باسمه تعالی
جمهوری اسلامی ایران
وزارت آموزش و پرورش
باشگاه دانش‌پژوهان جوان

دفترچه سوال رسمی آزمون
واحد سنجش و ارزیابی باشگاه دانش‌پژوهان جوان

علم برای یک ملّت مهم‌ترین ابزار آبرو، پیشرفت و اقتدار است. «امام خامنه‌ای (ره)»

دفترچهٔ سؤالات مرحلهٔ دوم سال تحصیلی ۱۴۰۵-۱۴۰۴

دومین دورهٔ المپیاد هوش مصنوعی

مدت پاسخگویی: ۱۵۰ دقیقه	نوع آزمون: تشریحی
	تعداد سؤالات: ۴

توضیحات مهم

استفاده از هرنوع ماشین‌حساب ممنوع است.

۱- مشخصات خود را با اطلاعات بالای هر صفحه تطبیق دهید در صورتی که حتی یکی از صفحات پاسخ نامه با مشخصات شما هم‌خوانی ندارد بلافاصله مراقبین را مطلع نمایید.

۲- پاسخ هر سوال را در محل تعیین شده خود بنویسید. چنانچه همه یا قسمتی از جواب سوال را در محل پاسخ سوال دیگری بنویسید به شما نمره ای تعلق نمی گیرد.

۳- با توجه به آنکه برگه های پاسخ نامه به نام شما صادر شده است امکان ارائه هیچ‌گونه برگه اضافه وجود نخواهد داشت. لذا توصیه می‌شود ابتدا سوالات را در برگه چرک نویس، حل کرده و آنگاه در پاسخ‌برگ پاکنویس نمایید.

٤- عملیات تصحیح توسط مصححین پس از برش سربرگ به صورت ناشناس انجام خواهد شد. لذا از درج هرگونه نوشته یا علامت مشخصه که نشان دهنده صاحب برگه باشد، خودداری نمایید. در غیر این صورت تقلب محسوب شده و در هر مرحله ای که باشید از ادامه حضور در المپیاد محروم خواهید شد.

٥- از مخدوش کردن **بارکدها و مربع‌ها در چهارگوشهٔ صفحه در دفترچهٔ پاسخ‌برگ** جداً خودداری کنید. در غیر این صورت برگهٔ شما تصحیح نخواهد شد.

٦- همراه داشتن هر گونه کتاب جزوه یادداشت و لوازم الکترونیکی نظیر تلفن همراه، ساعت هوشمند، دستبند هوشمند و لپ تاپ ممنوع است همراه داشتن این قبیل وسایل حتی اگر از آن استفاده نکنید یا خاموش باشد تقلب محسوب خواهد شد.

۷- این دفترچه شامل ۴ سوال و با احتساب جلد ۲ برگ است.

این صفحه جهت استفاده به عنوان چرک‌نویس در نظر گرفته شده است.

۱ یک عامل هوش مصنوعی (AI Agent) برای رسیدن به «وضعیت هدف» (Terminal State)، در هر گام تصمیم‌گیری یکی از سه الگوریتم زیر را اجرا می‌کند:

- **با احتمال ۵۰ درصد الگوریتم A را انتخاب می‌کند:** اجرای آن ۳ ثانیه طول می‌کشد و عامل را مجدداً به وضعیت اولیه برمی‌گرداند.
- **با احتمال ۳۰ درصد الگوریتم B را انتخاب می‌کند:** اجرای آن ۵ ثانیه طول می‌کشد و عامل را مجدداً به وضعیت اولیه برمی‌گرداند.
- **با احتمال ۲۰ درصد الگوریتم C را انتخاب می‌کند:** اجرای آن ۲ ثانیه طول می‌کشد و عامل با موفقیت به وضعیت هدف می‌رسد.

عامل فاقد حافظه بلندمدت است؛ بنابراین هر بار که به وضعیت اولیه برمی‌گردد، فرآیند انتخاب با همان احتمالات اولیه تکرار می‌شود. با این حال، الگوریتم A یک استثناست: اگر عامل یک‌بار الگوریتم A را اجرا کند، متوجه بن‌بست شده و آن را برای همیشه در «لیست سیاه» قرار می‌دهد تا دیگر هرگز انتخاب نشود (در این حالت، احتمال انتخاب B و C با حفظ نسبت اولیه پخش می‌شود). الگوریتم B این ویژگی را ندارد و ممکن است بارها انتخاب شود. مقدار دقیق امید ریاضی زمان لازم (بر حسب ثانیه) برای رسیدن عامل به وضعیت هدف را محاسبه کنید.

۲ یک سیستم تشخیص ناهنجاری (Anomaly Detection) مبتنی بر یادگیری ماشین، رفتار شبکه‌ای را با بردارهایی در فضای $\mathbb{R}^d$ مدل می‌کند. این سیستم از طریق اجرای الگوریتم تحلیل مؤلفه‌های اصلی (PCA) روی ماتریس کوواریانس داده‌ها (C)، مؤلفه اصلی غالب v_1 (متناظر با بزرگترین مقدار ویژه λ_1) را به عنوان الگوی رفتار طبیعی شبکه استخراج می‌کند. ماتریس C متقارن و مقادیر ویژه آن به صورت متمایز $\lambda_1 > \lambda_2 > \cdots > \lambda_d \geqslant 0$ مرتب شده‌اند.

یک مهاجم سایبری (Adversary) قصد دارد با تزریق داده‌های مسموم، سیستم را فریب دهد تا جهت دلخواه او، یعنی بردار یکه u، را به عنوان مؤلفه اصلی غالب جدید (رفتار طبیعی) بپذیرد. برای پنهان ماندن حمله، مهاجم بردار u را برابر با یکی از بردارهای ویژه کم‌اهمیت‌تر ماتریس C (متناظر با مقدار ویژه λ_k که $k > 1$) انتخاب می‌کند.

تزریق این داده‌ها باعث می‌شود ماتریس کوواریانس سیستم به صورت زیر مخدوش شود:

$$\tilde{C} = C + \alpha u u^T$$

که در آن ثابت $\alpha > 0$ نشان‌دهنده «بودجه حمله» (قدرت سیگنال مسموم) است.

- الف) از نظر ریاضی ثابت کنید که با وجود این حمله، بردار v_1 همچنان یک بردار ویژه برای ماتریس مخدوش $\tilde{C}$ باقی می‌ماند.
- ب) مقدار دقیق کمترین بودجه حمله ($\min \alpha$) را به دست آورید که موفقیت مهاجم را تضمین می‌کند؛ یعنی مقداری که باعث می‌شود بردار u به طور قطع جایگزین v_1 شده و به مؤلفه اصلی غالب ماتریس $\tilde{C}$ تبدیل شود.

۳ شما در حال برنامه‌نویسی یک مدل رگرسیون خطی (Linear Regression) برای پیش‌بینی انحراف مسیر یک ماهواره هستید. به دلیل محدودیت‌های سخت‌افزاری و برای جلوگیری از دستورات رانش با دامنه بالا، وزن‌های بزرگ در مدل باید جریمه شوند. شما به جای استفاده از روش‌های استاندارد، یک تابع منظم‌ساز (Regularizer) سفارشی به شکل زیر طراحی کرده‌اید:

$$R(w) = \lambda \log(1 + w^2)$$

بنابراین، تابع هزینه (Loss Function) مدل برای یک داده آموزشی (x, y) و مدلی که تنها دارای یک پارامتر وزن w (بدون بایاس) است، به صورت زیر تعریف می‌شود:

$$J(w) = \frac{1}{2}(y - wx)^2 + \lambda \log(1 + w^2)$$

الف) فرمول دقیق به‌روزرسانی وزن w را در الگوریتم گرادیان کاهشی (Gradient Descent) با نرخ یادگیری η محاسبه کنید.

ب) برای تحلیل رفتار تابع هزینه، فرض کنید یک داده آموزشی با مقادیر $x = ۱$ و $y = ۱$ به مدل داده شده است. معادله‌ای که نقاط ایستای (Stationary points) تابع زیان را در این حالت مشخص می‌کند، به دست آورید و آن را به شکل یک چندجمله‌ای استاندارد بر حسب w بنویسید.

ج) با استفاده از چندجمله‌ای به‌دست‌آمده در قسمت (ب)، از نظر ریاضی ثابت کنید که برای هر ضریب منظم‌سازی مثبت ($\lambda > ۰$)، تابع هزینه تنها دارای یک نقطه مینیمم محلی (که مینیمم سراسری نیز هست) می‌باشد. سپس نشان دهید که این وزن بهینه همواره در بازه $(۰, ۱)$ قرار دارد و با افزایش مقدار λ، مدل به شدت به سمت وضعیت کم‌برازش (Underfitting) و میل کردن وزن به سمت صفر سوق پیدا می‌کند.

۴ یک پهپاد خودران از یک شبکه عصبی برای پردازش داده‌های حسگرهای خود و پیش‌بینی اصلاحات مسیر پروازی استفاده می‌کند. برای افزایش توانایی شبکه در استخراج ویژگی‌های پیچیده، این شبکه اکنون دارای **دو لایه فعال‌ساز غیرخطی** است. برای اطمینان از اینکه داده‌های پایه حسگر در طول پردازش به طور کامل از بین نمی‌روند، یک اتصال پسماند (Skip connection) ورودی اولیه را مستقیماً به پیش از فعال‌ساز لایه نهایی اضافه می‌کند.

فرض کنید بردار ویژگی‌های ورودی $x \in \mathbb{R}^d$ و بردار هدف واقعی $y \in \mathbb{R}^d$ باشد. مسیر پیش‌رو (Forward pass) این شبکه به صورت زیر تعریف می‌شود:

$$z^{(۱)} = W^{(۱)}x + b^{(۱)}$$

$$a^{(۱)} = \sigma_۱(z^{(۱)})$$

$$z^{(۲)} = W^{(۲)}a^{(۱)} + b^{(۲)} + x$$

$$\hat{y} = \sigma_۲(z^{(۲)})$$

که در آن:

۱. $W^{(۱)} \in \mathbb{R}^{h \times d}$ و $b^{(۱)} \in \mathbb{R}^h$ ماتریس وزن‌ها و بردار بایاس در لایه اول هستند.

۲. $W^{(۲)} \in \mathbb{R}^{d \times h}$ و $b^{(۲)} \in \mathbb{R}^d$ ماتریس وزن‌ها و بردار بایاس در لایه دوم هستند.

۳. $\sigma_۱$ و $\sigma_۲$ توابع فعال‌ساز غیرخطی درایه به درایه (Element-wise) هستند.

این شبکه با استفاده از تابع خطای میانگین مربعات (MSE) آموزش داده می‌شود:

$$J(\hat{y}, y) = \frac{۱}{۲}||\hat{y} - y||_۲^۲$$

الف) ابتدا بردار خطای محلی لایه دوم یعنی $\delta^{(۲)} = \nabla_{z^{(۲)}} J$ را به دست آورید. سپس با استفاده از آن، گرادیان‌های تابع خطا نسبت به پارامترهای لایه دوم یعنی $\nabla_{W^{(۲)}} J$ و $\nabla_{b^{(۲)}} J$ را محاسبه کنید.

ب) گرادیان‌های تابع خطا نسبت به پارامترهای لایه اول یعنی $\nabla_{W^{(۱)}} J$ و $\nabla_{b^{(۱)}} J$ را به دست آورید. (راهنمایی: ابتدا عبارت خطای محلی $\delta^{(۱)} = \nabla_{z^{(۱)}} J$ را پیدا کنید).

پ) گرادیان تابع خطا نسبت به بردار ورودی اولیه یعنی $\nabla_x J$ را محاسبه کنید. با فرض اینکه در هنگام مقداردهی اولیه، ماتریس‌های وزن دارای میانگین صفر هستند ($\mathbb{E}[W^{(۱)}] = \mathbb{E}[W^{(۲)}] = ۰$) و از ورودی‌ها مستقل‌اند، از نظر ریاضی ثابت کنید که چگونه وجود این اتصال پسماند باعث می‌شود که «به طور میانگین» (در امید ریاضی)، سیگنال گرادیان بدون کاهش و افت شدید به ورودی بازگردد و شبکه در برابر مشکل محوشدگی گرادیان (Vanishing Gradient) مقاوم شود.