



دانشگاه تهران

دانشکده علوم و فنون نوین

گزارش هفته چهارم و هفته پنجم

نام و نام خانوادگی	فاطمه چیت ساز
شماره دانشجویی	830402092
تاریخ ارسال گزارش	17 دی 1402

Contents

1.....	برسی week to strong learner
1.....	ترکیب SO و W2SG
2.....	برسی clip مدل open ai برای image Classification
3.....	برسی مقاله Let's Verify Step by Step
4.....	یکسری ایده از کنفرانس های ACL
5.....	برسی tiny gpt
5.....	برسی چندتا کار ایرانی: PersianLLaMA-Zero
6.....	برسی dall e
7.....	برسی lora
8.....	برسی Byte Pair Encoding

بررسی week to strong learner

این مقاله به بررسی چالش هم‌ترازی هوش مصنوعی (AI) می‌پردازد، به‌ویژه در مورد مدل‌های فوق هوش مصنوعی (superintelligent) که از توانایی‌های انسان فراتر رفته‌اند.

مسئله اصلی این است که چگونه می‌توانیم مدل‌های فوق هوش مصنوعی را طوری کنترل کنیم که با ارزش‌های انسانی همسو باشند. روش‌های سنتی هم‌ترازی مانند یادگیری تقویتی از بازخورد انسانی (RLHF) به توانایی انسان در نظارت بر رفتار مدل‌ها متکی هستند. اما برای مدل‌های فوق هوش مصنوعی، این کار دشوار یا غیرممکن خواهد بود.

راه‌حل پیشنهادی :

این مقاله یک راه‌حل جدید برای این مشکل ارائه می‌دهد: استفاده از تعمیم‌پذیری مدل‌های یادگیری عمیق برای کنترل مدل‌های قوی با ناظران ضعیف.

در این روش، از یک مدل ضعیف‌تر (با توانایی کمتر) برای نظارت بر یک مدل قوی‌تر (با توانایی بیشتر) استفاده می‌شود. مدل ضعیف می‌تواند به عنوان یک ناظر عمل کند و بازخوردهایی را به مدل قوی‌تر ارائه دهد تا به آن کمک کند تا رفتار مطلوب را یاد بگیرد.

نتایج

این مقاله نتایج امیدوارکننده‌ای را از آزمایش این روش بر روی طیف وسیعی از مدل‌های زبانی پیش‌آموزشی (pretrained language models) در وظایف پردازش زبان طبیعی (NLP)، شطرنج و مدل‌سازی پاداش ارائه می‌دهد.

این مقاله نشان می‌دهد که تعمیم‌پذیری مدل‌های یادگیری عمیق می‌تواند ابزاری قدرتمند برای هم‌ترازی مدل‌های فوق هوش مصنوعی باشد. با این حال، هنوز کارهای زیادی برای انجام باقی مانده است

<https://github.com/openai/weak-to-strong>

<https://cdn.openai.com/papers/weak-to-strong-generalization.pdf>

ترکیب W2SG و SO

سوال این‌ه چطور اعتماد کنیم <--- با ترکیب so w2sg

تصور کنید مدل شما در حوزه یادگیری تقویتی (Reinforcement Learning) استفاده می‌شود و شما قصد دارید آن را با دو مدل مهم یعنی "Weak-to-Strong Generalization (W2SG)" و "Scalable Oversight (SO)" ترکیب کنید.

:Weak-to-Strong Generalization (W2SG)

آموزش با داده‌های ضعیف به قوی: ابتدا مدل شما با داده‌های ضعیف (برچسب‌های نسبی ضعیف) آموزش می‌بیند.

هدایت به تصمیم‌گیری‌های قوی‌تر: با استفاده از داده‌های آموزشی ضعیف، مدل به تصمیم‌گیری‌های دقیق‌تر و قوی‌تر هدایت می‌شود.

:Scalable Oversight (SO)

آموزش با دستورات انسانی: حالا مدل شما با دستورات و تصمیمات انسانی (SO) آموزش می‌بیند. این دستورات ممکن است محدودیت‌ها، الزامات یا هدف‌های خاص برای عملکرد مدل باشند.

استفاده از ابزار W2SG برای ارزیابی تصمیمات: مدل حاصل از W2SG به عنوان یک نقدگر برای ارزیابی تصمیمات مدیریتی (Scalable Oversight) استفاده می‌شود.

حالا به طور خلاصه، شما از مدل W2SG برای افزایش دقت و قوت مدل خود استفاده کرده و همچنین از مدل SO برای هدایت مدل به سمت تصمیمات مدیریتی انسانی استفاده کرده‌اید. این ترکیب این دو مدل به شما این امکان را می‌دهد که هم دقت مدل را ارتقا دهید و هم از تصمیمات انسانی موثرتری برای هدایت مدل بهره‌مند شوید.

<https://aligned.substack.com/p/combining-w2sg-with-scalable-oversight>

بررسی مدل open ai برای image Classification

CLIP (Contrastive Language-Image Pre-training) یک مدل پیش‌آموزشی مبتنی بر Transformer است که برای دسته‌بندی تصاویر بدون نیاز به یادگیری (zero-shot) طراحی شده است. این مدل با استفاده از یک مجموعه داده عظیم از تصاویر و متن آموزش داده می‌شود و قادر است تصاویر را بر اساس توضیحات متنی دسته‌بندی کند.

در واقع اینطوریه که تو یک سری متن بهش میدی و یک تصویر و با یک احتمالی بهت می‌گه هر متن آیا در تصویر وجود داره یا نه

- زیبایی قضیه اینه که zero shot است

حالا open ai کجا ازش استفاده میکنه در dall e

در dall e برای ارزیابی عملکرد میاد از clip استفاده میکنه

<https://huggingface.co/openai/clip-vit-large-patch14>

برسی مقاله Let's Verify Step by Step

یکی از چالش‌های مهم در هوش مصنوعی، استدلال ریاضی درست و قابل اعتماد است. مدل‌های هوش مصنوعی اغلب به "توهمات" دچار می‌شوند و پاسخ‌های اشتباه، اما به ظاهر منطقی، ارائه می‌دهند. این موضوع می‌تواند خطرات بزرگی به همراه داشته باشد.

راه حل: نظارت گام به گام:

نظارت گام به گام، به جای فقط بررسی نتیجه نهایی، به تک تک مراحل استدلال مدل توجه می‌کند. این کار به کمک یک مدل بزرگ‌تر و قابل اعتماد انجام می‌شود که هر مرحله از استدلال مدل کوچک‌تر را بررسی و تایید می‌کند. این رویکرد چندین مزیت دارد:

ایمنی و دقت بالاتر: با بررسی هر مرحله، احتمال بروز توهمات و خطاهای بزرگ کاهش می‌یابد.

عملکرد بهتر: برخلاف انتظار، نظارت گام به گام حتی باعث بهبود عملکرد مدل در حل مسائل می‌شود.

کاربرد گسترده‌تر: با افزایش ایمنی و دقت، مدل‌های هوش مصنوعی ریاضی می‌توانند با اطمینان بیشتری در موارد حساس و حیاتی مورد استفاده قرار گیرند.

جزئیات رویکرد:

مدل پایه: از مدل GPT-4 با تنظیمات خاص برای ریاضیات استفاده می‌شود.

مجموعه داده PRM800K: این مجموعه داده شامل 800 هزار برچسب گام به گام برای 75 هزار راه حل و 12 هزار مسئله ریاضی است.

جستجوی بهترین N: برای یافتن بهترین راه حل، مدل چندین گزینه را بررسی و بهترین را انتخاب می‌کند.

یکسری ایده از کنفرانس های ACL

چند تا چیز در اسن کنفرانس ها بهش تاکید شده بود یک اینکه مثلا ما یک نالج گراف داشته باشیم و مدل ما بیاد از آن اطلاعات مفیدی استخراج کنه

یا اینکه حتی اطلاعات رو بدیم به مدل بیاد خودش نالج گراف رو بکشه

یا اینکه نالج گراف رو تبدیل کنه به یک سری جملات و عبارات منطقی

قضیه دیگ اینه ک میشه مثلا به جای اینکه کل مدل را تغییر بدی فقط لایه اخر رو تغییر بدی خب قطعا این بار پردازشیش کمتره مثلا بیایم یک مدل رو فقط لایه اخرشو جوری تغییر بدیم که به احساسات اهمیت بیشتری بده

کارای جالبی هم پیشنهاد شد برای این مثلا ایجاد جملات مثبت اندیشی و اینا

و کلا کارای تحلیل احساسات و اینا

قضیه بعدی اینه که میشه ما حجم llm رو کم کنیم یک ارزیابی بدست بیاریم بعد بگیم اقا ما با این حجم کم به این ارزیابی رسیدیم

کارای جالب دیگه این بیایم بریم توکگل و لاما رو fine tuning کنیم

یا مثلا چندتا از state of art رو باهم ترکیب کنیم که یک application بسازیم

مثلا یک کارایی مثل اینکه بیایم نالج گرافی از ادمای سیاسی بکشیم و بعد ببینیم که قضیه چیه؟؟

یا مثلا ما خیلی کارای ریاضی داریم که کانفیگش رو میشه با هوش انجام داد

some finetuning with llama

https://colab.research.google.com/github/MuhammadMoinFaisal/LargeLanguageModelsProjects/blob/main/Fine_Tune_Llama2_Generating_data_OpenAI/Fine_Tune_Llama_2_by_generating_data_from_the_LLM_OpenAI.ipynb#scrollTo=5eAvh3nsA36t

بررسی tiny gpt

TinyGPT-V یک مدل زبانی چندوجهی (Multimodal) جدید است که با استفاده از تکنیک‌های نوآورانه، کارایی و عملکرد را به طور همزمان بهینه می‌کند

چیزای فان:

کارایی بالا: TinyGPT-V تنها به 24 گیگابایت حافظه GPU برای آموزش و 8 گیگابایت حافظه GPU یا CPU برای استنتاج نیاز دارد. این امر آن را به گزینه‌ای ایده‌آل برای دستگاه‌های کم‌توان تبدیل می‌کند. عملکرد قوی: TinyGPT-V با وجود پارامترهای کوچک، عملکردی قابل مقایسه با مدل‌های زبانی بزرگ‌تر ارائه می‌دهد.

قابلیت چندوجهی: TinyGPT-V می‌تواند وظایف مختلفی را در حوزه‌های مختلف انجام دهد.

تکنیک‌های جالب :

LoRA: این تکنیک به مدل زبان اجازه می‌دهد تا با استفاده از یک شبکه عصبی کوچک، پارامترهای خود را به طور کارآمد تنظیم کند. این امر به طور قابل توجهی نیاز به حافظه و قدرت پردازش را کاهش می‌دهد. Q-Former: این تکنیک به رمزگذار تصویری کمک می‌کند تا اطلاعات بصری را به طور دقیق‌تر با مدل زبان همسو کند. این امر منجر به بهبود عملکرد در وظایف مرتبط با بینایی رایانه می‌شود.

<https://arxiv.org/abs/2312.16862v1>

بررسی چندتا کار ایرانی: PersianLLaMA-Zero

آموزش از ابتدا (PersianLLaMA-Zero):

در این حالت، مدل PersianLLaMA از ابتدا با استفاده از دو منبع اصلی، یعنی مجموعه داده OSCAR و ویکی‌پدیا فارسی، آموزش داده شده است. مجموعه داده OSCAR شامل ۲۳ میلیون متن فارسی از وب می‌باشد، و مجموعه داده ویکی‌پدیا فارسی نیز شامل ۲.۴ میلیون متن فارسی از ویکی‌پدیا استفاده کرده است. برای آموزش PersianLLaMA از ابزارهای DeepSpeed و روش TencentPretrain استفاده شده است.

آموزش با استفاده از روش LoRA (Low-Rank Adaptation):

در این روش، مدل LLaMA-13B انگلیسی به عنوان مدل پایه مورد استفاده قرار گرفته و از تکنیک LoRA برای آموزش PersianLLaMA استفاده شده است. روش LoRA به مدل این امکان را می‌دهد که با استفاده از حجم کمی از داده‌های فارسی، دانش مدل انگلیسی LLaMA-13B را به زبان فارسی انتقال دهد.

مزایای PersianLLaMA:

1 توانایی انجام وظایف مختلف: PersianLLaMA می‌تواند وظایف مختلفی مانند تولید متن، ترجمه زبان، پاسخ به سوالات و نوشتن انواع مختلف محتوای خلاقانه را انجام دهد.

عملکرد قوی: PersianLLaMA در مقایسه با سایر مدل‌های زبانی فارسی، عملکرد قوی‌تری دارد.

قابلیت دسترسی: PersianLLaMA به صورت رایگان در دسترس عموم قرار دارد.

<https://arxiv.org/ftp/arxiv/papers/2312/2312.15713.pdf>

بررسی dall e

Dall-E یک مدل مولد تصویر از متن است که توسط OpenAI توسعه یافته است. این مدل قادر است تصاویر را از توضیحات متنی کوتاه تولید کند. Dall-E با ترکیب دو مدل Transformer و VQ-VAE (Vector Quantized Variational Autoencoder) کار می‌کند.

نحوه عملکرد:

رمزگذاری متن: متن به توکن‌های BPE (Byte Pair Encoding) تبدیل می‌شود. سپس، توکن‌های موقعیتی و پدینگ به توکن‌ها اضافه می‌شوند.

رمزگذاری تصویر: تصویر به توکن‌های سی و دو در سی و دو با استفاده از VQ-VAE تبدیل می‌شود. سپس، توکن‌های پدینگ به توکن‌ها اضافه می‌شوند.

ترکیب متن و تصویر: توکن‌های متن و تصویر به یک مدل Transformer داده می‌شوند.

تولید تصویر: مدل Transformer توکن‌های تصویر نهایی را تولید می‌کند.

جزئیات:

مدل Transformer: مدل Transformer از معماری مشابه GPT-3 استفاده می‌کند.

VQ-VAE: VQ-VAE یک مدل یادگیری عمیق برای تبدیل تصاویر به توکن‌های برداری است.

توکن‌های BPE: توکن‌های BPE توکن‌هایی هستند که با استفاده از الگوریتم BPE از متن استخراج می‌شوند.

توکن‌های موقعیتی: توکن‌های موقعیتی توکن‌هایی هستند که به مدل Transformer اطلاعات مربوط به موقعیت هر توکن در جمله را می‌دهند.

توکن‌های پدینگ: توکن‌های پدینگ توکن‌هایی هستند که برای پر کردن فضای خالی در توکن‌های متن و تصویر استفاده می‌شوند.

تابع زیان: از یک تابع زیان آن‌تروپی متقابل برای تصاویر استفاده می‌کند.

https://github.com/lucidrains/DALLE-pytorch/blob/main/dalle_pytorch/dalle_pytorch.py

بررسی lora

الگوریتم لورای (LoRA) یک تکنیک جدید برای آموزش مدل‌های زبانی بزرگ (LLM) است که توسط مایکروسافت توسعه یافته است. این الگوریتم با هدف کاهش ابعاد ماتریس وزن مدل‌های زبانی بزرگ و بهبود کارایی آنها ارائه شده است.

نحوه عملکرد:

الگوریتم لورای بر اساس ایده حذف ستون‌های خطی وابسته از ماتریس وزن مدل زبانی است. این کار با استفاده از یک ماتریس کم‌رتبه انجام می‌شود که به آن "ماتریس لورا" می‌گویند. ماتریس لورا به مدل اجازه می‌دهد تا با استفاده از تعداد کمتری پارامتر، به همان عملکرد مدل اصلی دست یابد.

مزایا:

کاهش ابعاد: الگوریتم لورای می‌تواند ابعاد ماتریس وزن مدل‌های زبانی بزرگ را تا 90٪ کاهش دهد.

بهبود کارایی: کاهش ابعاد ماتریس وزن منجر به بهبود کارایی مدل در زمان آموزش و استنتاج می‌شود.

بهبود عملکرد: در برخی موارد، الگوریتم لورای می‌تواند عملکرد مدل زبانی را نیز بهبود بخشد.

معایب:

پیچیدگی: الگوریتم لورای از نظر مفهومی پیچیده‌تر از روش‌های سنتی آموزش مدل‌های زبانی است.

نیاز به داده: الگوریتم لورای برای آموزش به مقدار زیادی داده نیاز دارد.

کاربردها:

آموزش مدل‌های زبانی بزرگ: الگوریتم لورای می‌تواند برای آموزش مدل‌های زبانی بزرگ با کارایی بیشتر مورد استفاده قرار گیرد.

استقرار مدل‌های زبانی بزرگ: الگوریتم لورای می‌تواند به استقرار مدل‌های زبانی بزرگ در دستگاه‌های کم‌توان کمک کند.

جزئیات فنی:

ماتریس لورا: ماتریس لورا یک ماتریس کم‌رتبه است که برای کاهش ابعاد ماتریس وزن مدل زبانی استفاده می‌شود.

حذف ستون‌های خطی وابسته: الگوریتم لورای ستون‌های خطی وابسته از ماتریس وزن مدل زبانی را با استفاده از ماتریس لورا حذف می‌کند.

تابع زیان: الگوریتم لورای از یک تابع زیان مبتنی بر آنتروپی متقابل برای آموزش مدل زبانی استفاده می‌کند.

<https://arxiv.org/abs/2106.09685>

بررسی Byte Pair Encoding

Byte Pair Encoding یا BPE یک روش هوشمندانه برای تقسیم کلمات به واحدهای کوچک‌تر است که در پردازش زبان طبیعی استفاده می‌شود. این روش به ویژه برای مدل‌های زبانی بزرگ، که با حجم زیادی از متن آموزش می‌بینند، مفید است.

نحوه عملکرد BPE:

تقسیم کلمات اولیه: ابتدا، تمام کلمات متن به واحدهای تک حرفی (با استفاده از حروف الفبا یا بایت‌ها) تقسیم می‌شوند.

پیدا کردن جفت‌های پرتکرار: الگوریتم BPE به دنبال جفت حروف یا بایت‌هایی می‌گردد که بیشترین تکرار را در متن دارند.

ادغام جفت‌های پرتکرار: جفت‌های پرتکرار با یک نماد جدید جایگزین می‌شوند.

تکرار: مراحل ۲ و ۳ به تعداد مشخصی (معمولاً بین ۵۰ هزار تا ۵۰ میلیون بار) تکرار می‌شوند تا تعداد واحدهای مختلف به اندازه دلخواه کاهش یابد.

مزایا:

واژه‌نامه کوچک‌تر: BPE می‌تواند اندازه واژه‌نامه را تا حد زیادی کاهش دهد، چرا که به جای ذخیره تک تک کلمات، فقط واحدهای کوچک‌تر را ذخیره می‌کند.

بهبود کارایی: کاهش اندازه واژه‌نامه منجر به بهبود کارایی مدل‌های زبانی در زمان آموزش و استنتاج می‌شود.

انعطاف‌پذیری: BPE می‌تواند با هر زبانی سازگار شود، زیرا به جای حروف الفبا، بر اساس بایت‌ها کار می‌کند. مقابله با کلمات ناشناخته: BPE می‌تواند کلماتی را که در زمان آموزش ندیده است، به خوبی مدیریت کند، زیرا قادر است آنها را به واحدهای کوچک‌تر تجزیه کند.

مثال کاربردی:

GPT-2 و RoBERTa: مدل‌های زبانی GPT-2 و RoBERTa از BPE در سطح بایت استفاده می‌کنند. این کار باعث می‌شود که آنها بتوانند با هر زبانی کار کنند و با کلمات ناشناخته به خوبی مواجه شوند.