

بسم الله الرحمن الرحيم



دانشگاه شهید بهشتی کرمان

دانشکده فنی و مهندسی  
بخش مهندسی کامپیوتر

پایان نامه تحصیلی برای دریافت درجه کارشناسی ارشد

رشته مهندسی کامپیوتر گرایش هوش مصنوعی

---

تشخیص قدرتمند بدافزارهای اندروید با استفاده از شبکه‌های عصبی  
ترنسفورمر

---

مؤلف:

علیرضا ایرانمنش

استاد راهنما:

دکتر حمید میروزی

اردیبهشت ۱۴۰۴

## بـنام خدا

### مـموراـخـلـقـ پـوـشـ

با احـسـانـ اـنـدـهـ اـیـ جـانـ وـ اـعـتـدـ اـلـ اـخـلـقـ اـیـ بـنـامـ عـالـ مـصـرـفـ دـاـستـ وـ اوـ هـوـلـهـ نـافـرـ اـعـالـ مـاـسـتـ بـهـ مـطـورـ فـاجـمـ شـایـرـتـیـ پـوـشـ بـهـ اـسـلـ،ـ تـوـیدـ اـنـشـ جـعـیدـ وـ بـسـارـیـ نـزـکـلـیـ بـشـرـمـاـ اـنـجـیـانـ وـ اـعـتـادـ بـیـاتـ عـلـیـ اـلـخـاـهـ دـوـشـ بـلـخـادـ بـهـ کـشـرـ:

- تمامـ تـلـاشـ خـودـ رـاـیـ کـشـتـ وـ خـلـقـ تـحـیـتـ بـکـارـ خـانـیـمـ بـتـ وـ اـزـ کـوـنـ جـلـ وـ خـرـیـتـ دـفـایـتـ بـهـ عـلـیـ پـرـسـیـزـ کـشـمـ.
- حقـقـ پـوـرـشـکـانـ،ـ پـوـرـمـیـکـانـ (ـاـنـانـ،ـ جـیـانـ،ـ بـنـاتـ وـ آـشـیـاءـ)،ـ سـانـانـ بـهـ سـایـرـ صـاحـبـانـ حقـقـ رـاـبـرـیـتـ مـیـ شـایـمـ وـ «ـحـظـ آـنـ مـیـ کـوـشـمـ».
- بـاـلـکـیـتـ اـدـیـ وـ مـمـونـیـ آـثـرـشـوـشـیـ اـنـجـ مـیـ نـسـیـمـ،ـ بـرـایـ اـخـبـرـشـوـشـیـ اـسـلـ (ـاـنـامـ وـ زـنـیدـ وـ اـزـ سـرـقـتـ عـلـیـ وـ اـرـجـاعـ نـهـاـبـ اـبـتـابـ کـشـمـ).
- خـسـنـ پـایـندـیـ بـهـ اـنـصـافـ وـ اـبـتـابـ اـزـ کـوـنـ تـبـیـنـ تـحـسـبـ وـ کـیـنـهـیـ نـهـایـتـ بـهـ پـوـشـشـ،ـ رـیـانـیـ تـمـادـ اـخـادـ خـانـیـمـ کـردـ.
- خـسـنـ اـنـاسـ دـارـیـ،ـ اـزـ سـایـجـ وـ اـنـخـانـتـ اـقـسـادـیـ،ـ اـنـسـانـ وـ فـنـ مـوـجـودـ،ـ اـسـخـادـ وـ دـوـرـلـهـ خـانـیـمـ کـردـ.
- اـزـ اـنـمـاـرـ غـیرـ اـخـلـقـیـ اـنـجـ پـوـشـ،ـ نـهـیـ اـنـمـاـرـ مـوـازـیـ،ـ بـهـ شـانـ وـ چـنـکـدـ کـهـ اـیـ پـرـسـیـزـ کـشـمـ.
- اـسـلـ مـرـبـدـ بـوـنـ وـ رـاـلـدـارـیـ رـاـحـوـرـ تـمـ نـهـایـتـ بـهـ پـوـشـشـ خـوـقـرـمـ دـیـمـ.
- دـهـدـ نـهـایـتـ بـهـ پـوـشـشـ بـلـانـجـ مـلـ تـبـجـدـ کـرـدـ وـ بـرـایـ تـحـقـیـقـ آـنـ مـیـ کـوـشـمـ.
- خـوـشـ رـاـلـزـمـ بـهـ رـیـاضـتـ کـیـ بـیـخـدـهـیـ عـلـیـ رـشـخـوـدـ،ـ قـوـنـینـ وـ مـرـتـرـاتـ بـیـاسـتـهـیـ حـرـفـاـیـ،ـ سـانـانـ،ـ دـوـتـیـ وـ رـاـبـرـهـدـهـیـ فـیـ دـهـدـ مـرـاـلـ پـوـشـشـ مـیـ دـانـمـ.
- رـیـاتـ اـصـلـ اـخـلـقـ دـوـشـ بـرـاـهـمـیـ فـرـکـلـیـ وـ اـنـسـمـ وـ بـهـ مـطـبـرـانـگـیـ اـیـ فـرـنـکـ بـهـ تـوـجـ وـ اـلـهـ آـنـ دـجـاسـ اـنـامـ مـیـ وـزـیـمـ.



دانشگاه شید بآهنر کرمان

### تعهدنامه

اینجانب علیرضا ایرانمنش به شماره دانشجویی ۱۵۵۰۱۵۰۱۴۰ دانشجوی مقطع کارشناسی ارشد رشته مهندسی کامپیوتر-هوش مصنوعی دانشکده فنی مهندسی دانشگاه شهید باهنر کرمان نویسنده پایاننامه با عنوان « تشخیص

قدرتمند بدافزارهای اندروید با استفاده از شبکه‌های عصبی ترانسفورمر» تحت راهنمایی دکتر حمید میروزیری تأیید

می‌کنم که این پایاننامه نتیجه پژوهش اینجانب می‌باشد و در عین حال که موضوع آن تکراری نیست، در صورت

استفاده از منابع دیگران، نشانی دقیق و مشخصات کامل آن درج شده است. همچنین موارد زیر را نیز تعهد می‌کنم:

۱- برای انتشار تمام یا قسمتی از داده‌ها یا دستاوردهای خود در مجامع و رسانه‌های علمی اعم از همایش‌ها و مجلات داخلی و خارجی به صورت مقاله، کتاب، ثبت اختراع و ... به صورت مکتوب یا غیرمکتوب، با کسب مجوز از دانشگاه شهید باهنر کرمان و استاد(ان) راهنما اقدام نمایم.

۲- از درج اسمی افراد خارج از کمیته پایاننامه در جمع نویسنده‌گان مقاله‌های مستخرج از پایاننامه، بدون مجوز استاد(ان) راهنما اجتناب نمایم و اسمی افراد کمیته پایان نامه را در جمع نویسنده‌گان مقاله درج نمایم.

۳- از درج نشانی یا وابستگی کاری (affiliation) نویسنده‌گان سازمان‌های دیگر (غیر از دانشگاه شهید باهنر کرمان) در مقاله‌های مستخرج از پایان‌نامه بدون تأیید استاد(دان) راهنما اجتناب نمایم.<sup>۱</sup>

۴- کلیه ضوابط و اصول اخلاقی مربوط به استفاده از موجودات زنده یا بافت‌های آنها را برای انجام پایان‌نامه رعایت نمایم.

۵- در صورت اثبات تخلف (در هر زمان) مدرک تحصیلی صادر شده توسط دانشگاه شهید باهنر کرمان از درجه اعتبار ساقط و اینجانب هیچ‌گونه ادعایی نخواهم داشت.

کلیه حقوق مادی و معنوی این اثر (مقالات مستخرج، برنامه‌های رایانه‌ای، نرم افزارها و تجهیزات ساخته شده) مطابق با آئین‌نامه مالکیت فکری، متعلق به دانشگاه شهید باهنر کرمان است و بدون اخذ اجازه کتبی از دانشگاه قابل واگذاری به شخص ثالث نیست. همچنین استفاده از اطلاعات و نتایج این پایان‌نامه بدون ذکر مرجع مجاز نمی‌باشد. چنانچه مبادرت به عملی خلاف این تعهدنامه محرز گردد، دانشگاه شهید باهنر کرمان در هر زمان و به هر نحو مقتضی حق هرگونه اقدام قانونی را در استیفای حقوق خود دارد.

تاریخ و امضاء:  
علیرضا ایرانمنش  
۱۴۰۴ اردیبهشت

<sup>۱</sup> تنها آدرس مورد قبول برای دانشگاه به این صورت می‌باشد:

Shahid Bahonar University of Kerman, Kerman, Iran.

نام و آدرس واحدهای دانشگاه در تولیدات علمی محققان دانشگاه به تشخیص بخش و دانشکده به شرح زیر می‌باشد:

Department of Computer, Faculty of Engineering Shahid Bahonar University of Kerman, Kerman, Iran.

آدرس صحیح جهت درج در مقالات و سایر تولیدات علمی فارسی:  
گروه (بخش) کامپیوتر، دانشکده فنی مهندسی، دانشگاه شهید باهنر کرمان، کرمان، ایران.

## تقدیم به:

«این مجموعه را با کمال افتخار و احترام تقدیم می‌کنم به:  
روح بلند بنیانگذار دانشگاه، مرحوم افضلی پور و همسر گرامیشان بانو فاخره صبا.  
آنان که عاشقانه سوختند تا گرمابخش وجود ما و روشنگر راهمان باشند...  
به پاس تعبیر عظیم و انسانی‌شان از کلمه ایثار.  
به پاس عاطفه سرشار و گرمای امیدبخش وجودشان که در این سرددترین روزگاران بهترین پشتیبان ماست.  
به پاس قلب بزرگشان، و به پاس محبت‌های بی دریغشان که هرگز فروکش نمی‌کند»

## تشکر و قدردانی:

با سپاس از خداوند بزرگ که به من توانایی و انگیزه برای پیمودن این مسیر علمی را عطا نمود. این پایان نامه حاصل تلاش و کوشش های فراوان است و بدون حمایت و راهنمایی های ارزشمند افراد بسیاری به ثمر نمی نشست.

به مصداق شعر «به یاد کسی که در این راه بود، به یاد کسی که در این راه رفت»، شایسته می دانم مراتب سپاس و قدردانی صمیمانه خود را تقدیم نمایم به استاد فرهیخته و فرزانه، جناب آقای دکتر حمید میروزیری، که با دانش و تجربه‌ی خود همواره راهنمای من بودند و با صبر و شکیابی به سوالات و ابهاماتم پاسخ دادند، صمیمانه تشکر می کنم.

همچنین از دوست عزیزم، محمدحسین شبانی، که با حمایت های بی دریغ و تشویق های همیشگی اش، انگیزه و انرژی مضاعفی به من بخشید، قدردانی می نمایم.

در پایان، از خانواده‌ی عزیزم که با عشق و محبت بی پایان خود همواره پشتیبان من بودند و در تمامی مراحل این مسیر پرچالش، همراه و همدم من بودند، بی نهایت سپاسگزارم.

## چکیده:

تشخیص بدافزارهای اندرویدی با افزایش روزافرون تهدیدات سایبری، یکی از چالش‌های اصلی در حوزه امنیت اطلاعات به شمار می‌رود. روش‌های سنتی، بهویژه آن‌هایی که صرفاً بر تحلیل ویژگی‌های تک‌وجهی تکیه دارند، اغلب با محدودیت‌هایی نظری ناتوانی در پردازش داده‌های پیچیده چندوجهی و تعیین‌پذیری ضعیف در برابر تهدیدات جدید مواجه‌اند. این کاستی‌ها، نیاز به توسعه رویکردهای نوین و کارآمد را بیش از پیش آشکار می‌سازد. این پژوهش مدلی چندوجهی با عنوان تبدیل‌گر چندوجهی مبتنی بر جاسازی گراف دینامیک با توجه پویا (MAGNET) توسعه داد که از ترکیب داده‌های جدولی، گراف و ترتیبی، نظری توالی فراخوانی‌های API، برای شناسایی بدافزارهای اندرویدی بهره برد. هدف اصلی، بهبود دقت و پایداری تشخیص با استفاده از معماری پیشرفته مبتنی بر یادگیری عمیق و ترانسفورمر بود. روش تحقیق شامل بهینه‌سازی هایپرپارامترها با الگوریتم‌های پیشرفته مانند PIRATES و Optuna، آموزش مدل با مجموعه داده‌ای شامل ۴۶۴۱ نمونه آموزشی و ۱۴۵۱ نمونه آزمایشی، و اعتبارسنجی متقطع ۵-تایی شد. ویژگی‌های مورد استفاده شامل ویژگی‌های ایستا مانند مجوزها، فراخوانی‌های API، مقاصد، و نام‌های مؤلفه و ویژگی‌های پویا مانند فعالیت شبکه و دسترسی به فایل‌ها بود. داده‌ها به صورت بردارهای عددی باینزی یا نرمال‌سازی شده بودند. ابعاد ویژگی‌ها پس از پیش‌پردازش به ۴۳۰ ویژگی تنظیم شد. ابزارهای مورد استفاده شامل کتابخانه‌های یادگیری عمیق مانند PyTorch، تکنیک‌های پیش‌پردازش داده‌ها نظری استاندارد سازی و نرمال‌سازی، و ساختارهای داده‌ای گرافی بودند. مواد اولیه شامل داده‌های واقعی از رفتار اپلیکیشن‌های اندرویدی، شامل ویژگی‌های ایستا و پویا، بود که با دقت آماده‌سازی شدند. نتایج نشان داد که مدل پیشنهادی عملکردی برجسته با دقت بالا، پایداری قابل توجه و قابلیت تعیین‌پذیری خوب ارائه کرد و نسبت به روش‌های پیشین بهبود قابل ملاحظه‌ای داشت. این دستاوردها پتانسیل کاربرد مدل در سیستم‌های امنیتی واقعی را برجسته ساخت. پیشنهاد می‌شود تحقیقات آینده بر افزایش حجم داده‌ها، ادغام روش‌های خودناظارتی پیشرفته، آزمایش مدل در محیط‌های متنوع‌تر و بهینه‌سازی زمان اجرای آن متمرکز شوند تا کارایی مدل در سناریوهای پیچیده‌تر و واقعی‌تر ارتقا یابد. همچنین، بررسی تأثیر ترکیب داده‌های جدیدتر و توسعه الگوریتم‌های مقاوم در برابر حملات مخرب می‌تواند مسیرهای نوینی برای تحقیقات بعدی گشوده کند. این پژوهش، گامی مؤثر در راستای ارتقای سیستم‌های تشخیص خودکار بدافزارها برداشت و پایه‌ای محکم برای توسعه راه حل‌های امنیتی پیشرفته‌تر فراهم آورد.

**واژگان کلیدی:** تشخیص بدافزار، ترانسفومر، یادگیری عمیق، داده‌های چندوجهی، امنیت اندروید، بدافزار اندروید.

## فهرست مطالب

صفحه

عنوان

۳	کلیات پژوهش	۱
۴	مقدمه و بیان مسئله	۱-۱
۵	روش‌های تشخیص بدافزار	۱-۱-۱
۵	مجموعه داده‌های مربوطه	۲-۱-۱
۵	ضرورت تحقیق و اهداف	۲-۱
۶	سازماندهی پایان نامه	۳-۱
۸	پیشینه تحقیق و مفاهیم پایه	۲
۹	مقدمه	۱-۲
۹	بررسی مدل‌های زبانی بزرگ	۲-۲
۱۰	تاریخچه و تکامل مدل‌ها	۱-۲-۲
۱۱	معماری‌ها و کاربردهای اصلی	۲-۲-۲
۱۳	مدل بزرگ زبانی Mistral	۳-۲-۲
۱۴	مهندسی اعلان	۳-۲
۱۴	روش‌های دستی در مهندسی اعلان	۴-۲
۱۶	یادگیری درون متنی	۱-۴-۲
۲۰	روش زنجیره تفکر	۲-۴-۲
۲۰	روش استدلال بدون دیدن نمونه آموزشی	۳-۴-۲
۲۲	روش برنامه تفکر	۴-۴-۲
۲۲	روش بهینه سازی با اعلان	۵-۴-۲
۲۴	روش برنامه‌ریزی و حل	۶-۴-۲
۲۶	بهینه‌سازی خودکار اعلان‌ها	۵-۲
۲۶	روش زنجیره تفکر خودکار	۱-۵-۲
۲۷	روش مهندس اعلان خودکار	۲-۵-۲
۲۸	روش مولد اعلان	۳-۵-۲
۳۰	جمع‌بندی مباحث ارائه شده	۶-۲

۳۲	<b>روش های پیشنهادی</b>	۳
۳۳	مقدمه . . . . .	۱-۳
۳۵	روش مولد اعلان ساده . . . . .	۲-۳
۳۶	نمونه گیری . . . . .	۱-۲-۳
۳۷	انتخاب . . . . .	۲-۲-۳
۴۱	ارزیابی . . . . .	۳-۲-۳
۴۳	<b>نتایج و بحث</b>	۴
۴۴	مجموعه داده های مورد استفاده . . . . .	۱-۴
۴۴	متغیرهای روش مولد اعلان ساده . . . . .	۲-۴
۴۵	روش های مرجع . . . . .	۳-۴
۴۵	نمایش دو بعدی اعلان ها . . . . .	۴-۴
۴۶	نتایج . . . . .	۵-۴
۴۷	سریار محاسباتی . . . . .	۶-۴
۴۸	خروجی ها . . . . .	۷-۴
۵۲	<b>نتیجه گیری و پیشنهادات آتی</b>	۵
۵۳	نتیجه گیری . . . . .	۱-۵
۵۳	پیشنهادات آتی . . . . .	۲-۵
۵۹	<b>پیوست</b>	
۶۱	<b>توضیحات تکمیلی</b>	
۶۱	مقدمه . . . . .	
۶۱	اعلان های دستوری برای نمونه گیری روش مولد اعلان ساده . . . . .	
۶۶	ارزیابی . . . . .	
۶۹	سایر روش ها . . . . .	

## فهرست جداول

صفحه

عنوان

---

جدول ۳ - ۱ توصیف مسئله برای مجموعه داده های مختلف . . . . . ۳۷

جدول ۴ - ۱ مقایسه دقیق روش مولد اعلان ساده با سایر روش های موجود . . . . . ۴۴

جدول ۱ اعلان های دستوری برای سایر روش ها جهت مقایسه نتایج . . . . . ۶۹

## فهرست تصاویر

عنوان

صفحه

شکل ۲-۱	دیاگرام معماری ترانسفورمر	۱۲
شکل ۲-۲	مثالی از یادگیری بدون نمونه در یادگیری درون متنی	۱۷
شکل ۲-۳	مثالی از روش زنجیره تفکر برای حل یک سوال از دیتابست GSM8K	۲۱
شکل ۲-۴	مقایسه روش استدلال بدون دیدن نمونه آموزشی و روش زنجیره تفکر	۲۱
شکل ۲-۵	مقایسه روش برنامه تفکر و روش زنجیره تفکر	۲۳
شکل ۲-۶	دیاگرام روش بهینه سازی با اعلان	۲۴
شکل ۲-۷	یک مثال از روش برنامه ریزی و حل	۲۶
شکل ۲-۸	دیاگرام روش auto-CoT	۲۸
شکل ۲-۹	دیاگرام روش مولد اعلان	۳۰
شکل ۳-۱	مقایسه پیچیدگی محاسباتی روش مولد اعلان و روش مولد اعلان ساده	۳۴
شکل ۳-۲	دیاگرام روش مولد اعلان ساده	۳۵
شکل ۳-۳	دیاگرام مرحله ارزیابی روش مولد اعلان ساده	۴۲
شکل ۴-۱	نمایش دو بعدی بردار اعلان ها برای ارزیابی انتخاب در روش مولد اعلان ساده	۴۶

## فهرست الگوریتم‌ها

---

عنوان	صفحة
الگوریتم ۱ - ۳ مولد اعلان ساده . . . . .	٣٦

date, = date booktitle, = booktitle title, = title author, = author @inbookID,  
OPTe- editora, = OPTeditora editor, = OPTeditor bookauthor, = OPTbookauthor  
OPTanno- translator, = OPTtranslator editorc, = OPTeditorc editorb, = ditorb  
in- = OPTintroduction commentator, = OPTcommentator annotator, = tator  
= OPTsubtitle afterword, = OPTafterword foreword, = OPTforeword trduction,  
OPTmainsubtitle maintitle, = OPTmaintitle titleaddon, = OPTtitleaddon subtitle,  
book- = OPTbooksubtitle maintitleaddon, = OPTmaintitleaddon mainsubtitle, =  
OP- language, = OPTlanguage booktitleaddon, = OPTbooktitleaddon subtitle,  
OPTedition part, = OPTpart volume, = OPTvolume origlanguage, = Toriglanguage  
number, = OPTnumber series, = OPTseries volumes, = OPTvolumes edition, =  
OPTisbn location, = OPTlocation publisher, = OPTpublisher note, = OPTnote  
addendum, = OPTaddendum pages, = OPTpages chapter, = OPTchapter isbn, =  
= OPTeprintclass eprint, = OPTeprint doi, = OPTdoi pubstate, = OPTpubstate  
urldate, = OPTurldate url, = OPTurl eprinttype, = OPTeprinttype eprintclass,

akefnintext[ \ ]mmakefnmark\

# فصل اول:

# کلیات پژوهش

## ۱-۱ مقدمه و بیان مسئله

در سال‌های اخیر، گسترش تلفن‌های همراه و بهویژه سیستم عامل اندروید<sup>۱</sup>، موجب افزایش وابستگی کاربران به این ابزارها شده است. این دستگاه‌ها نه تنها در زندگی روزمره، بلکه در حوزه‌های تجاری و نظامی نیز نقش مهمی ایفا می‌کنند. با این حال، محبوبیت و فرآگیری اندروید، آن را به هدفی جذاب برای حملات بدافزاری<sup>۲</sup> تبدیل کرده است. عرضه نرم‌افزارهای غیرمعتبر و تهدیداتی مانند ویروس‌ها و بدافزارها، امنیت کاربران را به خطر انداخته است. مطالعات اخیر نشان می‌دهد که بیش از ۷۰ درصد دستگاه‌های هوشمند از سیستم عامل اندروید استفاده می‌کنند و این امر باعث شده است که این پلتفرم به هدف اصلی حملات امنیتی تبدیل شود [۱]. با وجود پیشرفت‌های قابل توجه در روش‌های تشخیص بدافزار، همچنان چالش‌های جدی در شناسایی بدافزارهای جدید و پیچیده وجود دارد.

در ابتدا، روش‌های سنتی مبتنی بر تحلیل مجوزها<sup>۳</sup> و بازکردن فایل‌ها مورد استفاده قرار می‌گرفتند که به دلیل دقت پایین و ضعف در شناسایی بدافزارهای پیچیده، محدودیت‌هایی داشتند. پژوهش‌های اخیر نشان داده‌اند که روش‌های مبتنی بر یادگیری ماشین<sup>۴</sup> و یادگیری عمیق<sup>۵</sup> می‌توانند عملکرد بهتری در تشخیص بدافزارها داشته باشند [۲]. با این حال، همچنان چالش‌های مهمی در زمینه تفسیرپذیری مدل‌ها<sup>۶</sup> و قابلیت تعمیم‌پذیری<sup>۷</sup> وجود دارد. این چالش‌ها به ویژه در مواجهه با بدافزارهای جدید و ناشناخته (Zero-Day)<sup>۸</sup> بیشتر خود را نشان می‌دهند.

مدل MAGNET<sup>۹</sup> که در این پژوهش معرفی شده است، با بهره‌گیری از معماری ترانسفورمر<sup>۱۰</sup> چندوجهی و ترکیب داده‌های جدولی، گراف و توالی، تلاش می‌کند تا این چالش‌ها را برطرف کند. این مدل با استفاده از مکانیزم‌های توجه پویا<sup>۱۱</sup> و تحلیل همزمان داده‌های مختلف، قادر به تشخیص دقیق‌تر بدافزارها خواهد بود. نتایج اولیه نشان می‌دهد که این رویکرد می‌تواند دقت تشخیص را تا ۹۸٪ افزایش دهد و قابلیت تعمیم‌پذیری مناسبی در مواجهه با بدافزارهای جدید داشته باشد.

<sup>1</sup>Android

<sup>2</sup>Malware

<sup>3</sup>Permissions

<sup>4</sup>Machine Learning

<sup>5</sup>Deep Learning

<sup>6</sup>Model Interpretability

<sup>7</sup>Generalization

<sup>8</sup>Zero-Day

<sup>9</sup>MAGNET(Multi-Modal Analysis for Graph and Network Threat Detection)

<sup>10</sup>Transformer

<sup>11</sup>Attention Mechanism

## ۱-۱-۱ روش‌های تشخیص بدافزار

تشخیص بدافزارهای اندرویدی به دو روش کلی پویا<sup>۱</sup> و ایستا<sup>۲</sup> انجام می‌شود. در روش پویا، رفتار اپلیکیشن در زمان اجرا مانند مصرف باتری، پردازنده یا ترافیک شبکه بررسی می‌شود تا الگوهای غیرعادی شناسایی گردد. این روش بهتایی کافی نیست و ممکن است برخی تهدیدات پنهان را نادیده بگیرد. روش ایستا با تحلیل ساختار و کد اپلیکیشن، مانند بررسی فراخوانی‌های API<sup>۳</sup> و مجوزها، اطلاعات ارزشمندی ارائه می‌دهد که می‌تواند در تشخیص دقیق‌تر کمک کند. پژوهش‌های اخیر نشان داده‌اند که ترکیب این دو روش می‌تواند نتایج بهتری در تشخیص بدافزارها ارائه دهد [۳].

## ۲-۱-۱ مجموعه داده‌های مربوطه

در حوزه تشخیص بدافزار اندروید، مجموعه داده‌های متنوعی برای ارزیابی عملکرد مدل‌ها مورد استفاده قرار گرفته‌اند. از جمله این مجموعه داده‌ها می‌توان به موارد زیر اشاره کرد:

- مجموعه داده‌های Drebin [۴] و AndroZoo [۵] که شامل نمونه‌های گسترده‌ای از بدافزارها و برنامه‌های سالم اندرویدی هستند.
- مجموعه داده‌های VirusShare [۶] و CICMalDroid که شامل نمونه‌های جدید و بهروز از بدافزارها می‌باشند.
- مجموعه داده‌های خصوصی و صنعتی که توسط شرکت‌های امنیتی و مراکز تحقیقاتی گردآوری شده‌اند.

این مجموعه داده‌ها به عنوان شاخص‌های استاندارد، امکان ارزیابی دقیق و جامع عملکرد الگوریتم‌های تشخیص بدافزار را فراهم می‌کنند و نقش مهمی در اثبات قابلیت تعییم و کارایی روش‌های پیشنهادی دارند.

## ۱-۲ ضرورت تحقیق و اهداف

پلتفرم اندروید به دلیل محبوبیت گسترده و سهم عظیمش از بازار جهانی، به هدف اصلی بدافزارها و حملات امنیتی تبدیل شده است. این سیستم عامل، که بیش از ۷۰ درصد دستگاه‌های هوشمند را پشتیبانی می‌کند، به دلیل ساختار باز و دسترسی‌پذیری بالا، با تهدیدات پیشرفته‌ای مواجه است. بدافزارهای اندرویدی،

<sup>1</sup>Dynamic Analysis

<sup>2</sup>Static Analysis

<sup>3</sup>API

از جمله تروجان‌ها<sup>۱</sup>، جاسوس‌افزارها<sup>۲</sup> و باج‌افزارها<sup>۳</sup>، با روش‌های پیچیده‌ای طراحی شده‌اند و پیشرفت‌های چشمگیری داشته‌اند. این تهدیدات، از سرقت اطلاعات حساس گرفته تا ایجاد اختلال در عملکرد دستگاه‌ها، چالش‌های امنیتی جدی ایجاد کرده‌اند. از این رو، نیاز به سیستمی قدرتمند و کارآمد برای تشخیص بدافزارهای اندرویدی بیش از پیش احساس می‌شود. هدف اصلی این پژوهش، تمرکز بر شناسایی بدافزارهای ناشناخته و نادیده (Zero-Day)<sup>۴</sup> است که تا کنون شناسایی نشده‌اند و می‌توانند تهدیداتی پنهان برای کاربران ایجاد کنند.

با توجه به چالش‌ها و نیازهای مطرح شده، اهداف اصلی این تحقیق بدین شرح می‌باشد:

- توسعه یک مدل چندوجهی پیشرفته با نام MAGNET که قادر به تحلیل همزمان داده‌های جدولی، گرافی و ترتیبی باشد.
- بهبود دقت تشخیص بدافزارهای اندرویدی با استفاده از معماری ترانسفورمر و مکانیزم‌های توجه پویا<sup>۵</sup>.
- کاهش نرخ خطای تشخیص و افزایش قابلیت تعیین‌پذیری مدل در مواجهه با بدافزارهای جدید.
- بهینه‌سازی مصرف منابع محاسباتی و افزایش سرعت تشخیص با استفاده از الگوریتم‌های پیشرفته.
- ایجاد یک چارچوب استاندارد برای ارزیابی و مقایسه روش‌های مختلف تشخیص بدافزار.

### ۱-۳- سازماندهی پایان نامه

در این پایان‌نامه، ساختار مطالب به گونه‌ای تدوین شده که مسیر پژوهش از مبانی نظری و معرفی مسئله تا ارائه نتایج تجربی به صورت پیوسته و منطقی دنبال شود. به عبارت دیگر، هدف از سازماندهی مطالب این است که خواننده بتواند به راحتی با مباحث پایه، چالش‌ها، روش‌های موجود و نوآوری‌های پیشنهادی آشنا شود و در نهایت به درک جامع از دستاوردهای تحقیق دست یابد. ساختار کلی پایان‌نامه به شرح زیر است:

- فصل دوم - پیشینه تحقیق و مفاهیم پایه:
- در این فصل، ابتدا به بررسی کلی امنیت اندروید و اهمیت تشخیص بدافزار پرداخته می‌شود. سپس، چالش‌ها و محدودیت‌های روش‌های سنتی بیان شده و مسئله تحقیق به تفصیل معرفی می‌شود. هدف این فصل ایجاد زمینه نظری مناسب برای درک اهمیت تشخیص خودکار بدافزارهای است.

---

<sup>1</sup>Trojan

<sup>2</sup>Spyware

<sup>3</sup>Ransomware

<sup>4</sup>Zero-Day

<sup>5</sup>Attention Mechanism

در ادامه به بررسی جامع مطالعات پیشین در حوزه تشخیص بدافزار اندرودید پرداخته می‌شود. در این بخش، رویکردهای مختلف از جمله روش‌های مبتنی بر یادگیری ماشین و یادگیری عمیق مورد تحلیل قرار می‌گیرند. نقاط قوت و ضعف هر یک از این رویکردها همراه با چالش‌های موجود در هر کدام به تفصیل بررسی می‌شود.

#### • فصل سوم – روش پیشنهادی (MAGNET):

در این فصل، مدل پیشنهادی MAGNET به صورت کامل تشریح می‌شود. ابتدا معماری کلی مدل و اجزای اصلی آن معرفی می‌شوند. سپس، جزئیات پیاده‌سازی و الگوریتم‌های بهینه‌سازی مورد استفاده توضیح داده می‌شود. در نهایت، نوآوری‌های اصلی این روش نسبت به سایر روش‌ها برجسته می‌شود.

#### • فصل چهارم – نتایج و بحث:

این فصل به ارائه نتایج آزمایش‌های انجام شده بر روی چندین مجموعه داده معتبر اختصاص دارد. عملکرد مدل MAGNET از نظر دقت، کارایی و صرفه‌جویی در منابع محاسباتی مورد مقایسه قرار گرفته و نتایج به دست آمده تحلیل می‌شوند.

#### • فصل پنجم – نتیجه‌گیری و پیشنهادات آتی:

در فصل نهایی، یافته‌های اصلی تحقیق به طور خلاصه ارائه شده و به نتیجه‌گیری کلی از دستاوردهای پژوهش پرداخته می‌شود. در این بخش، چالش‌های باقی‌مانده، محدودیت‌های تحقیق و نیز پیشنهادات آتی جهت تحقیقات آتی و بهبود رویکرد ارائه می‌شود.

**فصل دوم:**

**پیشینه تحقیق و مفاهیم پایه**

مدل‌های زبانی بزرگ بر اساس داده‌های متنه گستردۀ آموزش دیده و قابلیت درک و تولید زبان طبیعی را دارند. عملکرد این مدل‌ها بر پایه پیش‌بینی کلمات بعدی در یک جمله یا به عبارتی تکمیل متون بر اساس ورودی داده‌شده است.

در سال‌های اخیر، مدل‌های زبانی بزرگ رشد چشمگیری داشته‌اند و به دنبال این رشد، ایده استفاده از این مدل‌ها در تمامی زمینه‌های پردازش زبان طبیعی مورد توجه قرار گرفته است. قابلیت یادگیری مبتنی بر محتوا<sup>۱</sup>، که باعث می‌شود مدل‌ها به ورودی‌های دریافتی دقت ویژه‌ای کنند، کیفیت متن تولید شده جدید را به متن ورودی وابسته می‌کند. فلندا مهندسی اعلان یکی از اجزای کلیدی در بهبود عملکرد مدل‌های زبانی است. با طراحی دقیق اعلان‌ها، می‌توان ورودی‌های مدل را به گونه‌ای تنظیم کرد که پاسخ‌های تولیدی با اهداف و نیازهای خاص همخوانی بیشتری داشته باشند. این فرایند نه تنها به بهبود کیفیت و دقت خروجی‌های مدل کمک می‌کند، بلکه در کنترل و هدایت رفتار آن در مواجهه با وظایف مختلف نقش حیاتی دارد. استفاده از مهندسی اعلان زمینه‌ساز تطبیق بهتر مدل با شرایط متغیر و کاهش ابهامات در تولید جواب است.

مسئله اصلی این تحقیق، چالش‌های موجود در طراحی دستی اعلان‌هاست که به دلیل پیچیدگی و زمان بر بودن، نیازمند راهکارهایی خودکار می‌باشد. در این راستا، هدف این تحقیق ارائه روشی مبتنی بر الگوریتم جستجو در فضای اعلان‌ها برای تولید خودکار اعلان‌های بهینه است. این رویکرد می‌تواند باعث بهبود دقت و کارایی مدل‌های زبانی شده و از بروز خطاهای ناشی از طراحی دستی جلوگیری کند.

## ۲-۲ بررسی مدل‌های زبانی بزرگ

مدل‌های زبانی بزرگ سیستم‌های پیشرفته‌ای هستند که با بهره‌گیری از تکنیک‌های یادگیری عمیق، توانایی پردازش و تولید زبان طبیعی را به سطحی بالا رسانده‌اند. این مدل‌ها با تحلیل حجم عظیمی از داده‌های متنه، قادر به درک مفاهیم، استخراج اطلاعات و تولید متونی دقیق و معنادار می‌باشند. از کاربردهای آن‌ها می‌توان به ترجمه، خلاصه‌سازی، پاسخگویی به سوالات و حتی تولید محتوا در حوزه‌های مختلف اشاره کرد. تحولات اخیر در این حوزه، مسیر توسعه و بهبود این مدل‌ها را هموار ساخته است. شناخت تاریخچه و معماری این مدل‌ها نقش مهمی در درک عملکرد و پتانسیل‌های آن‌ها دارد که در ادامه به آن می‌پردازیم.

---

<sup>1</sup>In-context Learning

## ۱-۲-۲ تاریخچه و تکامل مدل‌ها

تکامل مدل‌های زبانی، مسیر پیچیده‌ای از رویکردهای اولیه‌ی مبتنی بر قواعد نمادین تا استفاده از شبکه‌های عصبی پیشرفته و معماری‌های نوین مانند ترنسفورمر را در بر می‌گیرد. در ادامه به تفصیل به بررسی مراحل مختلف این تکامل پرداخته می‌شود.

### دوران اولیه: رویکردهای نمادین و قواعد دست‌نویس

در دهه‌های ۱۹۵۰ و ۱۹۶۰، اولین تلاش‌ها برای پردازش زبان طبیعی به وسیله‌ی روش‌های نمادین انجام شد. پژوهشگران در آن زمان سعی می‌کردند ساختارهای دستوری و قوانین زبان را به صورت صریح و دستی تعریف کنند. این رویکردها با وجود تلاش‌های ارزشمند، به دلیل محدودیت‌های محاسباتی و عدم وجود داده‌های کافی، نتوانستند به دقت و کارایی مورد انتظار دست یابند.

### ورود به عصر آماری

با گذر زمان و ورود به دهه‌های ۱۹۶۰ و ۱۹۷۰، رویکردهای آماری جایگزین بخش‌هایی از روش‌های نمادین شدند. در این دوران، مدل‌های n-gram که بر مبنای احتمال وقوع یک کلمه با توجه به کلمات قبلی محاسبه می‌شدند، به عنوان اولین قدم‌های موفق در مدل‌سازی زبان مطرح شدند. اگرچه این مدل‌ها ساده بودند، اما توانستند برخی از پیچیدگی‌های اولیه‌ی پردازش زبان را کاهش دهند.

### ظهور یادگیری ماشین و شبکه‌های عصبی

در دهه‌های ۱۹۸۰ و ۱۹۹۰، با پیشرفت‌های چشمگیر در فناوری‌های محاسباتی و افزایش دسترسی به داده‌های متنی، روش‌های یادگیری ماشین وارد عرصه شدند. الگوریتم‌های یادگیری ناظارت شده و غیرناظارتی به منظور تشخیص الگوهای زبانی به کار گرفته شدند. با این حال، محدودیت‌های موجود همچنان مانع از دستیابی به درک عمیق‌تر و تولید متن‌های طبیعی به سطح امروزی می‌شدند.

### عصر شبکه‌های عصبی عمیق

ورود به قرن ۲۱ و بهویژه دهه ۲۰۱۰، با ظهور شبکه‌های عصبی عمیق مانند شبکه‌های عصبی بازگشتی<sup>۱</sup> و شبکه‌های حافظه بلندمدت<sup>۲</sup> همراه بود. این مدل‌ها توانستند وابستگی‌های زمانی و روابط بلندمدت موجود در متن را بهتر مدل‌سازی کنند. با این حال، چالش‌هایی همچنان در زمینه بهبود کیفیت و کارایی تولید متن وجود داشت.

### انقلاب ترنسفورمر و ظهور مدل‌های بزرگ

نقشه عطف مهم در تکامل مدل‌های زبانی، معرفی معماری ترنسفورمر [؟] بود. این معماری با بهره‌گیری از مکانیزم توجه<sup>۳</sup> توانست وابستگی‌های بین کلمات را به صورت موازی و با کارایی بالا پردازش کند.

<sup>1</sup>Recursive Neural Networks (RNNs)

<sup>2</sup>Long short-term memory (LSTM)

<sup>3</sup>Attention Mechanism

ویژگی‌های کلیدی ترنسفورمر شامل پردازش موازی داده‌ها، درک بهتر وابستگی‌های طولانی مدت در متن و افزایش سرعت و بهبود کارایی مدل‌های زبانی است.

### توسعه مدل‌های پیشرفته مانند GPT و BERT

با معرفی ترنسفورمر، مدل‌های بزرگی نظری GPT و BERT توسعه یافتد:

- GPT<sup>۱</sup>: این مدل‌ها با افزایش تعداد پارامترها (به عنوان مثال، ۳-GPT با ۱۷۵ میلیارد پارامتر) توانسته‌اند وظایفی مانند ترجمه، خلاصه‌سازی و پاسخ به سؤالات را با دقت بسیار بالا انجام دهنند.
- BERT<sup>۲</sup>: این مدل با تمرکز بر درک بهتر معنایی کلمات در متن، در وظایف مختلف پردازش زبان عملکرد قابل توجهی از خود نشان داده است.

### تکنیک‌های بهبود عملکرد: تنظیم دقیق و یادگیری انتقالی

علاوه بر افزایش تعداد پارامترها و مقیاس داده‌های آموزشی، تکنیک‌هایی مانند تنظیم دقیق<sup>۳</sup> و یادگیری انتقالی<sup>۴</sup> نقش مهمی در بهبود عملکرد مدل‌های زبانی داشته‌اند. این تکنیک‌ها امکان تطبیق مدل‌های پیش‌آموزش داده شده با وظایف خاص را فراهم می‌آورند که باعث بهبود کیفیت و دقت در کاربردهای متنوع می‌شود.

پیشرفتهای حاصل از توسعه مدل‌های زبانی بزرگ، مزهای جدیدی در تعامل انسان و ماشین ایجاد کرده است. سیستم‌های هوشمند مبتنی بر این مدل‌ها قادرند که به صورت طبیعی و انسانی با کاربران تعامل کنند، همچنین در زمینه‌های مختلفی از جمله خدمات مشتری، ترجمه ماشینی، تحلیل متون و تولید محتوا به کار گرفته شوندو وظایف پیچیده زبانی را با دقت و سرعت بالا انجام دهنند.

تکامل مدل‌های زبانی از روش‌های نمادین اولیه به سوی استفاده از شبکه‌های عصبی عمیق و معماری‌های پیشرفته مانند ترنسفورمر، نشان‌دهنده یک مسیر پر فراز و نشیب اما پر از نوآوری است. این پیشرفتهای بهبود قابل توجهی در درک و تولید زبان انسانی ایجاد کرده و نقش مهمی در توسعه فناوری‌های هوش مصنوعی و تعامل انسان–ماشین داشته‌اند.

## ۲-۲-۲ معماری‌ها و کاربردهای اصلی

در ادامه، به تفصیل به بررسی معماری‌های کلیدی این مدل‌ها می‌پردازیم.

### ۱. معماری ترنسفورمر<sup>۵</sup>: معماری ترنسفورمر پایه و اساس بسیاری از مدل‌های زبانی بزرگ است.

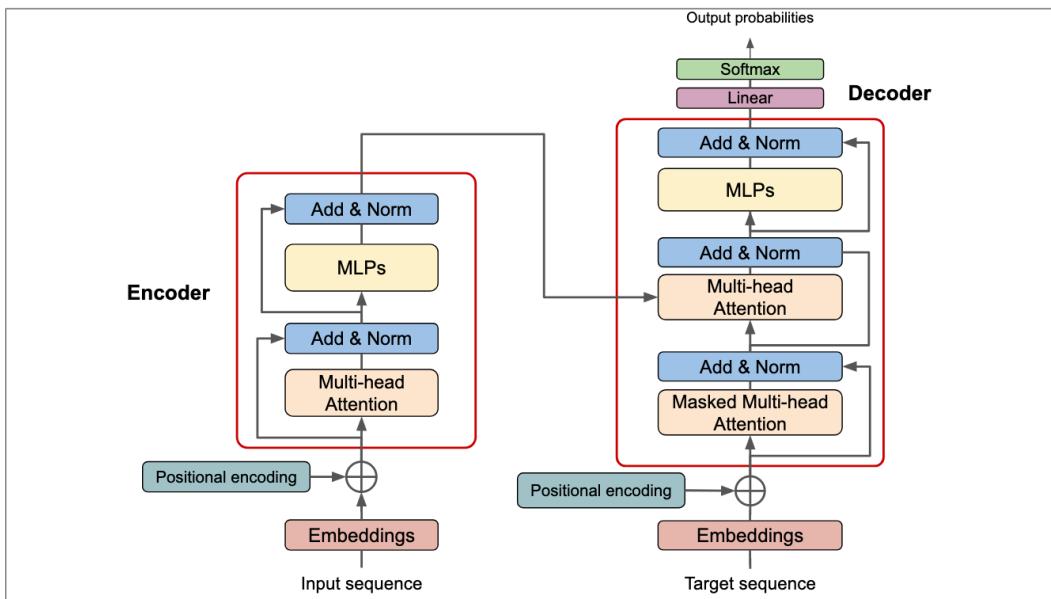
<sup>1</sup>Generative Pre-trained Transformer

<sup>2</sup>Bidirectional Encoder Representations from Transformers

<sup>3</sup>Fine-tuning

<sup>4</sup>Transfer Learning

<sup>5</sup>Transformer



شکل ۱-۲ دیاگرام معماری ترانسفورمر

این معماری با استفاده از مکانیزم توجه<sup>۱</sup>، امکان پردازش موازی داده‌ها و درک وابستگی‌های طولانی مدت در متن را فراهم می‌کند. برخلاف مدل‌های پیشین که بر پایه شبکه‌های عصبی بازگشتی<sup>۲</sup> بودند، ترانسفورمرها با حذف وابستگی‌های ترتیبی، کارایی و سرعت پردازش را بهبود بخشیدند. دیاگرام این معماری در شکل ۱-۲ نمایش داده شده است.

۲. مکانیزم توجه: مکانیزم توجه به مدل‌ها اجازه می‌دهد تا به بخش‌های مختلف ورودی با وزن‌های متفاوت نگاه کنند و وابستگی‌های معنایی را بهتر درک نمایند. این مکانیزم به‌ویژه در ترجمه ماشینی و خلاصه‌سازی متون کاربرد دارد.

### ۳. معماری‌های خودبازگشتی<sup>۳</sup> و خودرمزنگذار<sup>۴</sup>:

- مدل‌های خودبازگشتی مانند سری GPT متن را به صورت ترتیبی تولید می‌کنند و هر کلمه را بر اساس کلمات قبلی پیش‌بینی می‌نمایند.
- مدل‌های خودرمزنگذار مانند BERT با استفاده از ماسک‌کردن کلمات در ورودی، سعی در درک زمینه و پیش‌بینی کلمات ماسک‌شده دارند.

<sup>1</sup>Attention Mechanism

<sup>2</sup>Recursive Neural Networks

<sup>3</sup>Autoregressive

<sup>4</sup>Autoencoder

### ۳-۲-۲ مدل بزرگ زبانی Mistral

مدل بزرگ زبانی Mistral [۹] از جمله دستاوردهای جدید در حوزه پردازش زبان طبیعی به شمار می‌آید که با بهره‌گیری از معماری ترانسفورمر، عملکرد بالایی در وظایف متعدد زبانی نشان داده است. در ادامه به بررسی جامع این مدل می‌پردازیم.

مدل Mistral بر پایه معماری ترانسفورمر طراحی شده است. همانطور که گفته شد، این معماری با استفاده از مکانیزم توجه قادر است وابستگی‌های طولانی‌مدت در متون را به صورت موازی پردازش کند. از ویژگی‌های برجسته این مدل می‌توان به استفاده از تعداد پارامترهای بالا<sup>۱</sup> اشاره کرد که موجب بهبود دقت و کیفیت تولید متن می‌شود.

برای رسیدن به عملکرد مطلوب، مدل Mistral با استفاده از مجموعه‌های داده گسترده و متعدد آموخته داده شده است. علاوه بر این، بهره‌گیری از تکنیک‌های تنظیم دقیق<sup>۲</sup> و بهینه‌سازی پیشرفته، موجب شده تا مدل بتواند در وظایف خاص، همچون ترجمه، خلاصه‌سازی و پاسخ به پرسش، عملکرد بهتری از خود نشان دهد.

مدل Mistral در حوزه‌های مختلف پردازش زبان طبیعی کاربرد دارد. از وظایف مهم آن می‌توان به توانایی تولید متونی با کیفیت بالا و طبیعی، ارائه ترجمه‌های دقیق و روان بین زبان‌ها، استخراج اطلاعات کلیدی و ارائه خلاصه‌های مفید از متون طولانی و همچنین درک دقیق سوالات و ارائه پاسخ‌های مرتبط و دقیق اشاره کرد.

با وجود این توانایی‌ها، مدل Mistral دارای نوآوری‌ها و مزایای متعددی نیز است که آن را از سایر مدل‌های زبانی متمایز می‌کند. این نوآوری‌ها شامل بهره‌گیری از معماری ترانسفورمر جهت پردازش موازی و بهبود سرعت محاسبات است، همچنین استفاده از تعداد پارامترهای بالا به افزایش دقت و کیفیت خروجی‌ها منجر می‌شود و قابلیت تنظیم دقیق برای تطبیق با وظایف خاص و کاربردهای صنعتی و پژوهشی را فراهم می‌آورد و به دنبال آن، بهبود چشمگیری در درک وابستگی‌های زبانی و تولید متون طبیعی حاصل می‌شود.

با وجود دستاوردهای قابل توجه، مدل Mistral همچنان با چالش‌هایی همچون مصرف بالای منابع محاسباتی و نیاز به داده‌های آموزشی گسترده مواجه است. پژوهش‌های آتی در زمینه بهبود کارایی، کاهش هزینه‌های محاسباتی و افزایش دقت در کاربردهای خاص، افق‌های روشن‌تری را برای این مدل ترسیم می‌کند.

<sup>۱</sup> در این پژوهش از مدل‌های ۷ میلیارد پارامتری استفاده شده است

<sup>۲</sup>Fine-tuning

## ۳-۲ مهندسی اعلان

مهندسي اعلان<sup>۱</sup> به فرآيند طراحی و بهينه‌سازی ورودی‌های متنی اطلاق می‌شود که به مدل‌های زبانی بزرگ ارائه می‌گردد تا خروجی‌های مطلوب و دقیقی تولید کنند. این ورودی‌ها می‌توانند شامل دستورات، سوالات یا داده‌های زمینه‌ای باشند که به مدل کمک می‌کنند تا پاسخ‌های خود را در چارچوب معنایی و ساختاری مشخصی ارائه دهد. می‌دانیم که مهندسی اعلان تأثیر مستقیمی بر کارایی و دقت مدل‌های زبانی بزرگ دارد از این رو با تدوین اعلان‌های دقیق و مناسب با وظیفه موردنظر، می‌توان رفتار مدل را به‌گونه‌ای هدایت کرد که خروجی‌های مرتبطتر و با کیفیت‌تری تولید کند. این امر به‌ویژه در شرایطی که داده‌های آموزشی محدود یا ناموجود هستند، اهمیت بیشتری پیدا می‌کند. از مزایای مهندسی اعلان می‌توان به موارد زیر اشاره کرد :

- با استفاده از اعلان‌های دقیق و مناسب می‌توان نتایج مدل را به سمت پاسخ‌های موردنظر هدایت کرد و کنترل بیشتری بر خروجی مدل داشت.
- مهندسی اعلان می‌تواند به کاهش سوگیری‌های موجود در مدل‌های زبانی کمک کند و نتایج منصفانه‌تری ارائه دهد.
- با تدوین اعلان‌های مؤثر، می‌توان زمان و منابع موردنیاز برای رسیدن به نتایج مطلوب را کاهش داد و کارایی را افزایش داد.

در نتیجه، مهندسی اعلان به عنوان ابزاری قدرتمند برای بهبود عملکرد مدل‌های زبانی بزرگ محسوب می‌شود و نقش کلیدی در توسعه و بهره‌برداری مؤثر از این مدل‌ها ایفا می‌کند.

## ۴-۲ روش‌های دستی در مهندسی اعلان

مهندسي اعلان دستی به فرآيند طراحی و بهينه‌سازی دستی ورودی‌ها (اعلان‌ها) برای هدایت بهتر مدل‌های زبانی بزرگ در تولید پاسخ‌های مطلوب گفته می‌شود. برخلاف روش‌های خودکار که از الگوریتم‌های یادگیری ماشین برای بهینه‌سازی اعلان‌ها استفاده می‌کنند، روش‌های دستی بر دانش زبانی، شهود انسانی و آزمایش‌های مکرر متکی هستند. این تکنیک‌ها در کاربردهای واقعی که نیاز به کنترل دقیق بر خروجی مدل دارند، مانند پاسخ‌گویی به سوالات، خلاصه‌سازی متون و انجام وظایف استدلالی، به کار گرفته می‌شوند.

مهندسي اعلان دستی برای افزایش اثربخشی مدل‌های زبانی ضروری است، به‌ویژه در مواردی که تنظیم و آموزش مجدد مدل امکان‌پذیر نیست. از آنجایی که مدل‌های زبانی پاسخ‌های خود را بر اساس ورودی‌ها

<sup>۱</sup>Prompt Engineering

تولید می‌کند، حتی تغییرات جزئی در ساختار یا نحوه بیان اعلان‌ها می‌تواند تأثیر قابل توجهی بر عملکرد آن‌ها داشته باشد. اعلان‌های طراحی شده به صورت بهینه می‌توانند دقت مدل را افزایش داده، توانایی استدلال آن را بهبود بخشنده و میزان سوگیری در پاسخ‌ها را کاهش دهند، در نتیجه پاسخ‌های دقیق‌تر و متناسب‌تری ارائه کنند.

از ویژگی‌های کلیدی مهندسی اعلان دستی می‌توان به موارد زیر اشاره کرد :

#### ۱. طراحی مبتنی بر دانش انسانی

- برخلاف روش‌های خودکار که از الگوریتم‌های بهینه‌سازی استفاده می‌کنند، مهندسی اعلان دستی بر شهود انسانی و دانش زبانی تکیه دارد.
- درک صحیح از زبان و زمینه موردنظر نقش مهمی در طراحی اعلان‌هایی دارد که مدل را به تولید خروجی‌های مطلوب هدایت می‌کنند.

#### ۲. بهینه‌سازی تدریجی و تکرارشونده

- طراحی اعلان‌های مؤثر نیازمند آزمایش‌های مداوم و اصلاحات متوالی است.
- تنظيمات و تغییرات مداوم در نحوه بیان اعلان به شناسایی بهترین ساختار و سبک ورودی کمک می‌کند.

#### ۳. انعطاف‌پذیری در کاربردهای مختلف

- مهندسي اعلان دستی امکان شخصی‌سازی ورودی‌ها را برای وظایف متنوعی مانند تولید محظوظ، برنامه‌نویسی و استدلال منطقی فراهم می‌کند.
- استراتژی‌های خاصی را می‌توان برای هر کاربرد به کار گرفت، مانند ارائه دستورالعمل‌های گام‌به‌گام، اضافه کردن نشانه‌های متنی یا استفاده از نمونه‌های مشابه.

#### ۴. کنترل و تفسیرپذیری بهتر

- از آنجا که اعلان‌های دستی توسط انسان طراحی می‌شوند، کنترل بیشتری بر رفتار مدل فراهم می‌کنند.
- این روش امکان درک بهتر نحوه پاسخ‌گویی مدل به ورودی‌های مختلف را فراهم کرده و به عیب‌یابی و بهبود عملکرد کمک می‌کند.

با وجود مزایای فراوان، این روش با چالش‌هایی همراه است:

- فرآیند زمانبر: طراحی و بهینه‌سازی دستی اعلان‌ها نیاز به صرف زمان زیادی دارد.
- مقیاس‌پذیری پایین: برخلاف روش‌های خودکار، اعلان‌های دستی به راحتی برای مدل‌ها یا وظایف دیگر تعمیم نمی‌یابند.
- ماهیت مبتنی بر آزمون و خطای اعلان بهینه اغلب نیازمند آزمایش‌های متعدد است که همیشه نتیجه‌ای ثابت و پایدار را تضمین نمی‌کند.

در نهایت مهندسی اعلان دستی به عنوان رویکردی بنیادین برای بهینه‌سازی تعاملات با مدل‌های زبانی شناخته می‌شود. در بخش‌های بعدی، روش‌های مختلف مهندسی اعلان دستی را بررسی خواهیم کرد و تأثیر هر یک را بر توانایی‌های استدلالی و کیفیت پاسخ‌دهی مدل می‌سنجمیم.

#### ۱-۴-۲ یادگیری درون‌متنی

یادگیری درون‌متنی<sup>۱</sup> از قابلیت‌های برجسته مدل‌های زبانی بزرگ است که به آن‌ها اجازه می‌دهد بدون نیاز به بازآموزی<sup>۲</sup> یا تنظیم مجدد وزن‌ها، تنها با دریافت چند نمونه در ورودی، وظایف جدید را تشخیص دهند و به درستی انجام دهند. این روش به مدل کمک می‌کند با تحلیل مثال‌های ارائه‌شده در ورودی، پاسخ‌هایی متناسب با همان زمینه تولید کند. از مزایای مهم این روش، افزایش انعطاف‌پذیری در مواجهه با وظایف و موضوعات جدید است که باعث می‌شود مدل‌های زبانی به سرعت خود را با زمینه‌های مختلف تطبیق دهند. با حذف نیاز به بازآموزی برای هر وظیفه جدید، این روش می‌تواند بهینه‌سازی قابل توجهی در مصرف منابع و زمان ایجاد کند. از سوی دیگر، این قابلیت نقش مهمی در بهبود کیفیت تعاملات میان انسان و ماشین ایفا می‌کند. مدل‌ها با درک بهتر زمینه و مثال‌های ارائه‌شده، پاسخ‌هایی طبیعی‌تر و دقیق‌تر تولید می‌کنند که باعث افزایش رضایت کاربران می‌شود.

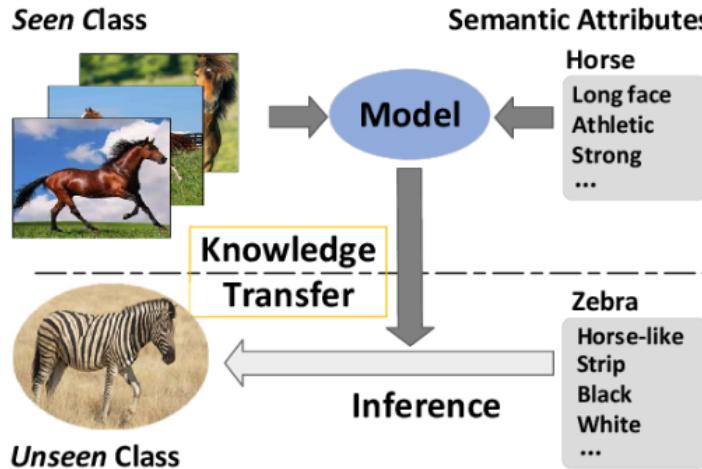
با وجود مزایای فوق، یادگیری درون‌متنی با چالش‌هایی نیز همراه است. عملکرد مدل‌ها به شدت به کیفیت و تنوع داده‌ها و مثال‌های ورودی وابسته است. مثال‌های ناقص یا ناسازگار می‌توانند منجر به تولید پاسخ‌های نادرست شوند. همچنین، در برخی موقعیت‌های پیچیده یا مبهم، مدل ممکن است در درک دقیق زمینه دچار مشکل شود.

از روش‌های یادگیری درون‌متنی می‌توان به یادگیری بدون نمونه و یادگیری با نمونه‌های کم اشاره کرد. در یادگیری بدون نمونه [؟]<sup>۳</sup> مدل‌ها وظیفه دارند اشیاء یا مفاهیمی را که در طول آموختش با آن‌ها روبرو نشده‌اند شناسایی و دسته‌بندی کنند. برخلاف یادگیری نظارت‌شده سنتی که نیاز به مثال‌های برچسب‌خورده

<sup>1</sup>In-Context Learning

<sup>2</sup>Training

<sup>3</sup>Zero-Shot Learning (ZSL)



شکل ۲-۲ مثالی از یادگیری بدون نمونه در یادگیری درون متنی

برای هر کلاس دارد، یادگیری بدون نمونه به مدل‌ها این امکان را می‌دهد که پیش‌بینی‌هایی در مورد دسته‌های دیده نشده در زمان آموزش با استفاده از اطلاعات کمکی انجام دهنند. برای شناسایی کلاس‌های دیده نشده در زمان آموزش، مدل‌های یادگیری بدون نمونه روابطی بین کلاس‌های مشاهده شده (دیده شده) و کلاس‌های مشاهده نشده (دیده نشده) برقرار می‌کنند. این ارتباط معمولاً از طریق ویژگی‌های مشترک یا اطلاعات معنایی که این دو به هم پیوند می‌دهند، تسهیل می‌شود. از طرفی وجود اطلاعات کمکی برای یادگیری بدون نمونه حیاتی است و داده‌های توصیفی در مورد کلاس‌های دیده شده و دیده نشده از ارائه می‌دهد. این اطلاعات می‌توانند شامل ویژگی‌هایی مانند توضیحات متنی، جاسازی‌های معنایی یا سایر داده‌های مرتبط باشد که به مدل کمک می‌کند تا کلاس‌ها را درک کرده و از هم تمایز دهد.

چگونگی عملکرد یادگیری بدون نمونه بدین صورت است که در غیاب مثال‌های برچسب‌خورده برای کلاس‌های دیده نشده، برای پر کردن شکاف به اطلاعات کمکی اتکا می‌کنند. به عنوان مثال، در طبقه‌بندی تصاویر، مدلی که بر اساس گونه‌های خاص حیوانات آموزش دیده باشد، می‌تواند از توضیحات متنی گونه‌های دیده نشده برای شناسایی صحیح آن‌ها استفاده کند. با درک اینکه یک گورخر مشابه یک اسب است اما با خطوط راهراه، مدل می‌تواند گورخرها را بدون دیدن آن‌ها در طول آموزش شناسایی کند (تصویر ۲-۲).

یادگیری بدون نمونه در حوزه‌های مختلفی کاربرد داشته است، از جمله:

- طبقه‌بندی تصویر: شناسایی اشیاء یا گونه‌هایی که در داده‌های آموزشی وجود ندارند.
- بخش‌بندی معنایی: بخش‌بندی اشیاء دیده نشده در تصاویر بر اساس ویژگی‌های یادگرفته شده.
- پردازش زبان طبیعی: انجام کارهایی مانند طبقه‌بندی متن یا شناسایی موجودیت‌ها بدون مثال‌های صریح.
- زیست‌شناسی محاسباتی: پیش‌بینی عملکرد ژن‌ها یا پروتئین‌هایی که قادر نشانه‌های آزمایشی هستند.

از چالش‌های مهم یادگیری بدون نمونه می‌توان به احتمال اشتباه کردن مدل در دسته‌بندی کلاس‌های دیده نشده اشاره کرد، به ویژه زمانی که این کلاس‌ها ویژگی‌های مشابه با کلاس‌های دیده شده دارند. تحقیقات جاری به دنبال افزایش کارایی و دقت مدل‌های یادگیری بدون نمونه است و روش‌هایی مانند تولید داده‌های مصنوعی برای کلاس‌های دیده نشده و بهبود کیفیت اطلاعات کمکی را بررسی می‌کنند.

در طرف دیگر ماجرا، برای یادگیری با نمونه‌های کم [؟] مدل‌ها طوری طراحی می‌شوند که بتوانند بر اساس تعداد بسیار محدودی از نمونه‌های آموزشی، یادگیری کرده و پیش‌بینی‌های دقیقی انجام دهنند. این رویکرد به ویژه در موقعیت‌هایی مفید است که جمع‌آوری مجموعه‌داده‌های بزرگ عملی یا مقرر نبهر صرفه نیست.

در یادگیری با نمونه‌های کم، مدل‌ها در مرحله استنتاج تنها تعداد کمی نمونه برچسب‌خورده (که اغلب به آن مجموعه پشتیبان<sup>۱</sup> گفته می‌شود) برای هر کلاس جدید دریافت می‌کنند. این تعداد محدود از نمونه‌ها به مدل امکان می‌دهد تا به سرعت خود را تطبیق داده و برای کلاس‌های نادیده شده پیش‌بینی انجام دهد. یک تنظیم رایج در یادگیری با نمونه‌های کم شامل الگوی K-shot N-way است که در آن 'N' نشان‌دهنده تعداد کلاس‌های جدید و 'K' نشان‌دهنده تعداد نمونه‌های برچسب‌خورده موجود برای هر کلاس است. برای مثال، در یک سناریوی 5-way 1-shot، 5 کلاس جدید وجود دارد که هر کدام تنها یک نمونه برچسب‌خورده دارند.

مدل‌های یادگیری با نمونه‌های کم معمولاً از تکییک‌های فرا-یادگیری<sup>۲</sup> استفاده می‌کنند که به آن "یادگیری برای یادگیری"<sup>۳</sup> نیز گفته می‌شود. در این چارچوب، مدل در طیف وسیعی از وظایف آموزش می‌بیند تا یک استراتژی برای تطبیق سریع با وظایف جدید با حداقل داده‌ها را یاد بگیرد. در زمان استنتاج، مدل با استفاده از همان تعداد اندک نمونه‌ها، پارامترهای خود را به‌طور مؤثری تنظیم می‌کند و می‌تواند دسته‌بندی‌های جدید را شناسایی و طبقه‌بندی کند.

از کاربردهای یادگیری با نمونه‌های کم می‌توان به موارد زیر اشاره کرد:

- یادگیری با نمونه‌های کم به مدل‌ها امکان می‌دهد تصاویر را با استفاده از تنها چند نمونه برچسب‌خورده در دسته‌های جدید طبقه‌بندی کنند که این موضوع به ویژه در حوزه‌هایی مانند تصویربرداری پزشکی که برچسب‌گذاری داده‌ها بسیار زمان بر است، اهمیت دارد.
- در حوزه پردازش زبان طبیعی، یادگیری با نمونه‌های کم می‌تواند در وظایفی مانند طبقه‌بندی متن و تحلیل احساسات به کار رود و به مدل‌ها کمک کند تا با حداقل داده متنی، موضوعات جدید را پردازش و درک کنند.

<sup>1</sup>support set

<sup>2</sup>meta Learning

<sup>3</sup>Learning to Learn

- ربات‌ها می‌توانند با استفاده از یادگیری با نمونه‌های کم وظایف جدید در زمینه دستکاری اشیاء یا تطبیق با محیط‌های تازه را یاد بگیرند، که این موضوع نیاز به آموزش مجدد گستردۀ را کاهش داده و امکان استقرار سریع در محیط‌های پویا را فراهم می‌آورد.

یکی از چالش‌های اصلی در یادگیری با نمونه‌های کم این است که اطمینان حاصل شود مدل‌ها خود را با داده‌های محدود به خوبی تعمیم می‌دهند و دچار بیش‌برازش<sup>۱</sup> نمی‌شوند. پژوهشگران در حال بررسی روش‌های مختلفی از جمله افزایش داده<sup>۲</sup>، یادگیری انتقالی<sup>۳</sup> و الگوریتم‌های پیشرفته فرا-یادگیری<sup>۴</sup> برای بهبود عملکرد مدل‌های یادگیری با نمونه‌های کم هستند.

برای فهم شفاف تر روش یادگیری درون متنی میتوان از یک چهارچوب ریاضیاتی [؟] کمک گرفت. در این چارچوب ریاضیاتی می‌توان یادگیری درون متنی را به عنوان یک استنتاج بیزی ضمنی<sup>۵</sup> تفسیر کرد. در چارچوب آن‌ها، در طی پیش‌آموزش<sup>۶</sup>، مدل‌های زبانی بزرگ با استنتاج مفاهیم پنهان در اعلان، که روابط معنایی و نحوی مختلفی را در متن در بر می‌گیرد، یاد می‌گیرند که توکن‌های بعدی را پیش‌بینی کنند. در زمان استنتاج<sup>۷</sup>، زمانی که مدلی با یک اعلان شامل مثال‌های ورودی-خروجی مواجه می‌شود، یک مفهوم پنهان مشترک بین این مثال‌ها را شناسایی می‌کند. این فرآیند شناسایی با استنتاج بیزی هم راستا است، جایی که مدل بر اساس داده‌های مشاهده شده، باورهای خود را به روزرسانی می‌کند تا پیش‌بینی انجام دهد.

$$P(\text{مفهوم} | \text{اعلان}) = \int P(\text{مفهوم} | \text{اعلان}, \text{خروجی}) P(\text{خروجی}) \cdot P(\text{مفهوم} | \text{اعلان}) \quad (1-2)$$

همانطور که در معادله ۱-۲ مشاهده می‌شود، از منظر بیزی، یادگیری درون متنی با پیدا کردن احتمال خروجی به شرط اعلان برابر است که انجام استنتاج توسط مدل برای یافتن یک مفهوم پنهان را در بر می‌گیرد که این مفهوم با وظیفه مورد نظر همخوانی دارد. با دریافت یک اعلان، مدل توزیع پسین<sup>۸</sup> را بر روی مفاهیم پنهان ممکن استنتاج می‌کند و مفهومی را انتخاب می‌کند که به بهترین نحو مثال‌های ارائه شده را توضیح می‌دهد. این فرآیند مشابه به روزرسانی بیزی است که در آن باورهای قبلی در پرتو شواهد جدید تنظیم می‌شوند تا پیش‌بینی‌های آگاهانه‌تری انجام گیرد.

<sup>1</sup>overfitting

<sup>2</sup>data augmentation

<sup>3</sup>transfer learning

<sup>4</sup>meta Learning

<sup>5</sup>implicit Bayesian inference

<sup>6</sup>pre-training

<sup>7</sup>inference time

<sup>8</sup>posterior

## ۲-۴-۲ روش زنجیره تفکر

روش زنجیره تفکر<sup>۱</sup> [۵] تکنیکی است که با هدف تقویت توانایی استدلال مدل‌های زبانی بزرگ طراحی شده و آن‌ها را راهنمایی می‌کند تا هنگام حل مسائل پیچیده، گام‌های میانی استدلالی تولید کنند. این رویکرد مدل‌ها را تشویق می‌کند تا وظایف را به بخش‌های متوالی و مرحله‌به‌مرحله تقسیم کرده و در نتیجه به خروجی‌هایی دقیق‌تر و قابل تفسیرتر برست.

این روش که توسط پژوهشگران گوگل معرفی شد، شامل ارائه نمونه‌هایی به مدل‌ها است که هم شامل مسئله و هم شامل راه حل گام‌به‌گام و دقیق هستند. به عنوان مثال، وقتی یک مسئله کلامی ریاضی به مدل داده می‌شود، مدل با استفاده از زنجیره تفکر تشویق می‌شود که محاسبات و مراحل منطقی منتهی به پاسخ نهایی را به صورت شفاف بیان کند. این روش نشان داده که عملکرد مدل‌ها را در وظایف نیازمند به محاسبات ریاضی، استدلال مبتنی بر عقل سليم و استدلال نمادین به شکل چشمگیری بهبود می‌دهد. به طور خاص، یک مدل با ۵۴۰ میلیارد پارامتر با استفاده از CoT موفق شد به دقتی فراتر از حد استاندارد در دیتابست GSM8K برای مسائل ریاضی دست پیدا کند و حتی بهتر از نسخه‌های تنظیم شده ۳-GPT عمل کند.

اثربخشی روش زنجیره تفکر بهویژه در مدل‌های بزرگ‌تر بیشتر مشهود است. مدل‌هایی با بیش از ۱۰۰ میلیارد پارامتر در مواجهه با زنجیره تفکر توانایی‌های نوظهوری در زمینه استدلال چند مرحله‌ای از خود نشان می‌دهند و می‌توانند مسائل چند گامی را به شکل موثرتری حل کنند. این تکنیک نه تنها دقت را افزایش می‌دهد، بلکه شفافیت فرآیند استدلال مدل را نیز بهبود می‌بخشد؛ چرا که هر گام به صورت صریح ارائه می‌شود.

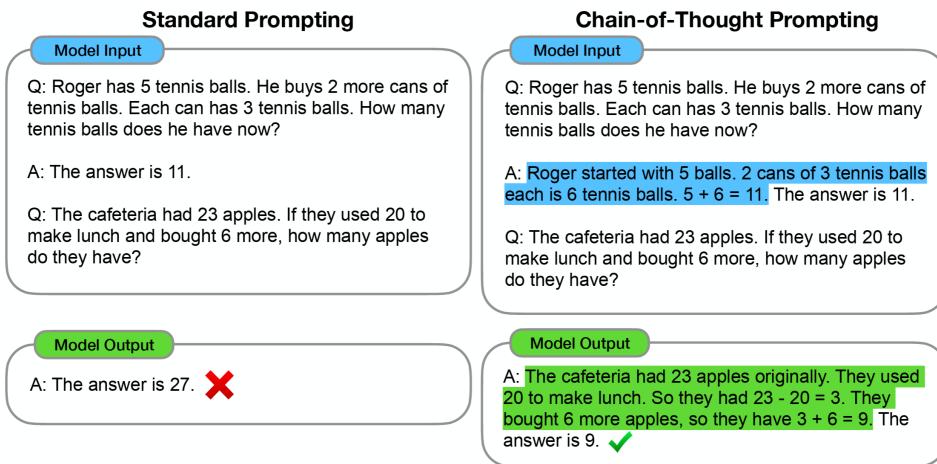
در شکل ۳-۲ یک نمونه از تولید جواب با استفاده از روش زنجیره تفکر آورده شده است. در این مثال به عنوان ورودی یک سوال و جواب نمونه به همراه راه حل قدم به قدم مسئله نیز آورده شده است تا مدل به سمت تولید راه حل سوق داده شود.

## ۳-۴-۲ روش استدلال بدون دیدن نمونه آموزشی

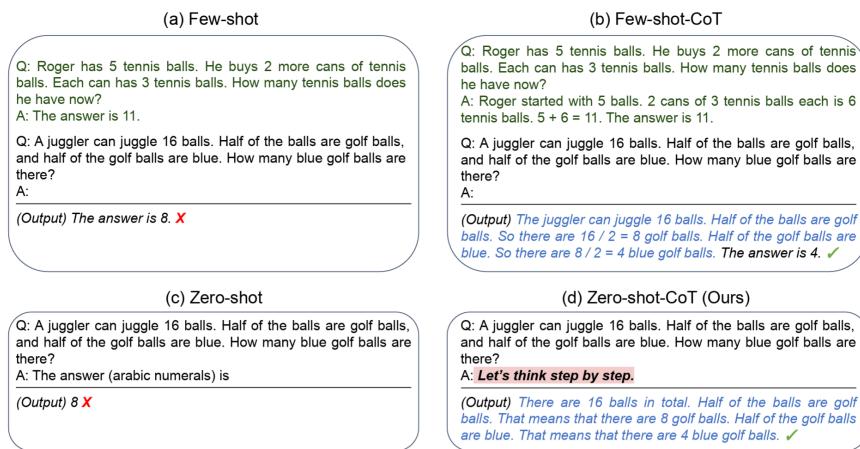
در مقاله‌ی استدلال بدون دیدن نمونه آموزشی<sup>۲</sup> [۶] ، پتانسیل مدل‌های بزرگ زبانی را برای انجام استدلال از طریق تغییرات ساده در اعلان‌ها و بدون افزودن نمونه‌ای از مثال‌های حل شده، بررسی شده است. با اضافه کردن عبارت «بایاید مرحله به مرحله فکر کنیم» به انتهای یک اعلان، مدل‌هایی مانند ۳-GPT و PaLM<sup>۳</sup> [۷] به‌طور قابل توجهی عملکرد بهتری در دیتابست‌های مختلف استدلالی ارائه می‌دهند. این روش بر توانایی ذاتی مدل‌ها در پردازش و تولید متن شبیه به انسان تکیه دارد و آن‌ها را تشویق می‌کند تا

<sup>1</sup>Chain-of-Thought

<sup>2</sup>Large Language Models are Zero-Shot Reasoners



شکل ۲ - ۳ مثالی از روش زنجیره تفکر برای حل یک سوال از دیتاست GSM8K



شکل ۴ - ۲ مقایسه روش استدلال بدون دیدن نمونه آموزشی و روش زنجیره تفکر

دباهه‌ای منطقی از تفکرات را که منجر به پاسخ نهایی می‌شود، تولید کنند. سادگی و کارآمدی این تکنیک، توانایی‌های استدلالی نهفته در مدل‌های بزرگ زبانی را آشکار می‌کند که می‌توان آنها را بدون نیاز به آموزش وسیع و خاص برای هر وظیفه فعال کرد. این یافته نشان می‌دهد که با مهندسی اعلان مناسب، این مدل‌ها می‌توانند طیف وسیعی از وظایف را به طور مؤثرتری انجام دهند و نیاز به دیتاست‌های بزرگ و برچسب‌گذاری شده و همچنین فرایندهای زمانبر تنظیم دقیق مدل‌ها را کاهش دهند. در شکل ۴ - ۲ نمونه از حل مسئله دیتاست GSM8K آورده شده است و جواب این روش با روش زنجیره تفکر مقایسه شده است.

## ۴-۴-۲ روش برنامه تفکر

روش برنامه تفکر<sup>۱</sup> [A] یک روش پیشرفته در مهندسی اعلان است که برای بهبود توانایی‌های استدلال عددی در مدل‌های زبانی بزرگ طراحی شده است. برخلاف تکنیک زنجیره تفکر که در آن مدل هم استدلال و هم محاسبات را در قالب متن تولید می‌کرد، در برنامه تفکر این دو فرآیند از یکدیگر جدا می‌شوند. در این روش، مدل استدلال خود را به صورت کد قابل اجرایی (معمولًاً با زبان‌هایی مانند پایتون) بیان می‌کند و این کد توسط یک مفسر خارجی اجرا می‌شود تا پاسخ نهایی به دست آید. این جداسازی باعث می‌شود محاسبه و استدلال از یکدیگر تفکیک شوند.

از مزایای روش برنامه تفکر می‌توان به موارد زیر اشاره کرد:

- با واگذاری محاسبات به یک مفسر خارجی، احتمال بروز خطاهای عددی که ممکن است در صورت انجام محاسبه و استدلال توسط خود مدل رخ دهد، کاهش می‌یابد و دقت بالاتر می‌رود.
- مطالعات تجربی نشان داده‌اند که برنامه تفکر می‌تواند عملکرد مدل را در وظایف عددی پیچیده به طور قابل توجهی افزایش دهد. برای مثال، آزمایش‌ها نشان داده‌اند که PoT نتایجی هم‌سطح با بهترین روش‌های موجود در دیتاست‌های مسائل ریاضی و نزدیک به بهترین عملکردها در دیتاست‌های مالی داشته است.
- نمایش مراحل استدلال به صورت کد، شفافیت فرآیند حل مسئله را افزایش می‌دهد و بررسی و درک هر مرحله را ساده‌تر می‌کند.

در شکل ۵-۲ حل مسئله دنباله فیبونانچی و پیداکردن ۵۰ امین عضو این دنباله، با استفاده از روش زنجیره تفکر و روش برنامه تفکر بررسی شده است. به دلیل طولانی بودن مراحل حل مسئله، روش زنجیره تفکر نتوانسته جواب درست را پیدا کند ولی روش برنامه تفکر ابتدا یک کد برای حل این مسئله ارائه داده است و پس از اجرای این کد با مفسر، به جواب صحیح رسیده است.

## ۵-۴-۲ روش بهینه سازی با اعلان

همانطور که گفته شد مدل‌های زبانی بزرگ تا به اینجا برای وظایفی مانند تولید متن، ترجمه و خلاصه‌سازی به کار گرفته می‌شدند. با این حال، تحقیقات اخیر ظرفیت این مدل‌ها را به عنوان بهینه‌سازها مورد بررسی قرار داده‌اند و از قابلیت‌های استدلالی آن‌ها برای حل مسائل پیچیده بهینه‌سازی بهره برده‌اند.

<sup>1</sup>Program-of-Thought

Question: In Fibonacci sequence, it follows the rule that each number is equal to the sum of the preceding two numbers. Assuming the first two numbers are 0 and 1, what is the 50th number in Fibonacci sequence?

The first number is 0, the second number is 1, therefore, the third number is  $0+1=1$ . The fourth number is  $1+1=2$ . The fifth number is  $1+2=3$ . The sixth number is  $2+3=5$ . The seventh number is  $3+5=8$ . The eighth number is  $5+8=13$ .  
..... (Skip 1000 tokens)  
The 50th number is 32,432,268,459.

CoT

```
length_of_fibonacci_sequence = 50
fibonacci_sequence = np.zeros(length_of_)
fibonacci_sequence[0] = 0
fibonacci_sequence[1] = 1
for i in range(3, length_of_fibonacci_sequence):
    fibonacci_sequence[i] = fibonacci_sequence[i-1] +
    fibonacci_sequence[i-2]
ans = fibonacci_sequence[-1]
```

PoT

 32,432,268,459



 python

 12,586,269,025



Question: Ketty saves 20000 dollars to the bank. After three years, the sum with compound interest rate is 1000 dollars more than the sum with simple interest rate. What is the interest rate of the bank?

Assuming the interest rate is  $x$ . The sum after two years with simple interest rate is  $20000 + x * 20000 * 3 = 20000 + 60000x$ . The sum after two years with compound interest rate is  $20000 * (1 + x)^3 = 200000 + 60000 * x + 60000x^2 + 20000x^3$ . The difference can be written as  $60000x^2 + 20000x^3 = 1000$ . In order to solve  $x$ , we can use the quadratic formula.  $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ , ...,  $x = \frac{(-20000 \pm 6160)}{120000}$ ,  $x = -0.051333$ .

CoT

```
interest_rate = Symbol('x')
sum_in_two_years_with_simple_interest = 20000 +
interest_rate * 20000 * 3
sum_in_two_years_with_compound_interest = 20000 * (1 +
interest_rate)**3
# Since compound interest is 1000 more than simple interest.
ans = solve(sum_after_in_yeras_with_compound_interest -
sum_after_two_years_in_compound_interest - 1000,
interest_rate)
```

PoT

 -0.051333



 python



 x = 0.24814



شکل ۲-۵ مقایسه روش برنامه تفکر و روش زنجیره تفکر

یکی از رویکردهای برجسته در این زمینه، روش بهینه سازی با اعلان<sup>۱</sup> [۹] است. این روش از مدل‌های زبانی بزرگ برای تولید راه حل‌های مسائل بهینه سازی بر اساس اعلان‌های زبان طبیعی استفاده می‌کند. این فرآیند شامل تکرارهای پی‌درپی است که در آن، اعلان جدید با راه حل‌ها و ارزیابی‌های قبلی طراحی می‌شود و در تکرارهای بعدی، راه حل‌های بهتری پیشنهاد می‌دهد. این روش در کاربردهای مختلفی همچون رگرسیون خطی<sup>۲</sup>، مسئله فروشنده دوره‌گرد<sup>۳</sup> و حتی بهینه سازی اعلان برای خود مدل‌های زبانی بزرگ مؤثر واقع شده است. جالب توجه اینکه این روش توانسته تا ۸٪ بهبود عملکرد در دیتاست GSM8K و تا ۵۰٪ بهبود در وظایف دشوار<sup>۴</sup> داشته باشد و حتی از اعلان‌های طراحی شده توسط انسان نیز پیشی بگیرد.

در روش بهینه سازی با اعلان، مسئله بهینه سازی با زبان طبیعی توصیف می‌شود تا مدل بتواند بافت و هدف مسئله را درک کند. همانطور که در شکل ۲-۶ در هر مرحله از بهینه سازی، مدل با توجه به اعلان شامل راه حل‌ها و ارزیابی‌های قبلی، راه حل‌های جدیدی تولید می‌کند. این راه حل‌ها ارزیابی شده و سپس برای تکرار بعدی در اعلان گنجانده می‌شوند و این چرخه بهبود مستمر ادامه پیدا می‌کند.

از مزایای استفاده از مدل‌های زبانی بزرگ به عنوان بهینه ساز می‌توان به موارد زیر اشاره کرد:

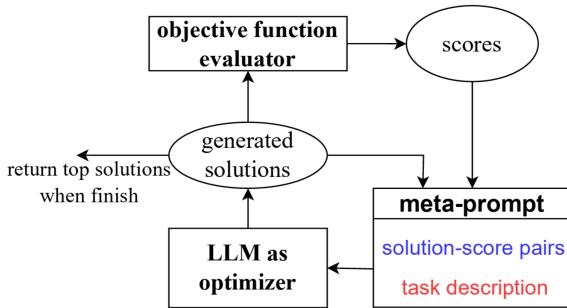
- مدل‌های زبانی بزرگ به دلیل توانایی درک و تولید متن مشابه انسان، می‌توانند به انواع مختلف مسائل بهینه سازی که با زبان طبیعی توصیف می‌شوند، پاسخ دهند.

<sup>1</sup> Optimization by PROMPTing

<sup>2</sup> Linear Regression

<sup>3</sup> Traveling Salesman Problem

<sup>4</sup> Big-Bench Hard



شکل ۲-۶ دیاگرام روش بهینه سازی با اعلان

- همچنین این مدل‌ها قادر به انجام بهینه‌سازی در مسائلی هستند که اطلاعات گرادیان در دسترس نیست یا بدست آوردن آن دشوار است و به همین دلیل رویکردی بدون نیاز به مشتق ارائه می‌دهند.
- از طرفی این مدل‌ها می‌توانند اعلان‌های خود را بهینه کنند و بدون نیاز به آموزش مجدد، عملکرد خود را در وظایف خاص بپسند دهند.

#### ۶-۴-۶ روش برنامه‌ریزی و حل

روش برنامه‌ریزی و حل<sup>۱</sup> یک تکنیک پیشرفته در مهندسی اعلان است که بهبود عملکرد مدل‌های زبانی بزرگ را در حل مسائل پیچیده مورد هدف قرار می‌دهد. در این روش، مدل ابتدا یک برنامه‌ریزی<sup>۲</sup> انجام داده و سپس بر اساس آن، به حل مسئله<sup>۳</sup> می‌پردازد.

برخلاف روش‌های سنتی که مدل را مستقیماً درگیر حل مسئله می‌کنند، این روش باعث کاهش نرخ خطای شده و دقت پاسخ‌های مدل را افزایش می‌دهد. روش برنامه‌ریزی و حل به‌ویژه در مسائلی که نیاز به چندین مرحله استدلالی دارند، مانند حل مسائل ریاضی، تحلیل منطقی و برنامه‌ریزی وظایف، بسیار کارآمد است.

این روش شامل دو مرحله اصلی است:

- برنامه‌ریزی<sup>۴</sup>: مدل یک برنامه کلی برای حل مسئله ارائه می‌دهد، شامل مراحل موردنیاز برای رسیدن به پاسخ.
- حل مسئله<sup>۵</sup>: مدل بر اساس برنامه تولیدشده، گام‌به‌گام راه حل را پیاده‌سازی کرده و پاسخ نهایی را استخراج می‌کند.

<sup>1</sup> Plan-and-Solve (PS)

<sup>2</sup> Planing

<sup>3</sup> Solve

<sup>4</sup> Plan Phase

<sup>5</sup> Solve Phase

این تفکیک دو مرحله‌ای، عملکرد مدل را بهبود می‌بخشد زیرا ابتدا ساختار حل مسئله مشخص شده و سپس محاسبات انجام می‌شود. در ادامه یک مسئله و راه حل این روش برای آن مسئله را بررسی می‌کنیم.

مسئله: سن علی ۳ برابر سن برادرش است. ۴ سال پیش، مجموع سن آن‌ها ۲۰ سال بوده است. سن هر یک را مشخص کنید.

#### ۱. اجرای مرحله برنامه‌ریزی:

- تعریف متغیرها: فرض کنیم سن برادر علی را  $X$  در نظر بگیریم.
- رابطه کنونی: سن علی برابر با  $3X$  است.
- رابطه در گذشته: ۴ سال پیش، سن برادر علی برابر  $4 - X$  و سن علی برابر  $4 - 3X$  بوده است.

#### • معادله کلی:

$$(X - 4) + (3X - 4) = 20$$

#### • حل معادله و یافتن مقدار $X$

#### ۲. اجرای مرحله حل:

$$X - 4 + 3X - 4 = 20$$

$$4X - 8 = 20$$

$$4X = 28$$

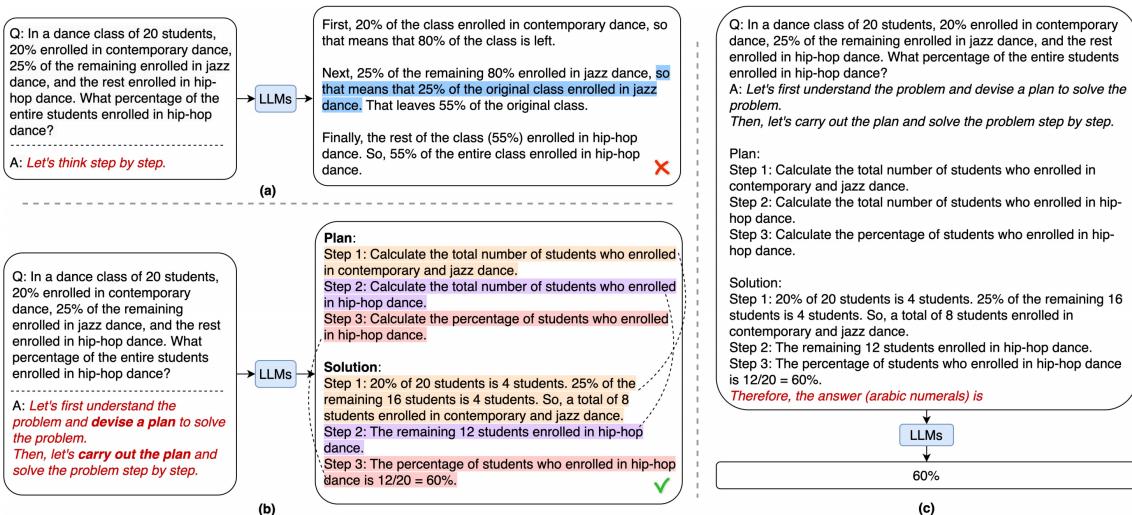
$$X = 7$$

در نتیجه :

#### • سن برادر علی : ۷ سال

#### • سن علی : $7 \times 3 = 21$ سال

با بررسی این مثال می‌توان متوجه افزایش دقت حل مسائل چند مرحله‌ای با استفاده از روش برنامه‌ریزی و حل شد و همچنین عملکرد برنامه ریزی و سپس عمل را مشاهده کرد که مشابه سیستم تفکر انسانی است. در شکل ۷-۲ یک مثال دیگر از این روش آورده شده است.



شکل ۷-۲ یک مثال از روش برنامه‌ریزی و حل

## ۵-۲ بهینه‌سازی خودکار اعلان‌ها

بهینه‌سازی خودکار اعلان‌ها یک رویکرد نوین در مهندسی اعلان است که با بهره‌گیری از الگوریتم‌های جستجو و بهینه‌سازی، به صورت سیستماتیک بهترین ورودی‌های متنی را برای مدل‌های زبانی شناسایی و تولید می‌کند. در این روش به جای تکیه بر شهود انسانی و روش‌های آزمون و خطأ، از تکنیک‌هایی مانند الگوریتم‌های تکاملی، جستجوی تصادفی و یادگیری تقویتی استفاده می‌شود. این الگوریتم‌ها فضای اعلان‌ها را مورد بررسی قرار داده و بر اساس معیارهای مشخصی مانند دقیق، انسجام و ارتباط معنایی، به انتخاب بهینه‌ترین اعلان‌ها می‌پردازند.

یکی از مزایای مهم بهینه‌سازی خودکار اعلان‌ها این است که در مقیاس‌های بزرگ و در زمان‌های کوتاه، قادر به دستیابی به نتایج بهینه می‌باشد. بهینه‌سازی خودکار پرامت‌ها با ارائه چارچوبی سیستماتیک، امکان ارزیابی سریع و انتخاب اعلان‌های بهینه را فراهم می‌آورد. این دو رویکرد می‌توانند مکمل یکدیگر عمل کرده و در کاربردهایی که نیاز به سرعت و دقیق بالا دارند، مانند پردازش دسته‌جمعی داده‌های متنی یا تنظیم خودکار اعلان‌ها برای وظایف متنوع، عملکرد بهتری ارائه دهند.

## ۵-۱ روش زنجیره تفکر خودکار

از اولین جرقه‌های خودکارسازی مهندسی اعلان، می‌توان به خودکارسازی تولید زنجیره‌های استدلالی در روش زنجیره تفکر اشاره کرد. روش زنجیره تفکر خودکار<sup>۱</sup> [؟] به طور خودکار زنجیره‌هایی از استدلال‌ها و سوالات را برای ساخت نسخه‌ها ایجاد می‌کند. این روش شامل دو مرحله اصلی است. مرحله اول خوشبندی

<sup>۱</sup> AUTOMATIC CHAIN-OF-THOUGHT PROMPTING (Auto-CoT)

سوالات و تقسیم سوالات یک مجموعه‌داده به چندین خوش و مرحله دوم نمونه‌گیری از نسخه‌ها و انتخاب یک سوال نماینده از هر خوش و تولید زنجیره استدلال برای آن است. روند کلی این روش در شکل ۸-۲ نشان داده شده است.

در مرحله اول، از آنجایی که خوشبندی متنی بر تنوع می‌تواند از گمراهی ناشی از شباهت جلوگیری کند، این روش تحلیل خوش‌های را برای مجموعه‌ای از سوالات  $Q$  انجام می‌دهد. بدین صورت که ابتدا برای هر سوال در  $Q$ ، یک بردار نمایشی با استفاده از Sentence-BERT [؟] محاسبه می‌شود و سپس این بردارهای متنی میانگین‌گیری شده و یک بردار با اندازه ثابت برای هر سوال ایجاد می‌شود. پس از آن، با استفاده از الگوریتم خوشبندی k-means، سوالات به  $k$  خوش تقسیم می‌شوند. در نهایت برای هر خوش  $i$ ، سوالات آن خوش را به صورت یک لیست مرتب شده  $[q_1^{(i)}, q_2^{(i)}, \dots]$  بر اساس فاصله از مرکز خوش به ترتیب صعودی مرتب می‌شوند.

در مرحله دوم، برای سوالات نمونه‌گیری شده، زنجیره‌های استدلال تولید می‌شوند و نسخه‌هایی که با معیارهای انتخاب مطابقت دارند استخراج می‌شوند. به طور دقیق‌تر، برای هر خوش  $i$ ، یک نسخه به صورت  $d^{(i)}$  (ترکیبی از سوال، استدلال و پاسخ) ساخته می‌شود. برای خوش  $i$ ، سوالات مرتب شده در لیست  $q^{(i)} = [q_1^{(i)}, q_2^{(i)}, \dots]$  تا زمانی که معیارهای انتخاب برآورده شوند، بررسی می‌شوند. به عبارت دیگر، سوالی که به مرکز خوش نزدیک‌تر است، زودتر بررسی می‌شود. فرض کنید سوال  $q_j^{(i)}$  که  $j$ -امین سوال نزدیک به مرکز خوش  $i$  است، در حال بررسی باشد. یک ورودی به شکل زیر ساخته می‌شود:

$$[Q: q_j^{(i)} \ A: [P]]$$

سپس یک نسخه کاندید برای خوش  $i$  به صورت زیر ساخته می‌شود:

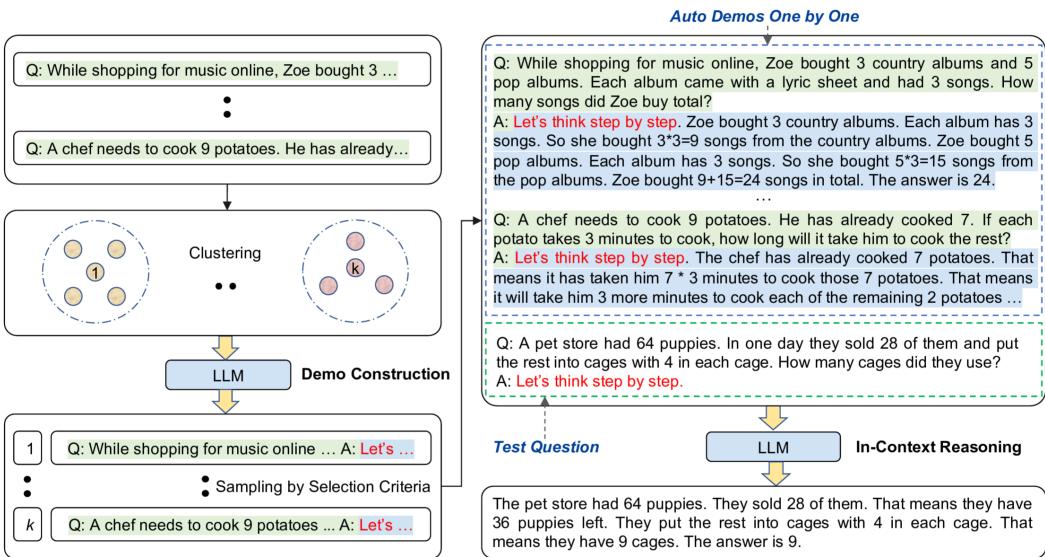
$$[Q: q_j^{(i)} \ A: r_j^{(i)} \ a_j^{(i)}]$$

مشابه معیارهای مورد استفاده در نسخه‌های دستی روش زنجیره تفکر [V]، معیار انتخاب این الگوریتم نیز بر قوانین ساده‌ای تکیه دارد تا سوالات و استدلال‌های ساده‌تر را انتخاب کند: نسخه  $d_j^{(i)}$  به عنوان  $d^{(i)}$  انتخاب می‌شود اگر سوال  $q_j^{(i)}$  دارای کمتر از ۶ توکن و استدلال  $r_j^{(i)}$  دارای کمتر از ۵ گام استدلالی باشد.

## ۲-۵-۲ روش مهندس اعلان خودکار

روش مهندس اعلان خودکار <sup>۱</sup> [؟] از خود مدل‌های زبانی بزرگ برای خودکارسازی فرآیند ایجاد و بهینه‌سازی اعلان‌ها استفاده می‌کند. در این روش، یک مدل زبانی، مجموعه‌ای از اعلان‌های مختلف تولید

<sup>۱</sup>Auto Prompt Engineer



شکل ۸-۲ دیاگرام روش auto-CoT

می‌کند و سپس این اعلان‌ها بر اساس کیفیت پاسخ‌هایی که از یک مدل دیگر دریافت می‌شود، ارزیابی می‌شوند. این فرآیند به صورت تکراری ادامه می‌یابد تا مؤثرترین اعلان‌ها شناسایی شوند. نتایج در ۲۴ وظیفه مختلف در حوزه پردازش زبان طبیعی نشان داده که اعلان‌های تولید شده توسط این روش در اغلب موارد عملکرد بهتری نسبت به روش‌های قبلی داشته‌اند و در ۱۹ مورد از ۲۴ وظیفه، کیفیتی معادل یا نزدیک به اعلان‌های طراحی شده توسط انسان ارائه کرده‌اند.

تأثیرات این روش قابل توجه است؛ این روش نیاز به مهندسان اعلان انسانی را کاهش می‌دهد، فرآیند توسعه را سریع‌تر می‌کند و سازگاری مدل‌های زبانی بزرگ با وظایف مختلف را افزایش می‌دهد. این پیشرفت نشان‌دهنده ظرفیت مدل‌های بزرگ زبانی برای نه تنها انجام وظایف، بلکه بهینه‌سازی دستورالعمل‌های خودشان نیز هست و گامی مهم به سوی سامانه‌های هوشمند خودمختارتر به شمار می‌رود.

### ۳-۵-۲ روش مولد اعلان

روش مولد اعلان<sup>۱</sup> [۹] یک سیستم خودارجاعی<sup>۲</sup> و تکاملی برای بهبود خودکار اعلان‌های مورد استفاده در مدل‌های زبانی بزرگ است. این روش با الهام از الگوریتم‌های تکاملی و فرآیندهای خودبهبوددهی<sup>۳</sup>، به جای اتکا بر اعلان‌های دستی و مهندسی شده، به طور خودکار اعلان‌هایی را تولید و اصلاح می‌کند که می‌توانند عملکرد مدل را در حل مسائل مختلف بهبود بخشنند. ویژگی کلیدی این روش این است که نه تنها

<sup>1</sup>Promptbreeder

<sup>2</sup>self-referential

<sup>3</sup>self-improvement

اعلان‌های وظیفه<sup>۱</sup> را تکامل می‌دهد، بلکه اعلان‌های تغییر<sup>۲</sup> را نیز که برای تغییر اعلان‌های مورد جستجو استفاده می‌شوند، بهبود می‌بخشد.

این الگوریتم از یک فرآیند تکاملی مبتنی بر جمعیت<sup>۳</sup> استفاده می‌کند. همانطور که در شکل ۹-۲ نشان داده شده است، در ابتدا یک مجموعه از اعلان‌های اولیه به همراه دستورات تغییر تولید می‌شود. سپس، در هر نسل از فرآیند تکامل:

۱. ارزیابی سازگاری<sup>۴</sup>: اعلان‌ها بر اساس عملکردشان در پاسخ‌دهی به مجموعه‌ای از سؤالات آموزشی ارزیابی می‌شوند.

۲. انتخاب<sup>۵</sup>: دو اعلان به صورت تصادفی انتخاب شده و مقایسه می‌شوند؛ اعلانی که عملکرد بهتری داشته باشد، انتخاب می‌شود.

۳. اعمال تغییرات<sup>۶</sup>: اعلان انتخاب شده با استفاده از عملگرهای تکاملی تغییر داده می‌شود. این تغییرات شامل تولید نسخه‌های جدید از اعلان، اصلاح بر اساس الگوهای موفق، و یا حتی بهبود خود دستور تغییر است.

۴. جایگزینی<sup>۷</sup>: نسخه‌ی بهبودیافته جایگزین اعلان با عملکرد ضعیفتر شده و این فرآیند در نسل‌های بعدی تکرار می‌شود.

عملگرهای تکاملی شامل جهش مستقیم<sup>۸</sup>، جهش مبتنی بر توزیع<sup>۹</sup>، ابرجهش<sup>۱۰</sup>، جهش لامارکین<sup>۱۱</sup>، و ترکیب اعلان‌ها<sup>۱۲</sup> هستند که هر یک روش‌های متفاوتی را برای اصلاح و بهبود اعلان‌ها ارائه می‌دهند. با ادامه این فرآیند در طی چندین نسل، اعلان‌ها به تدریج بهینه شده و به عملکرد بهتری در مدل‌های زبانی منجر می‌شوند.

روش مولد اعلان در آزمایش‌های مختلف نشان داده است که می‌تواند از روش‌های متداول مهندسی اعلان مانند CoT و PS عملکرد بهتری داشته باشد. همچنین، این سیستم در حوزه‌های مختلف مانند حل

<sup>1</sup>Task Prompts

<sup>2</sup>Mutation Prompts

<sup>3</sup>population base

<sup>4</sup>Fitness Evaluation

<sup>5</sup>Selection

<sup>6</sup>Mutation

<sup>7</sup>Replacement

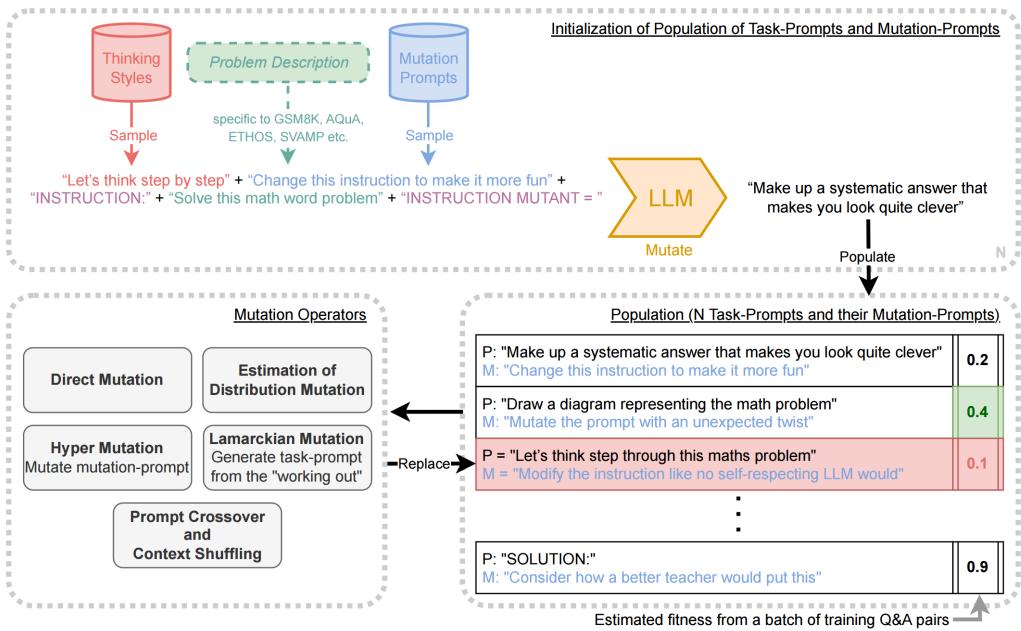
<sup>8</sup>Direct Mutation

<sup>9</sup>Estimation of Distribution (EDA) Mutation

<sup>10</sup>Hypermutation

<sup>11</sup>Lamarckian Mutation

<sup>12</sup>Prompt Crossover and Context Shuffling



شکل ۹-۲ دیاگرام روش مولد اعلان

مسائل ریاضی، استدلال عمومی<sup>۱</sup>، و کلاس‌بندی گفتار نفرت‌آمیز<sup>۲</sup> بهبود چشمگیری ایجاد کرده است. مهم‌ترین مزیت آن این است که به بروزرسانی پارامترهای مدل نیازی ندارد و تنها از طریق اصلاح اعلان‌ها، کارایی مدل را افزایش می‌دهد.

این روش نشان‌دهنده قدرت بهینه‌سازی خودکار اعلان‌ها و حرکت بهسوی سیستم‌های هوش مصنوعی خودبهبوددهنده و خودارجاعی است که می‌توانند با حداقل مداخله انسانی، عملکرد خود را در طی زمان بهبود بخشنند.

## ۶-۲ جمع‌بندی مباحث ارائه شده

این فصل با هدف بررسی پیشینه تحقیق و تبیین مفاهیم بنیادی مرتبط با موضوع پژوهش تدوین گردید. در این فصل، تلاش شد تا ضمن ارائه چارچوب نظری جامع، زمینه مناسبی برای درک بهتر مسأله تحقیق و مسیر پژوهش فراهم شود. با توجه به گستره و عمق موضوعات مطرح شده، می‌توان این فصل را به عنوان شالوده‌ای برای تحلیل‌ها و مطالعات تخصصی‌تر در فصول بعدی قلمداد نمود.

در این فصل، نخست به معرفی و تحلیل مدل‌های زبان بزرگ پرداخته شد و روند تکاملی این مدل‌ها از آغاز تا وضعیت کنونی آن‌ها مورد بررسی قرار گرفت. در ادامه، به معماری‌های رایج و کاربردهای متنوع این مدل‌ها اشاره شد و اهمیت آن‌ها در پیشبرد حوزه‌های مختلف پردازش زبان طبیعی و سامانه‌های مبتنی بر

<sup>1</sup>commonsense reasoning

<sup>2</sup>hate speech classification

هوش مصنوعی تبیین گردید.

سپس، به موضوع مهندسی اعلان و نقش آن در بهره‌برداری مؤثر از مدل‌های زبان بزرگ پرداخته شد. در این بخش، ابتدا روش‌های سنتی مهندسی اعلان، شامل استفاده از یادگیری درون متنی، روش زنجیره تفکر، استدلال بدون نمونه آموزشی، برنامه تفکر، بهینه سازی با اعلان و روش برنامه‌ریزی و حل به تفصیل بررسی شدند. در ادامه، به معروف و تحلیل رویکردهای نوین در بهینه‌سازی خودکار اعلان‌ها پرداخته شد. از جمله این روش‌ها می‌توان به زنجیره تفکر خودکار، مهندسی اعلان خودکار و روش مولد اعلان اشاره نمود که هریک با هدف افزایش دقت و توان استدلال مدل‌های زبانی توسعه یافته‌اند.

بر مبنای مباحث ارائه شده، آشکار شد که مهندسی اعلان و بهینه‌سازی آن از مهم‌ترین مؤلفه‌ها در افزایش کارایی مدل‌های زبان بزرگ به شمار می‌رود. این امر اهمیت طراحی الگوریتم‌های نوین و کارآمد برای بهبود ساختار و محتوای اعلان‌ها را دوچندان می‌سازد.

در فصل آتی، به تشریح کامل الگوریتم پیشنهادی پرداخته خواهد شد. این الگوریتم که مولد اعلان ساده نام دارد، یکی از رویکردهای نوین در زمینه بهینه‌سازی و تکامل خودکار اعلان‌ها محسوب می‌شود و مبتنی بر اصول الگوریتم‌های تکاملی و بهبود مستمر اعلان‌ها از طریق تولید، ارزیابی و گرینش نسل‌های مختلف اعلان‌ها طراحی شده است. در فصل آینده، بهطور دقیق به ساختار، مراحل اجرایی و مزایای این الگوریتم در مقایسه با سایر روش‌ها پرداخته خواهد شد.

# فصل سوم:

# روش‌های پیشنهادی

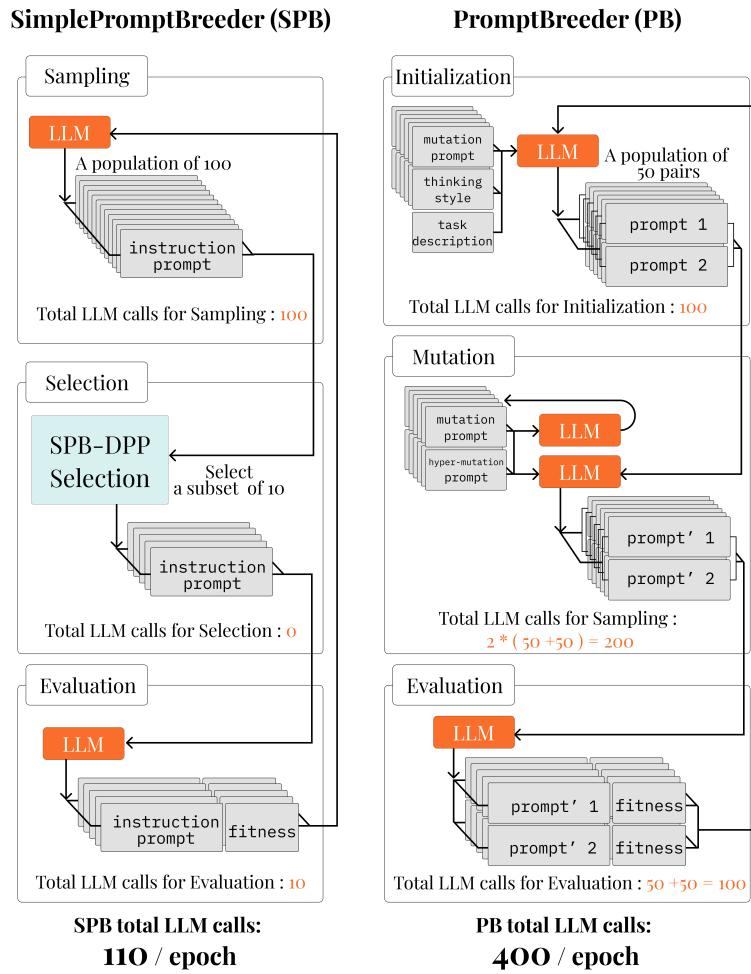
همانطور که گفته شد، عملکرد مدل‌های زبانی بزرگ بهشت به مهندسی اعلان وابسته است، چرا که دستورات به طور مستقیم بر تفسیر مدل از وظایف و همچنین نحوه تولید خروجی تاثیر می‌گذارند. بنابراین، دستورات نقش حیاتی در اثربخشی مدل‌های زبانی بزرگ ایفا می‌کنند، فرآیندی که معمولاً از طریق آنچه به عنوان مهندسی دستور شناخته می‌شود، بهینه‌سازی می‌گردد. استراتژی‌های پرکاربردی مانند زنجیره تفکر [۷] اثربخشی خود را در بهبود توانمندی‌های استدلالی مدل‌های زبانی با تجزیه مسائل پیچیده به گام‌های میانی نشان داده‌اند [۸]، [۹]، [۱۰]. با این حال، استراتژی‌های دستی طراحی شده توسط انسان، به دلیل وابستگی به شهود انسانی، غالباً برای وظایف خاص دامنه محور، بهینه نبوده و نمی‌توانند به طور کامل از ظرفیت مدل‌های پایه بهره‌برداری کنند. از سوی دیگر، با پیشرفت مدام مدل‌های زبانی و تغییر قابلیت‌های آن‌ها، مؤثرترین دستورات نیز ممکن است دستخوش تغییر شوند. به طور کلی، مهندسی اعلان که به صورت دستی انجام می‌شود، فرآیندی زمان‌بر بوده و نتایجی کمتر از حد بهینه به همراه دارد. این محدودیت‌ها موجب شده است که تولید خودکار دستورات به عنوان یک حوزه تحقیقاتی مهم در هوش مصنوعی مطرح گردد [۱۱]، [۱۲]. همانطور که در فصل قبل دیدیم، الگوریتم‌های مختلفی برای بهینه‌سازی دستورات معرفی شده‌اند؛ از جمله بهینه‌سازی با اعلان [۱۳]، مولد اعلان [۹] و سایر روش‌ها [۱۴]، [۱۵]. در این میان، روش مولد اعلان با استفاده از یک چارچوب تکاملی و خودارجاعی، از طریق تکرار فرآیند جهش و ارزیابی یک جمعیت از دستورات وظیفه، به بهینه‌سازی دستورات می‌پردازد. اگرچه نشان داده شده است که روش مود اعلان برای وظایف استدلالی و طبقه‌بندی مؤثر است، اما پیچیدگی طراحی آن موجب کاهش قابلیت تعمیم این روش می‌شود. افزون بر این، عدم تنوع کافی در دستورات تولید شده می‌تواند چالش‌زا باشد. وابستگی به چندین لایه بهینه‌سازی، سازوکارهای خودارجاعی و حتی به کارگیری تکنیک‌هایی برای فریب مدل زبانی ممکن است موجب عدم موفقیت این روش هنگام به کارگیری بر روی مدل‌های زبانی جدید شود.

در این مطالعه، جایگزینی ساده‌تر و شفاف‌تر برای مولد اعلان تحت عنوان مولد اعلان ساده<sup>۱</sup> پیشنهاد می‌شود که ضمن حفظ نقاط قوت اصلی، کاستی‌های آن را نیز برطرف می‌سازد. با ساده‌سازی چارچوب تکاملی بهینه‌سازی دستورات، روش پیشنهادی، ضمن کاهش پیچیدگی، قابلیت تفسیر و مقیاس‌پذیری را نیز بهبود می‌بخشد (همان‌طور که در شکل ۱-۳ نشان داده شده است). این رویکرد در تلاش است تا تولید خودکار دستورات را کاربردی‌تر و در دسترس‌تر سازد.

مولد اعلان ساده به صورت تکرارشونده دستورات را بررسی می‌کند و با بهره‌گیری مستقیم از یک مدل احتمالاتی به نام فرآیندهای نقطه‌ای دترمینانی، به بهینه‌سازی تنوع و کیفیت آن‌ها می‌پردازد. مدل‌های

<sup>۱</sup> صفحه ۷ مقاله مولد اعلان: «توجه داشته باشید که ما به مدل زبانی 'دروغ' گفته‌ایم و بیان کرده‌ایم که ترتیب نزولی است.»

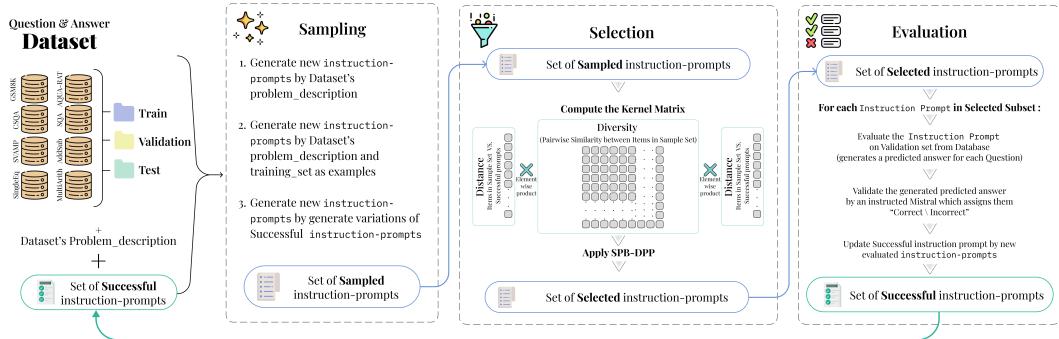
<sup>۲</sup> SimplePromptBreeder



شکل ۱-۳ مقایسه پیجیدگی محاسباتی روش مولد اعلان و روش مولد اعلان ساده

احتمالی فرآیندهای نقطه‌ای دترمینانی، به گونه‌ای طراحی شده‌اند که راهکارهای بهینه‌ای برای مسئله انتخاب در فضای دستورات ارائه دهند به گونه‌ای که هم با کیفیت و هم متنوع باشند.

فرضیه تحقیق ما این است که استفاده از فرآیندهای نقطه‌ای دترمینانی می‌تواند تعداد دفعات فراخوانی مدل زبانی بزرگ را برای یافتن دستورات بهینه کاهش داده و در عین حال، سطح عملکرد رقابتی را حفظ نماید. سادگی و ظرفت ریاضی این رویکرد همچنین می‌تواند موجب افزایش استحکام آن در برابر انواع مدل‌های زبانی شود که این روش بر روی آن‌ها اعمال می‌گردد. از طرفی ساختار ریاضی این روش، آن را به جایگزینی عملی و قابل تفسیر برای روش‌های پیچیده تبدیل می‌کند.



شکل ۲-۳ دیاگرام روش مولد اعلان ساده

## ۲-۳ روش مولد اعلان ساده

برای استفاده از مدل‌های زبانی بزرگ با دستورالعمل<sup>۱</sup> مانند Mistral [؟]، لازم است اعلان‌ها در قالب خاصی سازماندهی شوند تا حالت مکالمه‌ای<sup>۲</sup> شبیه‌سازی شود. این قالب بر پایه‌ی ساختار کلید-مقدار<sup>۳</sup> استوار است، که در آن هر کلید، نقش<sup>۴</sup> را مشخص می‌کند و مقدار متناظر، محتوا یا پیام مربوط به آن نقش را شامل می‌شود. سه نقش رایج در این قالب وجود دارد: سیستم، دستیار و کاربر. برای نقش سیستم، محتوا به عنوان دستورالعمل‌هایی برای مدل زبانی عمل می‌کند تا وظایف مشخصی را انجام داده و به اعلان‌های کاربر پاسخ دهد. این دستورالعمل‌ها با عنوان اعلان دستوری<sup>۵</sup> شناخته می‌شوند و تأثیر بسزایی بر کیفیت پاسخ‌های تولید شده توسط مدل دارند.

برای کشف این نوع اعلان‌های دستوری، از یک الگوریتم تکاملی استفاده می‌کند که به طور کارآمد یک جستجوی محلی<sup>۶</sup> را در فضای بینهایت اعلان‌ها انجام می‌دهد.

همان‌طور که در شکل ۲-۳ نشان داده شده است، مولد اعلان ساده یک چرخه سه مرحله‌ای را به صورت

تکراری دنبال می‌کند:

- **نمونه‌گیری<sup>۷</sup>**: مولد اعلان ساده با تولید مجموعه متنوعی از اعلان‌های دستوری شروع می‌کند و اطلاعاتی مانند توصیف وظایف<sup>۸</sup>، مثال‌ها یا تغییرات مبتنی بر اعلان‌های موفق قبلی را در نظر می‌گیرد.

- **انتخاب<sup>۹</sup>**: از میان اعلان‌های تولید شده، مولد اعلان ساده زیرمجموعه‌ای متنوع از اعلان‌های با

<sup>1</sup>instructed LLMs

<sup>2</sup>chat-mode

<sup>3</sup>key-value

<sup>4</sup>role

<sup>5</sup>instruction prompt

<sup>6</sup>Local Search

<sup>7</sup>Sampling

<sup>8</sup>task-description

<sup>9</sup>Selection

کیفیت را انتخاب می‌کند، به گونه‌ای که هم شباخت به اعلان‌های موفق قبلی حفظ شود و هم تنوع میان اعلان‌های انتخاب شده رعایت گردد.

- **ارزیابی<sup>۱</sup>** : اعلان‌های انتخاب شده بر روی یک مجموعه داده کوچک ارزیابی می‌شوند و بهترین‌ها به مجموعه نامزدها<sup>۲</sup> افزوده می‌شوند. این مجموعه به صورت تکراری بهروز شده و روند انتخاب در آینده را هدایت می‌کند.

در طول چندین تکرار<sup>۳</sup>، مولد اعلان ساده اعلان‌های موجود در مجموعه نامزدها را پالایش می‌کند تا اطمینان حاصل شود که این اعلان‌ها مؤثر و متناسب با وظیفه مورد نظر هستند.

---

### الگوریتم ۱ - ۳ مولد اعلان ساده

---

**Input:**

**problem\_description:** A description of the problem domain.

**epochs:** Number of epochs to repeat the searching method.

**C\_size:** Maximum size of the candidate set  $C$ .

**DPP\_selection\_size:** Number of prompts selected by DPP.

**Dataset:** A dataset of Q&A pairs relevant to the problem domain.

**Output:**  $C$  (a set of  $k$  best evaluated instruction prompts).

- 1: Initialize  $C \leftarrow \emptyset$  {Start with an empty candidate set}
  - 2: **for** epoch = 1 to epochs **do**
  - 3:   Generate sample set  $S$  from problem\_description and Dataset.training\_data
  - 4:   Select set  $P$  of prompts from  $S$  by SPB-DPP ,  $|P| = DPP\_selection\_size$
  - 5:   Evaluate prompts in  $P$
  - 6:   Merge  $P$  with  $C$
  - 7:   Select the  $k$  best prompts from  $C$  and set them as  $C$  for the next epoch
  - 8: **end for**
  - 9: **Return**  $C$  {Set of  $k$  best evaluated prompts}
- 

### ۱ - ۲ - ۳ نمونه‌گیری

مرحله نمونه‌گیری مشابه فرآیند ساختن جمعیت اولیه<sup>۴</sup> در الگوریتم‌های تکاملی عمل می‌کند. در این مرحله، مجموعه‌ای از دستورالعمل‌های اولیه بالقوه بر اساس توصیف مسئله، جفت‌های پرسش و پاسخ موجود در مجموعه داده به عنوان نمونه، و همچنین دستورالعمل‌های موفق استخراج شده از تکرارهای قبلی الگوریتم تولید می‌گردد.

هر مجموعه داده دارای توصیف مسئله مشخصی است که در جدول ۱ - ۳ آورده شده‌اند.

<sup>1</sup>Evaluation

<sup>2</sup>Candidate Set

<sup>3</sup>epoch

<sup>4</sup>initialization

توصیف مسئله	مجموعه داده
Solve the math word problem, giving your answer as an arabic numeral.	SVAMP, SINGLEEQ, ADDSUB, GSM8K, MULTIARITH
Solve the multiple choice math word problem, choosing (A),(B),(C),(D) or (E).	AQUA-RAT
Solve the multiple choice math word problem, choosing (A),(B),(C),(D) or (E).	CSQA
Work out an answer to the commonsense reasoning question above, and then answer yes or no.	SQA

جدول ۳ - ۱ توصیف مسئله برای مجموعه داده های مختلف

نخستین رویکرد نمونه‌گیری برگرفته از روش یادگیری بدون نمونه [؟] است که در آن نمونه‌ای صریح از مجموعه داده در متن اعلان ارائه نمی‌شود و تولید پاسخ صرفاً مبتنی بر توصیف مسئله انجام می‌پذیرد. به عنوان مثال، در مجموعه داده GSM8K توصیف مسئله به صورت زیر بیان شده است: ”مسئله کلمه‌ای ریاضی را حل کن و پاسخ را به صورت یک عدد عربی ارائه بده.“ <sup>۱</sup> در رویکرد دوم نمونه‌گیری، علاوه بر توصیف مسئله، از چندین پرسش و پاسخ به عنوان مثال‌هایی از خروجی مورد انتظار استفاده می‌شود که در روش مولد اعلان ساده این تعداد ۵ عدد است. این رویکرد مبتنی بر یادگیری با نمونه‌های کم [؟] بوده و با ارائه نمونه‌هایی از خروجی مورد انتظار، به مدل زبانی کمک می‌کند تا درک دقیق‌تری از ماهیت مسئله داشته باشد. به کارگیری این نمونه‌ها موجب تولید دستورالعمل‌های اولیه مرتبط‌تر و متناسب‌تر با مسئله خواهد شد.

در نهایت، در سومین رویکرد نمونه‌گیری، به مدل زبانی دستور داده می‌شود تا با استفاده از دستورالعمل‌های موفق و ارزیابی شده از تکرارهای پیشین، که به عنوان مجموعه کاندیدا شناخته می‌شوند، تغییرات و نسخه‌های جدیدی از این دستورالعمل‌ها تولید نماید.

در مجموع، بهره‌گیری از این سه رویکرد نمونه‌گیری منجر به ایجاد مجموعه‌ای متنوع و جامع از دستورالعمل‌های اولیه بالقوه می‌گردد. جزئیات بیشتر در خصوص این سه رویکرد نمونه‌گیری در ضمیمه B: دستورالعمل‌های اولیه برای سه رویکرد نمونه‌گیری ارائه شده است.

## ۲-۲-۳ انتخاب

تعیین دقت یک دستورالعمل مستلزم محاسبات قابل توجهی است، چرا که برای ارزیابی، لازم است هر دستورالعمل بر روی مجموعه آزمون اجرا شود. از این رو، ضروری است تا زیرمجموعه‌ای از دستورالعمل‌های نمونه‌گیری شده از مرحله قبلی، که دارای بیشترین پتانسیل هستند، برای ارزیابی انتخاب شوند. این زیرمجموعه

<sup>۱</sup>Solve the math word problem, giving your answer as an arabic numeral.

باید متنوع باشد تا امکان کاوش بیشتر فراهم شود و در عین حال به دستورالعمل‌های موفق پیشین و مجموعه کاندید نزدیک باقی بماند. یک روش ساده نظیر انتخاب صرفاً دستورالعمل‌هایی با بیشترین دقت، منجر به کاهش تنوع و همگرایی سریع به سمت بهینه محلی خواهد شد. برای مقابله با این مشکل، روش مولد اعلان ساده از مدل احتمالاتی فرآیندهای نقطه‌ای دترمینانی بهره می‌گیرد.

**مدل فرآیندهای نقطه‌ای دترمینانی** [۱۰] ، مدل‌های احتمالی هستند که برای انتخاب زیرمجموعه‌هایی متنوع و در عین حال مرتبط از یک مجموعه بزرگ‌تر طراحی شده‌اند. این مدل‌ها در ابتدا برای فیزیک کوانتم توسعه یافته‌اند، اما بعداً در مسائل یادگیری ماشین نظیر خلاصه‌سازی اسناد، سیستم‌های توصیه‌گر، انتخاب ویژگی و انتخاب زیرمجموعه‌های داده به کار گرفته شده‌اند [۱۱]. نکته مشترک در این کاربردها، بهینه‌سازی همزمان دو معیار تنوع<sup>۱</sup> و کیفیت<sup>۲</sup> است. در فرآیندهای نقطه‌ای دترمینانی، یک ماتریس کرنل<sup>۳</sup> نیمه مثبت معین<sup>۴</sup>  $L$  تعریف می‌شود، که هر درایه  $L_{ij}$  میزان شباهت<sup>۵</sup> بین عناصر<sup>۶</sup>  $i$  و  $j$  را نشان می‌دهد. احتمال انتخاب زیرمجموعه‌ای  $Y \subseteq S$ ، که  $Y$  مجموعه اصلی است، متناسب با دترمینان زیرماتریس  $L_S$  خواهد بود، که متناظر با سطرها و ستون‌های شاخص‌گذاری شده توسط  $S$  است:

$$P(S) \propto \det(L_S) \quad (1-3)$$

در این روش، دترمینان به عنوان معیار تنوع عمل می‌کند و زیرمجموعه‌هایی با عناصر نامشابه‌تر را ترجیح می‌دهد. به طور شهودی، زیرمجموعه‌هایی با عناصر نامشابه‌تر دارای دترمینان بزرگ‌تری هستند، چرا که بردارهای متعامد<sup>۷</sup> یا تقریباً متعامد<sup>۸</sup> در ماتریس کرنل، به دترمینان بزرگ‌تری منجر می‌شوند.

**مدل فرآیندهای نقطه‌ای دترمینانی شرطی** ، مدلی احتمالی است که به زیرمجموعه‌ای از آیتم‌ها، با توجه به ورودی یا قیودی مشخص، احتمال تخصیص می‌دهد. در روش مولد اعلان ساده، فرآیندهای نقطه‌ای دترمینانی شرطی توازن میان کیفیت (برحسب شباهت به دستورالعمل‌های موفق) و تنوع (برحسب عدم شباهت بین اعضاء زیرمجموعه) را برقرار می‌سازد.

به زبان ریاضی، احتمال انتخاب زیرمجموعه  $Y$  از مجموعه اصلی  $(X)$  با توجه به ورودی  $X$  متناسب با دترمینان یک ماتریس کرنل نیمه مثبت معین  $(L_Y(X))$  خواهد بود.

---

فرض کنید  $\mathcal{X}$  فضای ورودی (مثلاً مجموعه نمونه‌ها) و  $(X)$  مجموعه آیتم‌ها با توجه به ورودی  $X$

<sup>1</sup>Diversity

<sup>2</sup>Quality

<sup>3</sup>Kernel Matrix

<sup>4</sup>Positive semi-definit

<sup>5</sup>Similarity

<sup>6</sup>orthogonal

<sup>7</sup>near-orthogonal

(مثلاً مجموعه دستورالعمل‌های نمونه‌گیری شده) باشد. تعریف رسمی به صورت زیر خواهد بود:  
**تعریف:** یک فرآیندهای نقطه‌ای دترمینانی شرطی به صورت  $P(\mathbf{Y} = Y|X)$  مدلی احتمالاتی است که به هر زیرمجموعه ممکن  $Y \subseteq \mathcal{Y}(X)$  احتمال تخصیص می‌دهد و به صورت زیر تعریف می‌شود:

$$P(\mathbf{Y} = Y|X) \propto \det(L_Y(X)), \quad (2-3)$$

که در آن  $L_Y(X)$  ماتریس کرنل نیمه مثبت معینی با ابعاد  $|\mathcal{Y}(X)| \times |\mathcal{Y}(X)|$  و وابسته به  $X$  است.  
ثابت نرمال‌سازی فرآیندهای نقطه‌ای دترمینانی شرطی به صورت کارآمد با رابطه  $\det(L(X) + I)$  محاسبه می‌شود. اگر تنوع برابر  $\phi$  و کیفیت برابر  $q$  باشد، با استفاده از تجزیه کیفیت-تنوع، خواهیم داشت:

$$L_{ij}(X) = q_i(X)\phi_i(X)^T\phi_j(X)q_j(X) \quad (3-3)$$

که در آن  $\phi_i(X) \in \mathbb{R}^D$  و  $q_i(X) \in \mathbb{R}^+$  تعیین شده‌اند و هر دو به  $X$  وابسته هستند.

روش مولد اعلان ساده، تجزیه‌ای از فرآیندهای نقطه‌ای دترمینانی شرطی به کار گرفته است که به طور صریح توازن میان تنوع و کیفیت آیتم‌ها را نشان می‌دهد. برای این منظور، ساخت ماتریس کرنل بر مبنای دو مؤلفه کیفیت و تنوع انجام می‌شود. پارامتر تنوع از طریق شباهت زوجی میان دستورالعمل‌های موجود در مجموعه نمونه<sup>۱</sup> با نام  $\Phi$  از ابعاد  $n \times n$  سنجیده می‌شود. برای محاسبه  $\Phi$ ، ابتدا یک ماتریس صفر از ابعاد  $n \times n$  ایجاد می‌شود و سپس برای هر جفت از دستورالعمل‌ها  $(p_i, p_j)$  در مجموعه transformer sentence  $S = \{p_1, p_2, \dots, p_n\}$  استخراج می‌شوند. سپس شباهت کسینوسی بین  $e_i$  و  $e_j$  مطابق رابطه زیر محاسبه می‌شود:

$$\text{similarity}(e_i, e_j) = \frac{\sum_{k=1}^d e_i^k \cdot e_j^k}{\sqrt{\sum_{k=1}^d (e_i^k)^2} \cdot \sqrt{\sum_{k=1}^d (e_j^k)^2}} \quad (4-3)$$

که در آن  $d$  ابعاد بردارهای عددی است. در نهایت:

$$\Phi[i][j] = \text{similarity}(e_i, e_j) \quad (5-3)$$

---

<sup>1</sup> Sample set

از طرف دیگر، ماتریس  $Q_d$  که نشان دهنده پارامتر کیفیت است، از ابعاد  $1 \times n$  است که فاصله هر دستورالعمل  $s_{ik}$  را از مجموعه دستورالعمل های موفق  $S_{success}$  می سنجد. فرآیند محاسبه  $Q_d$  با محاسبه شباهت کسینوسی بین هر  $p_j \in S_{success}$  و هر  $p_i \in S$  با استفاده از رابطه ۴-۳ آغاز می شود. سپس:

$$\mu_i = \frac{1}{m} \sum_{k=1}^m s_{ik} \quad (6-3)$$

و انحرافات مثبت از میانگین محاسبه می گردد:

$$s'_{ik} = \max(0, s_{ik} - \mu_i) \quad (7-3)$$

که سپس با تابع softmax نرمال سازی می شود:

$$w_{ik} = \frac{\exp(s'_{ik})}{\sum_{j=1}^m \exp(s'_{ij})}. \quad (8-3)$$

وزن نهایی هر دستورالعمل  $p_i$  به صورت زیر محاسبه می شود:

$$W_i = \sum_{k=1}^m w_{ik} \quad (9-3)$$

و در درایه  $i$  ام قطر اصلی  $Q_d$  قرار می گیرد.  
در نهایت، این روش ماتریس کرنل را به صورت زیر می سازد:

$$L = Q_d \otimes \Phi \otimes Q_d \quad (10-3)$$

که در آن نماد  $\otimes$  به معنای ضرب عنصر به عنصر<sup>۱</sup> است. سپس، از این ماتریس در فرآیندهای نقطه ای دترمینانی برای انتخاب زیرمجموعه بهینه از نظر تنوع و کیفیت استفاده می شود. در این فرآیند، زیرمجموعه هایی که نقاط انتخابی آنها پراکندگی بیشتری دارند احتمال بالاتری خواهند داشت.

---

<sup>1</sup> element-wise product

### ۳-۲-۳ ارزیابی

برای ارزیابی<sup>۱</sup> از معیار دقت<sup>۲</sup> استفاده شده است. برای بدست آوردن دقت اعلان های زیرمجموعه<sup>۳</sup> انتخاب شده توسط فرآیندهای نقطه ای دترمینانی ، زیرمجموعه ای شامل ۱۰۰ جفت پرسش و پاسخ از هر مجموعه داده به عنوان مجموعه اعتبارسنجی<sup>۴</sup> مورد استفاده قرار می گیرد. هر دستور آموزشی در زیرمجموعه انتخاب شده برای هدایت مدل زبانی بزرگ به کار می رود. سپس این مدل زبانی هدایت شده، برای هر پرسش در مجموعه اعتبارسنجی، پاسخ هایی تولید می کند که به آنها پاسخ های پیش بینی شده گفته می شود. این پاسخ های پیش بینی شده سپس نیاز به اعتبارسنجی دارند. برای اعتبارسنجی، از رویکردی تحت عنوان مدل زبانی به عنوان داور<sup>۵</sup> استفاده می کنیم که در آن، پاسخ پیش بینی شده با پاسخ واقعی مقایسه می شود. ما از مدل Mistral به عنوان داور استفاده می کنیم.

جريان کلی این فرآیند در شکل ۳-۳ با استفاده از نمونه ای از مجموعه داده GSM8K نشان داده شده است. همانطور که دیده می شود، پس از ارزیابی دستورات آموزشی انتخاب شده، آنها با دستورات آموزشی موفق از آخرین دوره آموزشی ادغام می شوند. علاوه بر این، بهترین دستورات آموزشی برتر ( $k$  مورد بر اساس دقت آزمایشی) به عنوان دستورات آموزشی موفق جدید انتخاب می شوند تا در تکرار های بعدی الگوریتم مورد استفاده قرار گیرند. مقدار  $k$  در روش مولد اعلان ساده برابر ۱۰ است، این مقدار با آزمون و خطای مختلف بدست آمده است.

<sup>1</sup>Evaluation

<sup>2</sup>Accuracy

<sup>3</sup>Validation set

<sup>4</sup>LLM-as-a-Judge

For each **INSTRUCTION-PROMPT** on GSM8K dataset :



#### Guidelines

- Understand the Task: Use the problem\_description to understand the overall goal. Supplement this understanding with the two provided examples to clarify the problem's scope.
- ⋮

#### Edge Cases:

- Handle problems that involve multiple types of operations (e.g., addition, subtraction, multiplication, and division).
- Handle problems that require rounding or estimating values.
- Handle problems that involve fractions or decimals.

Ask all questions in validation set from the instructed Mistral

GSM8K



Validation set

**Question:** Every day, Wendi feeds each of her chickens three cups of mixed chicken feed, containing seeds, mealworms and vegetables to help keep them healthy. She gives the chickens their feed in three separate meals. In the morning, she gives her flock of chickens 15 cups of feed. In the afternoon, she gives her chickens another 25 cups of feed. How many cups of feed does she need to give her chickens in the final meal of the day if the size of Wendi's flock is 20 chickens?

**Answer:** 20

Analyze the problem\_description

⋮

#### Solution:

- Calculate the total amount of feed given so far by adding the amount of feed given in the morning and afternoon ( $15 + 25 = 40$  cups).
- Determine the amount of feed each chicken has received so far by dividing the total amount of feed given so far by the number of chickens ( $40 / 20 = 2$  cups per chicken).
- Calculate the amount of feed needed for the final meal by subtracting the amount of feed each chicken has received so far from the amount of feed each chicken needs in a day ( $3 - 2 = 1$  cup per chicken).
- Multiply the amount of feed needed for the final meal by the number of chickens ( $1 * 20 = 20$  cups).
- The final meal of the day requires 20 cups of feed.



Evaluate the this answers with evaluation instructed Mistral



By the provided information, Task:

- Compare the Predicted Answer with the Actual Answer.
- Determine if the Predicted Answer matches the Actual Answer exactly.
- Output "CORRECT" if the answers match, otherwise output "INCORRECT".

#### Response Format:

{CORRECT or INCORRECT}



CORRECT

شكل ٣-٣ دیاگرام مرحله ارزیابی روش مولد اعلان ساده

## فصل چهارم: نتایج و بحث

## ۱-۴ مجموعه داده های مورد استفاده

روش مولد اعلان ساده را در مجموعه‌های گسترده از وظایف مرتبط با استدلال حسابی<sup>۱</sup> و استدلال مبتنی بر درک مسئله<sup>۲</sup> مورد ارزیابی قرار داده‌ایم. برای این منظور از هشت مجموعه داده‌ی عمومی، شامل [۱۶] AQuA-RAT ، [۱۵] AddSub ، [۱۴] MultiArith ، [۱۳] SVAMP ، [۱۲] GSM&K [۱۷] SingleEq

به همراه [۱۸] CommonsenseQA و [۱۹] StrategyQA استفاده شده است.

همانطور که در جدول ۱-۴ می‌بینید، روش مولد اعلان ساده با روش‌های زنجیره تفکر، برنامه‌ریزی و حل با اعلان بهبود یافته و بدون آن، مهندس اعلان خودکار و بهینه‌سازی با اعلان‌ها مورد مقایسه قرار گرفته است. بالاترین دقت برای هر مجموعه داده به صورت فونت برجسته مشخص شده است. نتایج مدل زبان PaLM-۰۰۳ text-davinci مستقیماً از مقاله‌ی برنامه‌ریزی و حل [۲۰] استخراج شده و نتایج مدل زبان L-۲ نیز به طور مستقیم از مقاله‌ی مولد اعلان [۹] گرفته شده‌اند. جهت تضمین مقایسه‌ای عادلانه، تمامی روش‌ها با مدل زبانی Mistral ارزیابی شده‌اند و سپس نتایج مقایسه شده است.

Results from	Method	LLM	MultiArith	SingleEq	AddSub	SVAMP	SQA	CSQA	AQuA-RAT	GSM&K
PS ]۲۰[	COT	text-davinci	83.8	88.1	85.3	69.9	63.8	65.2	38.9	56.4
	POT	text-davinci	92.2	91.7	85.1	70.8	-	-	43.9	57.0
	PS	text-davinci	87.2	89.2	88.1	72.0	-	-	42.5	58.2
	PS+	text-davinci	91.8	94.7	92.2	75.7	65.4	71.9	46.0	59.3
PB[۹]	PS	PaLM ۲-L	97.7	90.6	72.4	83.8	50.0	77.9	40.2	59.0
	PS+	PaLM ۲-L	92.5	94.7	74.4	86.3	50.1	73.3	39.4	60.5
	APE	PaLM ۲-L	95.8	82.2	72.2	73.0	38.4	67.3	45.7	77.9
	OPRO	PaLM ۲-L	-	-	-	-	-	-	-	۲.۸۰
	PB	PaLM ۲-L	99.7	96.4	87.8	90.2	71.8	85.4	62.2	83.9
ساده (us) اعلان مولد	CoT	Mistral	79.0	85.0	78.0	64.0	54.0	51.0	33.0	72.0
	PS	Mistral	68.0	91.0	78.0	68.0	61.0	43.0	36.0	66.0
	PS+	Mistral	82.0	84.0	80.0	62.0	44.0	27.0	26.0	60.0
	APE	Mistral	78.0	86.0	84.0	69.0	54.0	51.0	36.0	66.0
	OPRO	Mistral	85.0	84.0	78.0	61.0	53.0	35.0	34.0	67.0
	ساده (ours) اعلان مولد	Mistral	92.0	94.0	89.0	93.0	92.0	91.0	93.0	84.0

جدول ۱-۴ مقایسه دقت روش مولد اعلان ساده با سایر روش‌های موجود

## ۲-۴ متغیرهای روش مولد اعلان ساده

از آنجایی که مولد اعلان ساده یک الگوریتم تکاملی است، این الگوریتم را در بازه ۲۰ تا ۳۰ تکرار<sup>۳</sup> اجرا می‌کنیم؛ تا جایی که در آخرین تکرارها، مجموعه کاندیدا تغییر نخواهد کرد. در هر دوره، جمعیتی متشکل از ۱۵۰ تا ۱۲۰ اعلان دستوری، بسته به مجموعه کاندیدا، تولید می‌شود. همانطور که در فصل قبل گفته شد، این اعلان‌ها بر اساس توضیحات مسئله و یک مجموعه آموزشی شامل ۲۰ سوال و پاسخ از مجموعه داده، نمونه‌گیری می‌شوند. از میان این جمعیت، زیرمجموعه‌ای شامل ۱۰ اعلان دستوری انتخاب شده و

<sup>1</sup> arithmetic reasoning

<sup>2</sup> commonsense reasoning

<sup>3</sup> Epoch

بر روی یک مجموعه اعتبارسنجی که شامل ۲۰ سوال و پاسخ متمایز از مجموعه آموزشی است، ارزیابی می‌گردد.

پس از اتمام تمامی دوره‌ها، اعلان‌های دستوری با بهترین عملکرد بر روی مجموعه‌ای شامل ۱۰۰ سوال و پاسخ که به طور تصادفی از مجموعه داده انتخاب شده و از هر دو مجموعه آموزشی و اعتبارسنجی متمایز می‌باشند، مورد آزمون قرار می‌گیرند.

پارامتر توضیحات مسئله به مجموعه داده بستگی دارد که در جدول ۳-۱ توضیح متناظر با هر مجموعه داده آورده شده است.

در این پژوهش، از مدل زبانی Mistral-VB [؟] برای تولید و آزمون اعلان‌های دستوری استفاده می‌شود. همچنین، به منظور تبدیل اعلان‌های دستوری به بردار عددی، از مدل تبدیل جمله‌ی<sup>۱</sup> bert-base موجود در سایت HuggingFace بهره گرفته شده است.

### ۳-۴ روش‌های مرجع

نتایج روش مولد اعلان ساده با استفاده از پیشرفته‌ترین روش‌های مهندسی که در فصل‌های قبلی به تفصیل توضیح داده شده‌اند، مورد مقایسه قرار گرفته‌اند. به منظور تضمین مقایسه‌ای عادلانه، در صورت امکان، این روش‌ها با استفاده از مدل پایه Mistral مجددًا اجرا شده‌اند زیرا امکان اجرای روش مولد اعلان ساده با مدل‌های ۰۰۳-L PaLM و text-davinci وجود ندارد چرا که این مدل‌ها به صورت عمومی در دسترس نمی‌باشند و روش‌های دسترسی به آن‌ها منسخ شده است. اعلان‌های دستوری این روش‌ها به طور مستقیم از مقاله مولد اعلان استخراج شده‌اند؛ اما اعلان‌های تولید شده توسط مولد اعلان مورد آزمون قرار نگرفته‌اند زیرا آن‌ها به گونه‌ای برای PaLM<sup>۲</sup> بهینه‌سازی شده‌اند که استفاده از آن‌ها در مدل Mistral مقایسه‌ای منصفانه ارائه نخواهد داد.

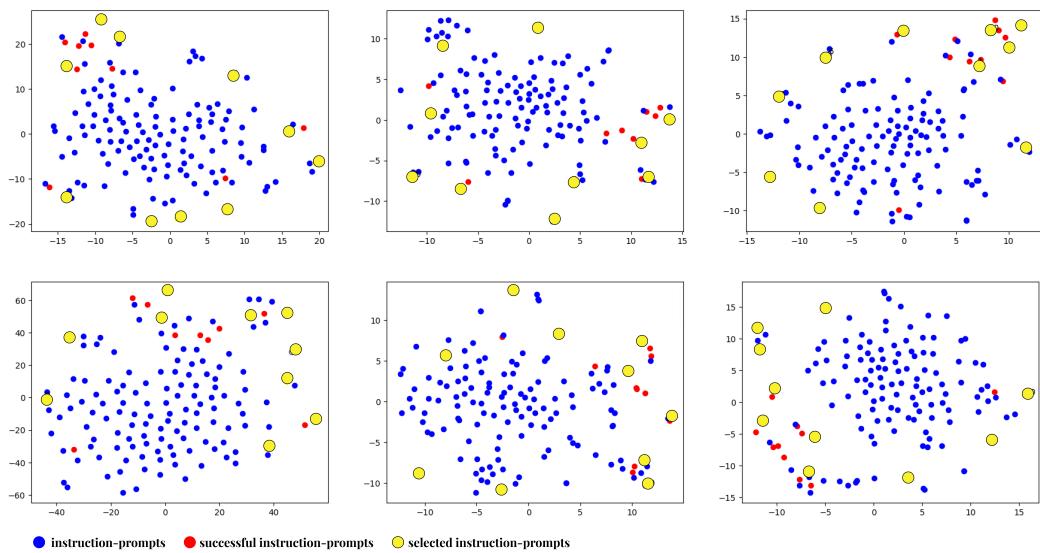
لازم به یادآوری است که برای هر مجموعه داده و هر روش، از دقت به عنوان معیار ارزیابی استفاده شده است.

### ۴-۴ نمایش دوبعدی اعلان‌ها

برای درک بهتر عملکرد مدل احتمالاتی فرآیندهای نقطه‌ای دترمینانسی در طول تکرارها، در شکل ۴-۱ توزیع دو بعدی بردارهای عددی اعلان‌ها را نمایش داده‌ایم. برای کاهش ابعاد این بردارهای عددی، ابتدا از روش کاهش بعد PCA [؟] برای کاهش ابعاد به ۵۰ و سپس از روش t-SNE [؟] برای کاهش بعد به ۲ بعد استفاده کردیم. همانطور که دیده می‌شود، توزیع یکنواخت دستورالعمل‌های انتخاب شده

<sup>1</sup>Sentence Embedding

در نواحی مختلف فضای جستجو نمایش داده شده است که بیانگر توازن میان تنوع و کیفیت در این روش است.



شکل ۱-۴ نمایش دو بعدی بردار اعلان ها برای ارزیابی انتخاب در روش مولد اعلان ساده

## ۵-۴ نتایج

نتایج اجرای روش مولد اعلان ساده بر روی مجموعه داده های مذکور نشان می دهد که این روش از پیشرفته ترین روش های مهندسی برتری دارد. همانطور که در جدول ۱-۴ مشاهده می شود، مولد اعلان ساده در تمامی مجموعه داده ها از سایر روش ها برتر است.

ابتدا عملکرد هر روش را در میان مدل های زبانی مختلف ارزیابی کردیم. مشاهده می شود که اکثر روش ها دقت مشابهی در میان مدل های مختلف دارند، اگرچه بهبودهایی در عملکرد هنگام تغییر از text- مدل ها دیده می شود؛ این بهبودها را می توان به پیشرفت های PaLM 2-L و PaLM 2-L davinci-003 موجود در دقت و ساختار مدل های زبانی نسبت داد.

برای تضمین صحت مقایسه، از روش برنامه ریزی و حل به عنوان نقطه مرجع استفاده شده و بهبود نسبی مولد اعلان و مولد اعلان ساده محاسبه گردیده است. در روش مولد اعلان، با استفاده از فرمول زیر به بهبود نسبی ۲۳.۴٪ نسبت به روش برنامه ریزی و حل در میان مجموعه داده ها دست یافتم:

$$\text{بهبود نسبی مولد اعلان ساده} = \frac{1}{8} \left[ \frac{99.7}{97.7} + \frac{96.4}{90.6} + \frac{87.8}{72.4} + \frac{90.2}{83.8} \right. \\ \left. + \frac{71.8}{50.0} + \frac{85.4}{77.9} + \frac{62.2}{40.2} + \frac{83.9}{59.0} \right],$$

در همین حال، برای مولد اعلان ساده با فرمول زیر، به بهبود نسبی % 54.7 نسبت به روش برنامه‌ریزی و حل در میان مجموعه داده‌ها دست یافتیم:

$$\text{بهبود نسبی مولد اعلان ساده} = \frac{1}{8} \left[ \frac{92.0}{68.0} + \frac{94.0}{91.0} + \frac{89.0}{78.0} + \frac{93.0}{68.0} \right. \\ \left. + \frac{92.0}{61.0} + \frac{91.0}{43.0} + \frac{93.0}{36.0} + \frac{84.0}{66.0} \right],$$

#### ۶-۴ سربار محاسباتی

همانطور که در بخش پارامتر های روش مولد اعلان ساده توضیح داده شد، مولد اعلان ساده به‌طور مشابه با مولد اعلان در بازه ۲۰ تا ۳۰ تکرار اجرا می‌شود. در هر تکرار، مولد اعلان ساده جمعیتی متشكل از ۱۰۰ تا ۱۲۰ اعلان دستوری تولید می‌کند که برای هر یک، یک فراخوانی مدل زبانی مورد نیاز است. در مقابل، مولد اعلان با جمعیتی متشكل از ۵۰ واحد عمل می‌کند؛ هر واحد شامل یک جفت اعلان است که منجر به ۱۰۰ فراخوانی مدل زبانی برای تولید آنها می‌شود. در گام بعدی، برای انتخاب و جهش، مولد اعلان از رویکرد ترکیبی جهش و ابرجهش استفاده می‌کند که برای هر آیتم از واحدهای جمعیت، حداقل دو فراخوانی مدل زبانی نیاز دارد. بنابراین، تعداد کل فراخوانی‌های مدل زبانی در این مرحله برای مولد اعلان به صورت زیر محاسبه می‌شود:

$$50 \times 2 \times 2 = 200.$$

در مقابل، مولد اعلان ساده این محاسبات را با استفاده از محاسبات روش DPP انجام می‌دهد و از فراخوانی‌های اضافی مدل زبانی در این گام صرف نظر می‌کند. در انتها، در گام ارزیابی، مولد اعلان کل جمعیت را مورد ارزیابی قرار داده و به هر واحد نمره می‌دهد.

از آنجا که هر واحد در جمعیت مولد اعلان شامل یک جفت اعلان است، ارزیابی ۵ واحد نیازمند:

$$50 \times 2 = 100$$

فراخوانی مدل زبانی می‌باشد. اما مولد اعلان ساده تنها ۱۰ اعلان دستوری از میان ۱۰۰ اعلان برای ارزیابی انتخاب می‌کند و هر اعلان یک فراخوانی مدل زبانی نیاز دارد؛ بنابراین:

$$10 \times 1 = 10.$$

از سوی دیگر، اندازه‌ی مجموعه داده اعتبارسنجی برای مولد اعلان شامل ۱۰۰ جفت سوال و پاسخ است، در حالی که برای مولد اعلان ساده به ۲۰ کاهش یافته است. علاوه بر این، مولد اعلان ساده پس از شناسایی اعلان‌های با عملکرد برتر، گام آزمون را به منظور تضمین مقایسه‌ای منصفانه اضافه می‌کند؛ این گام اعلان‌های انتخاب شده را بر روی مجموعه داده‌ای شامل ۱۰۰ جفت سوال و پاسخ مانند مولد اعلان ارزیابی می‌کند.

تعداد کل فراخوانی‌های مدل زبانی برای مولد اعلان و مولد اعلان ساده در هر دوره به صورت زیر بیان می‌شود:

$$\text{کل فراخوانی‌های مدل زبانی برای مولد اعلان} = 100 + 200 + 100 = 400,$$

$$\text{کل فراخوانی‌های مدل زبانی برای مولد اعلان ساده} = 110 \text{ تا } 120 + 10 = 110 \text{ تا } 130.$$

بنابراین، مولد اعلان ساده سربار محاسباتی را تقریباً به میزان ۳ برابر کاهش می‌دهد.

## ۷-۴ خروجی‌ها

با بررسی خروجی‌های روش مولد اعلان ساده، مشاهده شد که اعلان‌های دستوری با بهترین عملکرد برای هر مجموعه داده، در قالب چارچوبی صریح ساختاربندی شده‌اند. این چارچوب شامل چند بخش است: بخش اول، توضیح مفصل وظیفه می‌باشد که با دقت به تشریح آن می‌پردازد و در برخی موارد شامل دستورالعمل‌هایی است که جنبه‌های مختلف وظیفه را توضیح می‌دهند. بخش دوم این اعلان، مسیر حل مسئله با توضیحات گام به گام جهت رفع مشکلات موجود در حوزه مربوطه است. در مرحله بعد، تعدادی مثال ارائه شده است که به عنوان نمایش نمونه از مجموعه آموزشی با ارائه راه حل کامل و گام به گام، جهت هدایت روند تفکر مدل زبانی به کار رفته‌اند.

برای مثال، اعلان دستوری با بهترین عملکرد برای مجموعه داده MultiArith در ابتدا وظیفه را به‌طور

کامل تعریف می‌کند، سپس پنج مثال به همراه راه حل کامل آن‌ها ارائه می‌دهد و در نهایت، دستورالعمل‌هایی برای حل مسائل در این حوزه بیان می‌نماید. متن کامل این اعلان دستوری در کادر ۴-۷ آورده شده است.

### بهترین اعلان دستوری تولید شده برای مجموعه داده MultiArith

**Task:** Analyze the given math problem, break down the information, and compute the answer step by step. Present the final answer as an Arabic number.

**Examples:**

- . ۱ Understand that April makes \$9 for every rose she sells. Estimate how many roses April started with, then calculate how many roses she ended with, in order to figure out the revenue she generated.
  - Compute the difference between the number of roses April started with and the number of roses she ended with to find the quantity of roses April sold.
  - Multiply the number of roses sold by the cost per rose to determine the earnings incurred.
- . ۲ Understand the scenario in which Megan prepared 68 cupcakes, and her brother, Todd, consumed 32 of them. Find out how many packages Megan can assemble with 6 cupcakes per package.
  - Subtract the number of cupcakes Todd consumed from the total number of cupcakes Megan prepared to determine the remaining amount of uneaten cupcakes.
  - Divide the quantity of uneaten cupcakes by the number of cupcakes needed to make one package to find the number of packages Megan can assemble.
- . ۳ Identify the situation in which Katie organized and counted 9 albums with a consistent number of pictures in each album. Determine the number of pictures in each

album.

- Sum the total number of pictures Katie has to obtain the grand total.

- Divide the grand total by the number of albums to figure out the number of pictures in each album.

.<sup>f</sup> Grasp the details that Tiffany earns 6 points for each treasure she discovers. Figure out the point score Tiffany received from finding treasures on the first and second levels.

- Add the number of treasures Tiffany discovered on the first and second levels to get the sum of treasures found.

- Multiply the total number of treasures by the points per treasure to learn the point score Tiffany attained.

.<sup>d</sup> Recall the situation in which a waiter manages 33 customers. Estimate how many customers the waiter is still serving after some prospective diners left and others joined the restaurant.

- Subtract the number of customers who left from the current number of customers to determine the number of customers still at the restaurant.

- Add the number of new customers who arrived to find the updated number of customers the waiter is currently serving.

### **Instructions:**

.<sup>i</sup> Explore the given problem to recognize the necessary computations needed to derive the solution.

.<sup>r</sup> Break down the problem into more manageable parts for better organization and clarity.

. $\natural$  Calculate the solutions step by step.

. $\diamond$  Deliver the numerical solution.

**فصل پنجم:**

**نتیجه گیری و پیشنهادات آتی**

## ۱-۵ نتیجه‌گیری

در این پژوهش، با هدف ارتقای فرآیند تولید و بهینه‌سازی اعلان‌ها برای مدل‌های زبانی بزرگ، روشی نوین و کم‌هزینه با عنوان مولد اعلان شاده<sup>۱</sup> طراحی و پیاده‌سازی گردید. دلیل اصلی انجام این تحقیق، چالش‌های محاسباتی موجود در روش‌های پیشین نظری مولد اعلان [۹] بود که به سبب پیچیدگی‌های ذاتی خود، در جستجوی فضای وسیع اعلان‌ها با محدودیت‌های جدی مواجه بودند. به همین منظور، تلاش شد تا با ارائه رویکردی مبتنی بر جستجوی محلی، کارایی و بهره‌وری فرآیند بهینه‌سازی اعلان‌ها به شکل محسوسی افزایش یابد.

نتایج حاصل از آزمایش‌ها نشان می‌دهد که روش مولد اعلان شاده، ضمن حفظ دقت مطلوب، توانسته است به میزان قابل توجهی هزینه‌های محاسباتی را در مقایسه با الگوریتم‌های تکاملی مشابه کاهش دهد. این دستاورده، مؤید اثربخشی روش پیشنهادی در تسهیل و تسريع فرآیند مهندسی اعلان در زمینه‌های پژوهشی و کاربردی می‌باشد. به طور کلی، روش مولد اعلان شاده به عنوان ابزاری کارآمد، قادر است به نیازهای پژوهه‌ها و سامانه‌هایی که با محدودیت منابع محاسباتی روبرو هستند، پاسخ موثری ارائه دهد.

## ۲-۵ پیشنهادات آتی

با توجه به نتایج مثبت حاصل از این پژوهش و همچنین چالش‌های موجود در زمینه بهینه‌سازی اعلان‌ها برای مدل‌های زبانی، پیشنهاد می‌شود مسیرهای زیر در مطالعات آتی مورد توجه قرار گیرد:

۱. **گسترش مطالعات بر روی داده‌های گسترده‌تر و متنوع‌تر:** بررسی عملکرد الگوریتم مولد اعلان شاده بر روی مجموعه داده‌هایی با ابعاد و تنوع بیشتر، می‌تواند میزان پایداری و تعمیم‌پذیری این الگوریتم را در محیط‌های عملیاتی واقعی مورد ارزیابی قرار دهد.

۲. **افزودن شاخص‌های تکمیلی برای سنجش کیفیت و تنوع:** در ادامه پژوهش، می‌توان با افزودن معیارهای جدید جهت سنجش تنوع و کیفیت اعلان‌ها، الگوریتم را در برابر خطر همگرایی زودهنگام و تولید اعلان‌های یکنواخت مقاوم‌تر ساخت و توازن مطلوبی میان اکتشاف و بهره‌برداری برقرار نمود.

۳. **سازگاری با معماری‌های نوین مدل‌های زبانی:** با توجه به ظهور معماری‌های نوین در حوزه مدل‌های زبانی نظری معماری‌های مبتنی بر Sparse Attention و یا مدل‌های چندوجهی<sup>۲</sup>، توسعه نسخه‌های بهینه‌شده از مولد اعلان شاده متناسب با این معماری‌ها می‌تواند گامی مؤثر در راستای افزایش انعطاف‌پذیری و قابلیت‌های این الگوریتم باشد.

<sup>1</sup>Simple Prompt Breeder

<sup>2</sup>multimodal

۴. بررسی و پیاده‌سازی سایر روش‌های جستجوی محلی: از آنجا که مولد اعلان شاده ماهیتاً مشابه الگوریتم Hill-Climbing عمل می‌نماید، پیشنهاد می‌شود در مطالعات آتی از رویکردهای جایگزین نظیر Tabu Search یا Simulated Annealing تنوع در فرآیند جستجو، به بهبود کارایی الگوریتم در مسائل بیچیده‌تر منجر شود.

۵. ادغام با رویکردهای مبتنی بر یادگیری تقویتی: به منظور بهبود تدریجی و هدفمند سیاست‌های جستجو، می‌توان مولد اعلان شاده را با الگوریتم‌های یادگیری تقویتی ترکیب نمود و از این طریق، فرآیند بهینه‌سازی اعلان‌ها را با دریافت بازخوردهای پویا از محیط و مدل هدف، هوشمندانه‌تر و اثربخش‌تر ساخت.

در نهایت، نتایج این پژوهش زمینه‌ساز ارائه یک چارچوب توسعه‌پذیر برای بهینه‌سازی اعلان‌ها در مدل‌های زبانی بزرگ بوده و می‌تواند بستر مناسبی برای تحقیقات و کاربردهای آینده در حوزه مهندسی اعلان فراهم آورد.

# كتاب نامه

- [1] Parvez Faruki, Ammar Bharmal, Vijay Laxmi, Vijay Ganmoor, Manoj Singh Gaur, Mauro Conti, and Muttukrishnan Rajarajan. Android security: A survey of issues, malware penetration, and defenses. *IEEE Communications Surveys & Tutorials*, 17(2):998–1022, 2015.
- [2] Deqiang Li, Qi Li, Yanfang Ye, and Shouhuai Xu. Deep learning for android malware defenses: A systematic literature review. *ACM Computing Surveys*, 55(8):1–36, 2023.
- [3] Mohammed K. Alzaylaee, Suleiman Y. Yerima, and Sakir Sezer. A survey on android malware detection using machine learning. *Computers & Security*, 93:101792, 2020.
- [4] Daniel Arp, Michael Spreitzenbarth, Malte Hubner, Hugo Gascon, and Konrad Rieck. Drebin: Efficient and explainable detection of android malware in your pocket. In *Proceedings of the 21st Annual Network and Distributed System Security Symposium (NDSS)*, 2014.
- [5] Kevin Allix, Tegawendé F. Bissyandé, Jacques Klein, and Yves Le Traon. Androzoo: Collecting millions of android apps for the research community. *Proceedings of the 13th International Conference on Mining Software Repositories*, pages 468–471, 2016.
- [6] Ramin Taheri, Reza Javidan, Mohammad Shojafar, Zahra Pooranian, Ali Miri, and Mauro Conti. Cicmaldroid: A comprehensive android malware dataset. *IEEE Access*, 9:161539–161555, 2021.
- [7] Jason Wei, Xuezhi Wang, Dale Schuurmans, Maarten Bosma, Brian Ichter, Fei Xia, Ed Chi, Quoc Le, and Denny Zhou. Chain-of-thought prompting elicits reasoning in large language models. *Advances in Neural Information Processing Systems*, 35:24824–24837, 2022.
- [8] Wenhui Chen, Xueguang Ma, Xuezhi Wang, and William W. Cohen. Program of thoughts prompting: Disentangling computation from reasoning for numerical reasoning tasks. *arXiv preprint*, 2022.
- [9] Chrisantha Fernando, Dylan Banarse, Henryk Michalewski, Simon Osindero, and Tim Rocktäschel. Promptbreeder: Self-referential self-improvement via prompt evolution. *arXiv preprint*, 2023.

- [10] Alex Kulesza and Ben Taskar. k-dpps: Fixed-size determinantal point processes. *International Conference on Machine Learning*, pages 1193–1200, 2011.
- [11] Alex Kulesza and Ben Taskar. Determinantal point processes for machine learning. *Foundations and Trends in Machine Learning*, 5(2-3):123–286, 2012.
- [12] Karl Cobbe, Vineet Kosaraju, Mohammad Bavarian, Mark Chen, Heewoo Jun, Lukasz Kaiser, Matthias Plappert, Jerry Tworek, Jacob Hilton, Reiichiro Nakano, Christopher Hesse, and John Schulman. Training verifiers to solve math word problems. *arXiv preprint*, 2021.
- [13] Arkil Patel, Satwik Bhattacharya, and Navin Goyal. Are nlp models really able to solve simple math word problems? *Conference of the North American Chapter of the Association for Computational Linguistics*, pages 2080–2094, 2021.
- [14] Subhro Roy and Dan Roth. Solving general arithmetic word problems. *Conference on Empirical Methods in Natural Language Processing*, pages 1743–1752, 2015.
- [15] Mohammad Javad Hosseini, Hannaneh Hajishirzi, Oren Etzioni, and Nate Kushman. Learning to solve arithmetic word problems with verb categorization. *Conference on Empirical Methods in Natural Language Processing*, pages 523–533, 2014.
- [16] Wang Ling, Dani Yogatama, Chris Dyer, and Phil Blunsom. Program induction by rationale generation: Learning to solve and explain algebraic word problems. *arXiv preprint*, 2017.
- [17] Rik Koncel-Kedziorski, Hannaneh Hajishirzi, Ali Farhadi, Oren Etzioni, and Siena Dumas Ang. Parsing algebraic word problems into equations. *Transactions of the Association for Computational Linguistics*, 3:585–597, 2015.
- [18] Alon Talmor, Jonathan Herzig, Nicholas Lourie, and Jonathan Berant. Commonsenseqa: A question answering challenge targeting commonsense knowledge. *Conference of the North American Chapter of the Association for Computational Linguistics*, pages 4149–4158, 2019.
- [19] Mohit Iyyer, Jordan Boyd-Graber, Leonardo Claudino, Richard Socher, and Hal Daumé III. A neural network for factoid question answering over paragraphs. *Conference on Empirical Methods in Natural Language Processing*, pages 633–644, 2014.

- [20] Xuezhi Wang, Jason Wei, Dale Schuurmans, Quoc Le, Ed Chi, and Denny Zhou. Self-consistency improves chain of thought reasoning in language models. *arXiv preprint*, 2022.

پیوست‌ها

## توضیحات تکمیلی

## مقدمه

در پیوست در ابتدا، اعلان های دستوری که برای تنظیم کردن مدل زبانی استفاده شده اند، آورده شده اند که شامل سه بخش نمونه‌گیری روش مولد اعلان ساده، ارزیابی روش مولد اعلان ساده و اعلان های دستوری سایر روش ها می‌باشد. سپس اعلان های دستوری تولید شده توسط مولد اعلان ساده برای هر مجموعه داده آورده شده اند.

### اعلان های دستوری برای نمونه‌گیری روش مولد اعلان ساده

در روش مولد اعلان ساده از سه رویکرد برای نمونه‌گیری اعلان های دستوری جدید استفاده کردیم، رویکرد اول نمونه‌گیری براساس توضیح مسئله مربوط به مجموعه داده بود. اعلان دستوری برای این رویکرد در کادر ۲-۵ آورده شده است.

#### اعلان دستوری برای نمونه‌گیری براساس توضیح مسئله

Given a task description, produce a detailed system prompt to guide a language model in completing the task effectively.

#### Guidelines:

- **Understand the Task:** Grasp the core objective, goals, and expected output of the problem as described in the problem description. Identify any implicit requirements or constraints.
- **Minimal Changes:** Since this is a zero-shot approach, use only the information available in the problem description without assuming any additional context or knowledge. Clarify instructions where needed, but avoid adding new elements unless absolutely necessary for comprehension.
- **Reasoning Before Conclusions:** Guide the model to break down the problem step by step before arriving at any conclusions. Structure the prompt to ensure that reasoning is fully explored before the final solution is given.

- Reverse the order if reasoning is provided after conclusions in any sample content. Always start with the reasoning.
- **Clarity and Conciseness:** Make sure that the prompt uses clear, specific language. The instructions should avoid unnecessary complexity or ambiguity.
- **Examples:** Since no examples are provided in a zero-shot context, ensure the problem is fully explained with placeholders for any variables or specifics that may vary.
- **Formatting:** Use markdown for readability. Present steps clearly and in order.
- **Preserve User Content:** Focus entirely on the problem description without bringing in external examples, but structure it logically.

#### **Steps:**

- . ۱ Parse the problem description.
- . ۲ Identify key variables or constraints.
- . ۳ Guide the model to explore reasoning steps (list if applicable).
- . ۴ Ensure any assumptions or logical pathways are clearly outlined.

**Output Format:** The output should be structured as detailed paragraphs or step-by-step instructions, depending on the problem complexity.

**Notes:** Edge cases: Ensure prompts remain flexible for a variety of inputs, even though no examples are provided.

در رویکرد دوم از مدل زبانی خواسته می‌شد که براساس توضیح مسئله و چند نمونه مثال به همراه جواب از مجموعه داده اقدام به تولید اعلان‌های دستوری مناسب کند، اعلان دستوری برای این امر در کادر ۲-۵ آورده شده است.

**Given a problem description and two example Q&A pairs, produce a detailed system prompt to guide a language model in completing the task effectively.**

### Guidelines

- **Understand the Task:** Use the problem description to understand the overall goal. Supplement this understanding with the two provided examples to clarify the problem's scope.
- **Minimal Changes:** Incorporate key elements from the examples into the prompt, while maintaining the structure of the problem description. Only adjust where clarity or better instruction flow is necessary.
- **Reasoning Before Conclusions:** Guide the model to analyze the examples and reasoning patterns within the example Q&As. Ensure that prompts encourage reasoning steps before arriving at final answers.
  - Reverse the reasoning order if necessary to ensure it starts with analysis.
- **Examples:** Highlight the key learning points or steps from each of the two examples. Use placeholders [in brackets] to allow flexibility for future examples.
- **Clarity and Conciseness:** Be specific in what needs to be done, and avoid vague or generalized instructions. Ensure the combination of the problem description and examples provides enough guidance.
- **Formatting:** Use markdown for clear structure, with sections for example-based learning, reasoning, and solution paths.

- **Preserve User Content:** Include both the problem description and examples faithfully, without losing important context.

## Steps

- . ۱ Analyze the problem description.
- . ۲ Examine the example Q&As for patterns in reasoning and solutions.
- . ۳ Synthesize the information to produce a prompt that mirrors the examples while remaining flexible for new problems.

## Output Format

The output should be a structured set of instructions, with examples embedded for illustration. Use a mix of bullet points and paragraphs for clarity.

## Examples

Provide example reasoning paths based on the given Q&A pairs.

## Notes

Edge cases: Address how prompts should handle examples that deviate from common patterns found in the provided examples.

در رویکرد سوم نمونه‌گیری، از مدل زبانی خواسته شد که با الهام از اعلان‌های دستوری موفق، اقدام به تولید اعلان‌های دستوری جدید و مشابه با پرایپت‌های موفق کند، اعلان دستوری مربوط به این رویکرد در کادر ۲-۵ آورده شده است.

اعلان دستوری برای نمونه‌گیری براساس اعلان‌های دستوری موفق

Given a successful prompt, produce variations of the prompt while maintaining the original task's goals and structure.

## Guidelines

- **Understand the Task:** Start by identifying the core objective of the successful prompt. Determine why it was effective in completing the

task and maintain this focus.

- **Minimal Changes:** Focus on slight variations in wording, structure, or approach to maintain effectiveness. Do not change the task's essence or main steps unless necessary for clarity.
- **Reasoning Before Conclusions:** Ensure that all variations continue to follow reasoning-first structures. If the original prompt placed conclusions before reasoning, reverse the order for variations.
- **Clarity and Conciseness:** Variations should remain clear and to the point, without introducing ambiguity or confusion.
- **Examples:** Highlight variations with slight changes in phrasing, while retaining the core elements of the original prompt.
- **Formatting:** Keep formatting consistent across variations. Use bullet points or markdown headings to segment the variations clearly.
- **Preserve User Content:** Maintain the overall flow and details of the successful prompts, making variations in small increments.

## Steps

- . 1 Analyze the successful prompt to identify key elements that make it work.
- . 2 Create multiple variations by adjusting wording, step order, or clarity points.
- . 3 Ensure each variation follows the same reasoning and solution path, with slight differences in phrasing or structure.

## Output Format

Output only one variation in the given prompt form, with minor changes to structure, wording, or instruction flow.

### Notes

Edge cases: Test how different variations might perform across a range of inputs. Identify possible weaknesses in certain phrasing and adjust accordingly.

## ارزیابی

همانطور که در فصل ۳ بخش ارزیابی توضیح داده شد، هر اعلان دستوری تولید شده روی مجموعه داده ارزیابی می‌شود و برای سوال موجود در آن مجموعه داده، پاسخی تولید می‌کند. سپس نیاز است که این پاسخ با پاسخ واقعی مقایسه شود. این مقایسه و ارزیابی توسط مدل زبانی از طریق اعلان دستوری ۲-۵ به عنوان دستورالعمل انجام می‌شود.

### اعلان دستوری برای ارزیابی جواب تولید شده

By the provided information, Task:

- . ۱ Compare the Predicted Answer with the Actual Answer.
- . ۲ Determine if the Predicted Answer matches the Actual Answer exactly.
- . ۳ Output "CORRECT" if the answers match, otherwise output "INCORRECT".

Response Format:

{CORRECT or INCORRECT}

در ادامه یک سوال و جواب از مجموعه داده GSM8K به عنوان مثال و همچنین جواب تولید شده توسط بهترین اعلان دستوری برای بررسی نحوه پاسخدهی مدل زبانی آورده شده است.

**Question:** Henry made two stops during his 60-mile bike trip. He first stopped after 20 miles. His second stop was 15 miles before the end of the trip. How many miles did he travel between his first and second stops?

**Answer:** Henry traveled 20 miles + 15 miles = 20 + 15 = 35 miles, not counting the distance between stops.

Henry traveled 60 miles - 35 miles = 60 - 35 = 25 miles between his first and second stop.

Final Answer : 25

### Predicted-Answer:

#### Analyze the Problem Description:

The problem involves finding the distance traveled between two stops during a bike trip. The initial stop was after 20 miles, and the second stop was 15 miles before the end of the trip.

#### Example-Based Learning:

- Identify the key components of the problem: initial stop distance, final stop distance, and total trip distance.
- Understand the order of operations: find the distance between the two stops first, then subtract this value from the total trip distance to find the distance traveled between the stops.

#### Reasoning:

- Find the distance between the two stops:  $60 - (20 + 15) = 60 - 35 = 25$  miles.
- The distance traveled between the first and second stops is 25 miles.

### Solution Paths:

- Find the distance between the two stops by subtracting the sum of the initial and final stop distances from the total trip distance.
- The distance traveled between the first and second stops is the calculated distance between the two stops.

Example Q&A Pair 1 : Ken created a care package to send to his brother, who was away at boarding school. Ken placed a box on a scale, and then he poured into the box enough jelly beans to bring the weight to 2 pounds. Then, he added enough brownies to cause the weight to triple. Next, he added another 2 pounds of jelly beans. And finally, he added enough gummy worms to double the weight once again. What was the final weight of the box of goodies, in pounds?

Example Q&A Pair 2 : James creates a media empire. He creates a movie for \$2000. Each DVD costs \$6 to make. He sells it for 2.5 times that much. He sells 500 movies a day for 5 days a week. How much profit does he make in 20 weeks?

### Prompt and Example:

Prompt: Given a problem that involves finding the distance traveled between two stops during a trip, solve it by finding the distance between the two stops first, then subtracting this value from the total trip distance to find the distance traveled between the stops.

Example: Henry made two stops during his 60-mile bike trip. He first stopped after 20 miles. His second stop was 15 miles before the end of the trip. How many miles did he travel between his first and second stops?

### Solution:

- Find the distance between the two stops:  $60 - (20 + 15) = 60 - 35 = 25$  miles.
- The distance traveled between the first and second stops is 25 miles.

## سایر روش ها

در جدول ۱، اعلان‌های دستوری به کاررفته برای هدایت مدل زبانی Mistral به‌منظور ایفای نقش به‌عنوان روش‌های زنجیره تفکر، برنامه‌ریزی و حل، برنامه‌ریزی و حل پیشرفته، مهندس اعلان خودکار و بهینه‌سازی با اعلان ارائه شده است. این اعلان‌ها برگرفته از مقاله مولد اعلان [۹] می‌باشند.

Method	Instruction Prompt
CoT	“Let’s think step by step.”
PS	“Let’s first understand the problem and devise a plan to solve the problem. Then, let’s carry out the plan and solve the problem step by step.”
PS+	“Let’s first understand the problem, extract relevant variables and their corresponding numerals, and make a plan. Then, let’s carry out the plan, calculate intermediate variables (pay attention to correct numerical calculation and commonsense), solve the problem step by step, and show the answer.”
APE	“Let’s work this out in a step by step way to be sure we have the right answer.”
OPRO	“Take a deep breath and work on this problem step-by-step.”

جدول ۱ اعلان‌های دستوری برای سایر روش‌ها جهت مقایسه نتایج



دانشگاه شهرکرد

بسمه تعالیٰ

## فرم تایید اطلاعات تولیدات علمی \* مستخرج از پایان نامه دانشجویان کارشناسی ارشد

نام و نام خانوادگی دانشجو: ناهید عبدالالهی کرمانی شماره دانشجویی: ۵۰۰۱۱۵۶۰۴ نام دانشکده: فن مهندسی

رشته و گرایش: مهندسی کامپیوتر - هوش مصنوعی نام استاد راهنمای: دکتر مهدی افخاری

عنوان پایان نامه: خودکارسازی مهندسی اعلان: تولید اعلان های دستوری برای مدل های بزرگ زبانی جهت حل مسائل پردازش زبان طبیعی

مشخصات تولیدات علمی	
دریفت	عنوان تولیدات علمی
مرجح تایید کننده نام کنفرانس/نام مجله	Less is More: Prompt Optimization with SimplePromptBreeder
IJCAI2025	یک

تولیدات علمی فوق با نمره ( عدد ) ۱۵ ( حروف ) یک و پنج دهم ( حداًکثر ۲ نمره ) در ارزیابی پایان نامه قرار گرفت و نمره نهایی پایان نامه فوق با استناد به نمره تولیدات علمی ( عدد ) ( حروف ) چهار برابر باشد.

نام و نام خانوادگی استاد / استادان راهنمای: نام و نام خانوادگی نهاینده هیأت داوران: نام و نام خانوادگی مدیر گروه/ رئیس بخش:

تاریخ: تاریخ: تاریخ:

امضاء: امضاء: امضاء:

\* تولیدات علمی شامل مقاله، اختراع، ساخت دستگاه، انتساب، ثبت اربیلیت هنری می باشد که از پایان نامه استخراج شده باشد.

## Abstract

The performance of large language models (LLMs) relies heavily on prompt engineering. Manual methods such as programming and problem solving have improved the reasoning process to some extent, but they often fall short in ensuring diversity in the generated prompts and limit overall effectiveness. On the other hand, prompt generation methods have overcome this limitation by introducing a self-reflective improvement mechanism. By leveraging a genetic algorithm with a binary tournament selection strategy, they gradually evolve instructional prompts. This algorithm enables the prompt generator to iteratively explore the prompt space while optimizing for both diversity and performance simultaneously. Despite the significant advancements made by prompt generation methods in creating optimal prompts, a new challenge has emerged — the increased computational burden and complexity of these approaches, which makes their practical application difficult in many real-world scenarios. To address these issues, we propose SimplePromptBreeder that utilizes a local search strategy to optimize prompts. This approach employs a probabilistic model called Determinantal Point Processes (DPPs) to select high-quality and diverse prompts, directly balancing performance and diversity without relying on complex self-referential mechanisms.

We evaluated the optimal prompt generation method on eight benchmark datasets: MultiArith, SingleEq, AddSub, SVAMP, SQA, CSQA, AQuA-RAT, and GSM8K, achieving a relative improvement of 23.4% over the problem-and-solve approach and a relative improvement of 54.7% over the PromptBreeder method.

**Keywords:** Large Language Models, Prompt Engineering, Instructional Prompts, Determinantal Point Processes, Diversity, Quality

**Keywords:** Large Language Models, Prompt Engineering, Instructional Prompts, Determinantal Point Processes, Diversity, Quality



**Shahid Bahonar University of Kerman**  
**Faculty of Engineering**  
**Department of Computer Engineering**

---

---

**Robust Android Malware Detection using Transformer Neural Networks**

---

**Prepared by:**  
**Alireza Iranmanesh**

**Supervisor:**  
**Dr. Hamid Mirvaziri**

**A Thesis Submitted as a Partial Fulfillment of the Requirements for the  
Degree of Master of Science in Computer Engineering (M. Sc.)**

**April 2025**