# سوال اول: مرور جبر خطی

## ۱)

## ۲)

الف)

ب)

پ)

ت)

## ۳)

# سوال دوم: بهینه‌سازی

## ۱)

به صورت شهودی، هم برای نقطه زینی، و هم برای کمینه محلی، شرط صفر بودن مشتق جزئی در تمام جهات وجود دارد. اما برای کمینه محلی بودن، باید ماتریس Hessian، مثبت معین باشد، یعنی تمام مقادیر ویژه آن باید مثبت باشند. *[[1]](#footnote-1)* این در شرایطی است که برای نقطه زینی‌بودن، باید ماتریس Hessian هم مقادیر ویژه مثبت، و هم مقادیر ویژه منفی داشته باشد. از دید احتمالی، هرچه تعداد ابعاد بالاتر می‌رود، احتمال اینکه تمام مقادیر ویژه ماتریس هم‌علامت نباشند،‌ بالاتر می‌رود. در واقع، با بالاتر رفتن ابعاد، احتمال اینکه با حرکت در حداقل یک جهت، علامت مشتق خلاف جهات دیگر شود، بالاتر از اینکه علامت مشتق در حرکت در تمام جهات یکسان باشد خواهد بود.

## ۲)

الف)

نمودار مشکی،‌ که تقریبا با مسیری مستقیم به نقطه بهینه رسیده‌است، احتمالا مربوط به روش RMSprop است. این روش، که یک روش تطبیقی برای نرمال‌سازی نرخ یادگیری با میانگین متحرک (Moving Average) مربع گرادیان‌هاست، نرخ یادگیری هر وزن را، بر اساس این میانگین نمایی، اسکیل می‌کند. در چنین روشی، و برای تابع مرتبه دو، با هایپرپارامترهای معقول، احتمال اینکه مسیرمان به نقطه بهینه مستقیم باشد، بیشتر از روش‌های دیگر است.

نمودار سبز، احتمالا مربوط به روش momentum است. در این روش، با معرفی مفهوم تکانش و velocity، گرادیان‌های قبلی در آپدیت velocity دخیل هستند. بنابراین،‌ هر چه در مسیری مستمر حرکت کنیم، وقتی به نقطه‌ای برسیم که گرادیان محاسبه‌شده، جهت را تغییر می‌دهد، به خاطر velocity و تاثیر گرادیان‌های قبل‌، محتمل است که چند گام دیگر در راستای مسیر پیشین برداریم، پیش از آنکه مسیر تغییر کند. این تفسیر از نحوه کارکرد روش momentum در این مورد خاص،‌ با نمودار سبز همخوانی دارد.

نمودار قرمز، احتمالا مربوط به روش Nestrov-Momentum است. این روش، عملکرد روش momentum را اندکی بهبود می‌بخشد و با دخالت‌دادن velocity در محاسبه گرادیان، جهت حرکت کنونی را اندکی تغییر می‌دهد. این امر، منجر به بهبود در سرعت همگرا شدن، و کاهش زیگزاگ می‌شود. نمودار قرمز، با نحوه عملکرد این روش هم‌خوان است.

ب)

مشکل روش GD، کند بودن آن، و احتمال گیر کردن در نقطه مینیمم محلی است. در خصوص نحوه کارکرد هر ۳ روش و مزایا و معایب آن‌ها، در قسمت قبل تا حدی توضیح داده شد. به طور خلاصه، در مقایسه با GD، هر یک از روش‌ها این مزایا و معایب را دارند:

* روش Momentum، با دخالت‌دادن گرادیان‌های قبلی،‌ در حرکت یک momentum ایجاد می‌کند که منجر می‌شود از نقاط مینیمم محلی سطحی، به راحتی عبور کرد. با این حال، این momentum، همان‌گونه که در مثال تصویری دیدیم، ممکن است سبب شود که تغییر در جهت حرکت، به علت جمع‌شدن تاثیرات گرادیان‌های قبلی، کندتر انجام شود.
* روش Nestrov-Momentum،‌ مزیت روش Momentum را دارد و عملکرد آن‌را تا حدی بهبود می‌بخشد. این روش، با دخالت velocity کنونی در محاسبه گرادیان، به نوعی با آینده‌نگری، مسیر همگرایی را Smoothتر، و همگرایی را سریع‌تر می‌کند. با این حال، این روش هم می‌تواند زیگزاگ‌های بی‌هدف را در پی داشته باشد که با وجود همگرا شدن، مسیر همگرا شدن را غیربهینه می‌کند.
* روش RMSprop، با Adapt کردن نرخ یادگیری برای وزن‌های مختلف، منجر به نوسان کمتری شده و سرعت همگرایی را نیز بهبود می‌بخشد. در عین حال، این روش می‌تواند به انتخاب هایپرپارامترهایی نظیر نرخ میرایی (در محاسبه میانگین نمایی)، و نرخ یادگیری اولیه، بیشتر از روش‌های قبل حساس‌ باشد.

پ)

روش ADAM،‌ به نوعی دو روش Momentum،‌ و RMSprop را ترکیب کرده و ضعف‌های روش Momentum را بهبود می‌بخشد؛ یک مشکل اساسی روش Momentum این است که ممکن است حتی موقع رسیدن به نقطه مینیما، به علت Momentumيی که جمع‌شده، از آن نقطه بگذرد. در روش ADAM، علاوه بر Momentum (موسوم به moment اول)، میانگین نمایی مربع گرادیان‌ها در روش RMSprop نیز معرفی شده‌است. مطابق روش Momentum، گرادیان‌های قبلی نیز با میانگین نمایی در بروزرسانی وزن‌ها دخیل هستند. اما میزان بروزرسانی، توسط جذر ترم دوم، نرمال‌سازی می‌شود تا از Overshoot کردن نقطه مینیما جلوگیری شود.

# سوال سوم: منظم‌سازی

۱)

متدهای Ensemble، با تجمیع و اثردادن به خروجی چند مدل که در ساختار و معماری مدل،‌ یا داده ورودی تفاوت داشتند، تلاش می‌کردند واریانس را کاهش داده و از Overfit شدن مدل جلوگیری نمایند. مطابق مقاله معرفی‌شده، تکنیک Dropout، که در آن نورون‌هایی، به همراه تمام کانکشن‌هایشان به صورت رندم در حین آموزش دراپ می‌شوند، معادل یادگیری تعداد نمایی از مدل‌های با وزن مشابه، و میانگین‌گرفتن از خروجی آن‌ها عمل می‌کند، که کاری معادل روش‌های Ensemble است.

علت برتری این متد به روش‌های Ensemble در شبکه‌های با تعداد پارامتر بالا، اینست که این متد، از لحاظ محاسباتی بسیار Efficientتر است. استفاده از روش‌های Ensemble، نیاز به آموزش و نگه‌داری وزن‌های تعداد بالایی مدل شبکه عصبی عمیق، با تعداد بسیار بالای پارامتر دارد. تکنیک Dropout، عملا همین کار را شبیه‌سازی می‌کند، و در واقع از نتیجه تعداد بالایی از شبکه‌های عصبی سبک‌تر شده، میانگین می‌گیرد. اما این‌کار، در حین یک بار آموزش شبکه عصبی اتفاق می‌افتد که بسیار کاراتر، و پرکتیکال است.

۲)

با افزودن نویز و Randomness به فرایند یادگیری مدل، تکنیک Dropout از Overfit شدن مدل جلوگیری می‌کند؛ به بیان دیگر، با حذف رندم تعدادی نورون در حین آموزش، شبکه یاد می‌گیرد که با خروجی یک نورون وابسته نشود، و بر اساس خروجی یک نمونه از نورون‌های ورودی، فیچرهای مستقلی از ورودی را یاد گیرد. این عمل، که به کاهش معنادار احتمال Overfit شدن مدل منجر می‌شود، تکنیک Dropout را معادل یک تکنیک منظم‌سازی می‌کند.

۳)

تفاوت اساسی استفاده از تکنیک Dropout در ترین و تست مدل، اینست که در هنگام تست، Dropout اعمال نمی‌شود و هیچ واحدی از شبکه به صورت رندم حذف نمی‌گردد؛ چرا که می‌خواهیم از تمام قدرت شبکه برای پیش‌بینی استفاده کنیم. با این حال، به علت اینکه در حین ترین‌شدن نورون‌هایی به همراه کانکشن‌هایشان با احتمال معینی دراپ شده‌اند، در هنگام تست، وزن‌ها، با نسبت احتمال Dropout، Scale-Down می‌شوند تا مقدار مورد انتظار خروجی هر واحد، در ترین و تست برابر باشد.

۴)

۵)

- با نرمال‌سازی توزیع ورودی هر لایه، تکنیک Batch-Normalization، می‌تواند ریسک تغییر داخلی Covariance (Internal Covariance Shift)، که می‌تواند به خاطر تغییر در توزیع داده‌های ورودی اتفاق بیفتد را کم می‌کند. [[2]](#footnote-2) به همین خاطر،‌ می‌تواند از مقادیر بالاتری برای نرخ یادگیری، بدون نگرانی از خطر واگرایی استفاده نمود.

- این تکنیک، با نگه‌داشتن متوسط، و واریانس دیتای ورودی در یک رنج خاص، باعث پایداری مدل می‌شود، و احتمال مشکلاتی نظیر Vanishing Gradient، و Exploding Gradient را کم می‌کند. کاهش ریسک این خطرات، به ما آزادی بیشتری در کنترل نرخ یادگیری بدون نگرانی در خصوص این موارد می‌دهد.

۶)

تکنیک Batch-Normalization، با محاسبه میانگین و واریانس هر mini-batch، و نرمال‌سازی داده‌های mini-batch بر اساس این مقادیر، به گونه‌ای نویز وارد مدل می‌کند. چرا که هر بچ، میانگین و واریانس خود را خواهد داشت، و داده‌های آن بر اساس این میانگین و واریانس نرمال‌سازی خواهند شد. (نه میانگین و واریانس کل نمونه‌ها). این تفاوت در پارامترهای نرمال‌سازی هر بچ‌ را می‌توان به افزودن نویز،‌ و رندم‌نس به دیتا تفسیر کرد، که می‌تواند که لایه‌های مدل را وادار به این کند که فیچرهای اصلی‌تر، و منسجم‌تری را یاد بگیرند و Generalization بهتر انجام شود.

با بزرگ‌تر شدن سایز بچ، میانگین و واریانس تخمینی، به میانگین و واریانس واقعی نمونه‌ها نزدیک‌تر شده و نرمال‌سازی، دارای نویز و رندم‌نس پایین‌تری خواهد بود. به عنوان مثال اگر ۱۰۰۰ نمونه داشته‌باشیم و سایز بچ ۵۰۰ باشد، بسیار محتمل است که میانگین و واریانس هر بچ بسیار نزدیک به هم، و نزدیک به میانگین و واریانس کل نمونه‌ها باشد. (نسبت به بچ ۵۰تایی). این امر با کاهش اثر نویز و رندم‌نس، اثر منظم‌سازی Batch-Normalization را کم‌تر می‌کند، و احتمال Overfitشدن مدل بالاتر می‌رود. در عین حال و از سوی دیگر، ترین‌شدن مدل پایداری بیشتری داشته و احتمال همگرایی بیشتر می‌شود، چرا که بچ‌ها توزیع مشابه یکدیگر دارند و این امر پایداری را بالاتر می‌برد.

# سوال چهارم: توابع فعال‌سازی

۱)

(آ)

تابع سیگموید برای این طبقه‌بندی باینری مناسب است. خروجی تابع سیگموید یک عدد بین ۰ تا ۱ است که یک مقدار احتمالی را نشان می‌دهد. برای تسک دسته‌بندی باینری بین سگ و گربه، این تابع بهینه است.

(ب) تابع Softmax برای این طبقه‌بندی چند‌کلاسه مناسب‌تر است. خروجی این تابع، یک توزیع احتمالاتی، با ابعاد به اندازه تعداد کلاس‌هاست که برای هر کلاس، یک احتمال به آن نسبت می‌دهد و مجموع تمام احتمال‌ها، یک خواهد بود.

(ج)

یک تابع سیگموید، به ازای هر نورون در لایه خروجی (به تعداد کلاس‌های موجود) برای این مسئله مناسب است. از آن‌جایی که مسئله طبقه‌بندی چندکلاسه و چندلیبله است، هر نورون با تابع سیگموید، به عنوان نماینده یک کلاس عمل می‌کند که می‌تواند مقداری بین صفر و یک را داشته‌باشد و بیانگر حضور، یا عدم حضور یک حیوان در عکس باشد.

۲)

تابع ReLU، یکی از پرکاربردترین توابع در لایه‌های پنهان شبکه‌های عصبی عمیق است؛ اما صفر بودن مقدار این تابع برای مقادیر کوچک‌تر از صفر، می‌تواند مشکل‌ساز شود. (موسوم به مشکل Dying ReLU). برای حل این مسئله، Variantهای مختلفی از این تابع نظیر LeakyReLU معرفی شده‌اند. تابع DPReLU (Dynamic Parameter ReLU)، به صورت پویا، در طی آموزش، شکل خود را تغییر می‌دهد. این تابع، ۴ پارامتر قابل یادگیری در طی آموزش را اضافه می‌کند. با اضافه‌کردن این پارامترها، بسته به مدل و دامنه مسئله، می‌توان نسخه‌ای منعطف از ReLU، که برای مدل بهینه است را یاد گرفت. چهار پارامتر قابل یادگیری این تابع عبارتند از:

* آلفا، که شیب قسمت منفی تابع را کنترل می‌کند.
* بتا، که شیب قسمت مثبت تابع را کنترل می‌کند.
* بایاس، که تابع را به بالا یا پایین شیفت می‌دهد.
* آستانه (Threshold)، که تابع را به چپ یا راست شیف می‌دهد و در واقع آستانه‌ای که مرز میان قسمت مثبت و منفی تابع را کنترل می‌کند را تعیین می‌کند.

نسخه‌های قبلی این تابع، از جمله PReLU و FReLU، تنها دو تا از چهار پارامتر قابل یادگیری (آلفا، و بایاس) داشتند. این موضوع، منجر به این شده‌بود که تابع انعطاف‌پذیری و تطبق‌پذیری کم‌تری داشته‌باشد. همچنین،‌ شیب قسمت مثبت تابع نیز نادیده گرفته‌شده بود. از سوی دیگر، در این مقاله، روشی جدید برای مقداردهی اولیه به وزن‌ها معرفی شده تا جلوی اشباع تابع فعال‌سازی گرفته شود؛ در این روش، وزن‌های توابع بر اساس خروجی مورد انتظار آن‌ها مقداردهی می‌گردند تا از اشباع‌شدن توابع جلوگیری شود و سرعت همگرایی مدل افزایش یابد.

# سوال پنجم: شبکه‌های عصبی و انتشار رو به عقب

## ۱)

## ۲)

1. <https://en.wikipedia.org/wiki/Second_partial_derivative_test#Functions_of_many_variables> [↑](#footnote-ref-1)
2. <https://machinelearning.wtf/terms/internal-covariate-shift/> [↑](#footnote-ref-2)