه ابریشمی - علیرضا فرج تبریزی

دانشکده مهندسی کامپیوتر

تمرین ۰ (مرور ریاضیات) | مهلت تحویل: ساعت ۲۳:۵۹:۵۹ ۱۰ آبان ۱۴۰۴

نکات و قواعد

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

۲. 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.

۳. از تحویل تمرینات نظری به شکل تایپ شده (فایل latex-word یا هر نوع تایپ شده دیگری) بپرهیزید و حتما پاسخ دست نویس تحویل دهید.

۴. 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_HW0_StdNum_FirstName_LastName ذخیره کرده و ارسال نمائید.

سوال ۱ تجزیه مقدار تکین (SVD) و کاربردهای آن (نمره)

فرض کنید A یک ماتریس حقیقی $m \times n$ با رتبه r باشد. تجزیه مقدار تکین[۱] این ماتریس به صورت $A = U\Sigma V^T$ است که در آن $U \in \mathbb{R}^{m\times m}$ و $V \in \mathbb{R}^{n\times n}$ ماتریس‌های متعامد[۲] بوده و $\Sigma \in \mathbb{R}^{m\times n}$ یک ماتریس شبه‌قطری است که مقادیر تکین[۳] را به صورت نزولی روی قطر اصلی خود دارد:

$$\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_r > 0$$

بخش الف) ارتباط نورم ماتریس با بزرگترین مقدار تکین

نورم طیفی[۴] یا نورم‌ـ۲ القایی یک ماتریس به صورت $\|A\|_2 = \max_{\|x\|_2=1} \|Ax\|_2$ تعریف می‌شود. ثابت کنید که نورم طیفی ماتریس A دقیقاً برابر با بزرگترین مقدار تکین آن، یعنی σ_1 است.

بخش ب) ارتباط SVD با تجزیه ویژه[۵]

فرض کنید A یک ماتریس مربعی، متقارن[۶] $(A = A^T)$ و معین نیمه‌مثبت[۷] باشد. ارتباط بین تجزیه مقدار تکین $(A = U\Sigma V^T)$ و تجزیه ویژه $(A = PDP^T)$ این ماتریس چیست؟ پاسخ خود را توجیه کنید.

[1] Singular Value Decomposition (SVD)
[2] Orthogonal Matrices
[3] Singular Values
[4] Spectral Norm
[5] Eigen-decomposition
[6] Symmetric
[7] Positive Semidefinite

بخش ج) قضیه Eckart-Young-Mirsky و تقریب بهینه

قضیه Eckart-Young-Mirsky بیان می‌کند که بهترین تقریب رتبه-k[8] برای ماتریس A (از نظر نورم فروبنیوس[9] و نورم طیفی)، ماتریس $A_k = \sum_{i=1}^{k} \sigma_i u_i v_i^T$ است. ثابت کنید که خطای این تقریب از نظر نورم طیفی برابر است با:

$$\|A - A_k\|_2 = \sigma_{k+1}$$

بخش د) یکتایی (Uniqueness) در SVD

آیا تجزیه مقدار تکین یک ماتریس دلخواه A لزوماً یکتا است؟ اگر خیر، عدم یکتایی در این تجزیه را به طور دقیق شرح دهید.

بخش ه) پیاده‌سازی عملی: تقریب رتبه پایین تصویر

مفهوم تقریب رتبه-k در بخش (ج) کاربرد وسیعی در فشرده‌سازی تصویر دارد. برای پیاده‌سازی این بخش، فایل نوت‌بوک **HW0_SVD.ipynb** را باز کرده و بخش‌های مشخص شده با **TODO** را تکمیل نمایید. مراحل کلی کار در نوت‌بوک به شرح زیر است:

۱. SVD تصویر نمونه بارگذاری شده را محاسبه کنید.

۲. تصویر را برای پنج مقدار مختلف k بازسازی نمایید: $k \in \{5, 15, 30, 50, 100\}$. تصاویر بازسازی‌شده را در کنار یکدیگر نمایش دهید تا تفاوت کیفیت به وضوح قابل مشاهده باشد.

۳. برای هر یک از مقادیر k فوق، خطای تقریب $\|A - A_k\|_2$ را به صورت عملی محاسبه کرده و آن را با مقدار تئوری متناظر (σ_{k+1}) مقایسه کنید.

۴. در پایان، نتیجه را تحلیل نمایید. توضیح دهید که چگونه با افزایش k، کیفیت تصویر و خطای تقریب تغییر می‌کند و این موضوع چه ارتباطی با مفهوم فشرده‌سازی تصویر دارد.

[8] Rank-k Approximation
[9] Frobenius Norm

سوال ۲ کانولوشن با کرنل گاوسی و هموارسازی سیگنال (نمره)

عمل کانولوشن[10] یک سیگنال با یک هسته (فیلتر) گاوسی[11]، یکی از پایه‌ای‌ترین و در عین حال قدرتمندترین روش‌ها برای هموارسازی و حذف نویز است. این تمرین به بررسی جنبه‌های مختلف این فرآیند از دیدگاه‌های متفاوت می‌پردازد.

بخش الف) تحلیل از دیدگاه حسابان: خاصیت مشتق

یکی از دلایل اصلی که کانولوشن با گاوسی منجر به «هموار» شدن سیگنال می‌شود، به خواص مشتق‌پذیری آن بازمی‌گردد.

۱. «قضیه مشتق کانولوشن» را ثابت کنید. یعنی نشان دهید که مشتق عمل کانولوشن برابر است با کانولوشن سیگنال با مشتق کرنل:

$$\frac{d}{dt}(f * g) = f * \frac{dg}{dt}$$

۲. با توجه به اینکه کرنل گاوسی (g_σ) بی‌نهایت بار مشتق‌پذیر است، با استفاده از قضیه‌ی بالا توضیح دهید که چرا کانوالو کردن یک سیگنال دلخواه (حتی سیگنال ناپیوسته مانند یک پله) با یک فیلتر گاوسی، سیگنالی را نتیجه می‌دهد که بی‌نهایت بار مشتق‌پذیر و در نتیجه بسیار هموار است.

بخش ب) تحلیل در حوزه فرکانس[12]: شهود فیلتر پایین‌گذر

قدرت واقعی درک هموارسازی گاوسی در حوزه فرکانس نهفته است. قضیه کانولوشن[13] بیان می‌کند که کانولوشن در حوزه زمان/فضا معادل ضرب نقطه‌ای در حوزه فرکانس است: $\mathcal{F}\{f * g\} = \mathcal{F}\{f\} \cdot \mathcal{F}\{g\}$.

۱. با دانستن این‌که تبدیل فوریه[14] یک تابع گاوسی، خود یک تابع گاوسی دیگر است، به صورت شهودی توضیح دهید که چرا عمل کانولوشن با فیلتر گاوسی مانند یک فیلتر پایین‌گذر[15] عمل می‌کند. به عبارت دیگر، این فرآیند چگونه مولفه‌های فرکانس‌بالا (نویز و جزئیات سریع) را تضعیف کرده و مولفه‌های فرکانس‌پایین (ساختار کلی سیگنال) را حفظ می‌کند؟

۲. انحراف معیار کرنل گاوسی در حوزه زمان (σ)، چه تاثیری بر رفتار فیلتر در حوزه فرکانس دارد؟ توضیح دهید که چگونه افزایش σ (یعنی پهن‌تر شدن گاوسی در حوزه زمان) باعث تنگ‌تر شدن فیلتر پایین‌گذر در حوزه فرکانس و در نتیجه هموارسازی شدیدتر سیگنال می‌شود.

بخش ج و د) پیاده‌سازی عملی در نوت‌بوک

برای پیاده‌سازی و تحلیل بخش‌های عملی این سوال، فایل نوت‌بوک **Hw0_Gaussian_Filter.ipynb** را باز کرده و بخش‌های مشخص شده با **TODO** را تکمیل نمایید.

- در بخش اول نوت‌بوک (مربوط به بخش ج):

۱. یک سیگنال یک‌بعدی تمیز تولید کرده و با افزودن نویز، نسخه نویزی آن را می‌سازید.
۲. سیگنال نویزی را با دو کرنل گاوسی با انحراف معیارهای متفاوت هموار می‌کنید.
۳. مقایسه کمّی خطا: با محاسبه نورم‌ـ۲ تفاضل، بررسی کنید که کدام سیگنال به سیگنال تمیز و اصلی نزدیک‌تر است: سیگنال نویزی یا سیگنال‌های هموارشده؟

مقایسه کنید: $\|S_{\text{clean}} - S_{\text{noisy}}\|_2$ vs. $\|S_{\text{clean}} - S_{\text{smoothed}}\|_2$

۴. با رسم طیف فرکانسی سیگنال‌ها، اثر فیلتر پایین‌گذر را به صورت عملی تحلیل کرده و توضیح دهید که چگونه این اثر منجر به کاهش خطای محاسبه شده در گام قبل می‌شود.

- در بخش دوم نوت‌بوک (مربوط به بخش د):

[10] Convolution
[11] Gaussian Kernel (Filter)
[12] Frequency Domain
[13] Convolution Theorem
[14] Fourier Transform
[15] Low-pass Filter

۱. تصویر نمونه را بارگذاری کرده و به آن نویز گوسی اضافه کنید.
۲. با اعمال فیلتر گاوسی دو بعدی، تصویر نویزی را هموار (denoise) نمایید.
۳. مقایسه کمّی خطا: با محاسبه نورم‌ـ۲ تفاضل، بررسی کنید که کدام تصویر به تصویر اصلی نزدیک‌تر است: تصویر نویزی یا تصویر هموارشده؟

مقایسه کنید: $\|A_{\text{original}} - A_{\text{noisy}}\|_2 \quad \text{vs.} \quad \|A_{\text{original}} - A_{\text{smoothed}}\|_2$

۴. تحلیل نتیجه: اثر هموارسازی (بلور) و بده بستان (trade-off) بین حذف نویز و حفظ جزئیات تصویر را بررسی کرده و توضیح دهید که از نظر تئوری انتظار داریم کدام تصویر به تصویر اصلی نزدیک‌تر باشد؟

موفق باشید.