



دانشگاه صنعتی شریف
دانشکده علوم ریاضی

پایان نامه کارشناسی ارشد
ریاضی کاربردی

تحلیل نظریه اطلاعاتی محرمانگی تفاضلی موضعی و کاربردهای آماری آن

نگارش

فیروزه ابریشمی

استاد راهنما

دکتر جواد ابراهیمی بروجنی

۱۴۰۴ اسفند

الله اعلم

به نام خدا

دانشگاه صنعتی شریف

دانشکده علوم ریاضی

پایان نامه کارشناسی ارشد

این پایان نامه به عنوان تحقیق بخشی از شرایط دریافت درجه کارشناسی ارشد است.

عنوان: تحلیل نظریه اطلاعاتی محرمانگی تفاضلی موضعی و کاربردهای آماری آن

نگارش: فیروزه ابریشمی

کمیته ممتحنین

استاد راهنما: دکتر جواد ابراهیمی امضاء:

بروجنی

استاد مشاور: استاد مشاور امضاء:

استاد مدعو: استاد ممتحن امضاء:

تاریخ:



اظهارنامه

(اصالت متن و محتوای پایان نامه کارشناسی ارشد)

عنوان پایان نامه: تحلیل نظریه اطلاعاتی محترمانگی تفاضلی موضعی و کاربردهای آماری آن

استاد مشاور: استاد مشاور

استاد راهنما: دکتر جواد ابراهیمی بروجنی

این جانب فیروزه ابریشمی اظهار می دارد:

۱. متن و نتایج علمی ارائه شده در این پایان نامه اصیل بوده و زیرنظر استادان نام برده شده در بالا تهیه شده است.
۲. متن پایان نامه به این صورت در هیچ جای دیگری منتشر نشده است.
۳. متن و نتایج مندرج در این پایان نامه، حاصل تحقیقات این جانب به عنوان دانشجوی کارشناسی ارشد دانشگاه صنعتی شریف است.
۴. کلیه مطالبی که از منابع دیگر در این پایان نامه مورد استفاده قرار گرفته، با ذکر مرجع مشخص شده است.

نگارنده: فیروزه ابریشمی

تاریخ:

امضاء:

نتایج تحقیقات مندرج در این پایان نامه و دستاوردهای مادی و معنوی ناشی از آن (شامل فرمولها، توابع کتابخانه‌ای، نرم‌افزارها، سخت‌افزارها و مواردی که قابلیت ثبت اختراع دارد) متعلق به دانشگاه صنعتی شریف است. هیچ شخصیت حقیقی یا حقوقی بدون کسب اجازه از دانشگاه صنعتی شریف حق فروش و ادعای مالکیت مادی یا معنوی بر آن یا ثبت اختراق از آن را ندارد. همچنین، کلیه حقوق مربوط به چاپ، تکثیر، نسخه‌برداری، ترجمه، اقتباس و نظائر آن در محیط‌های مختلف اعم از الکترونیکی، مجازی یا فیزیکی برای دانشگاه صنعتی شریف محفوظ است. نقل مطلب با ذکر مأخذ بلامانع است.

نگارنده: فیروزه ابریشمی

تاریخ:

امضاء:

استاد راهنما: دکتر جواد ابراهیمی بروجنی

تاریخ:

امضاء:

چکیده

کلیدواژه‌ها:

اول

فهرست مطالب

۱	مقدمه	۱
۲	۱-۱ اهمیت داده‌ها و ضرورت حفظ حریم خصوصی	۲
۴	۱-۱-۱ محرمانگی تفاضلی (Differential Privacy)	۴
۷	۱-۱-۲ محرمانگی تفاضلی موضعی (Local Differential Privacy)	۷
۸	۲-۱ کارهای پیشین و مرور ادبیات	۸
۸	۲-۱-۱ آغازگرها: از پیمایش‌های آماری تا تعریف مدرن محرمانگی	۸
۱۲	۲-۱-۲ دسته‌بندی پروتکل‌های موضعی: تعاملی و غیرتعاملی	۱۲
۱۳	۳-۱ چالش سودمندی و موازنۀ دقت-محرمانگی	۱۳
۱۳	۴-۱ نگاهی آماری به LDP: چارچوب مینی‌مکس و حدود بنیادین	۱۳
۱۵	۱-۱ بیان مسئله و اهداف پژوهش	۱۵
۱۵	۱-۱-۱ رویکرد تحلیل: f -واگرایی‌ها به عنوان زبان مشترک	۱۵
۱۶	۱-۱-۲ رویکرد تحلیل: چارچوب انقباض f -واگرایی‌ها	۱۶
۱۶	۱-۲-۱ اهداف و ساختار پژوهش	۱۶
۱۷	۱-۲-۲ ساختار پایان‌نامه	۱۷
۱۹	۲ پیش‌نیازها	۱۹
۱۹	۱-۱ محرمانگی تفاضلی مرکز (CDP)	۱۹
۱۹	۱-۱-۲ مدل اعتماد و تعریف رسمی	۱۹

۲۲	۲-۱-۲ تفسیر پارامترهای محramانگی
۲۲	۳-۱-۲ تعاریف معادل و صورت بندی های جایگزین
۲۳	۴-۱-۲ مکانیزم های پایه
۲۵	۵-۱-۲ مکانیزم های بنیادی محramانگی تفاضلی
۲۹	۶-۱-۲ ترکیب پذیری
۲۹	۷-۱-۲ محramانگی گروهی
۳۰	۸-۱-۲ محدودیت مدل مرکز
۳۰	f	۲-۲ واگرایی ها
۳۰	۱-۲-۲ تعریف رسمی در فضای اندازه پذیر
۳۲	۲-۲-۲ نمونه های مهم و توابع مولد
۳۴	۳-۲-۲ خواص بنیادین و روابط بین f-واگرایی ها
۳۶	۳-۲ مبانی آماری و کران های اطلاعاتی
۳۶	۱	۲-۳-۲ نظریه تصمیم و ریسک مینی مکس
۳۷	۲-۳-۲ تقلیل به آزمون فرض (روش بسته بندی)
۳۸	۳-۳-۲ نامساوی های کران پایین
۴۰	۳ محramانگی تفاضلی موضعی
۴۰	۱	۱-۳ مقدمه
۴۰	۲	۲-۳ تعاریف رسمی و مدل های محاسباتی
۴۱	۱	۱-۲-۳ تعریف ریاضی LDP
۴۲	۲	۲-۲-۳ محramانگی تقریبی
۴۲	۳	۳-۳ پروتکل های تعاملی و خواص ترکیب
۴۲	۱	۱-۳-۳ پروتکل های غیر تعاملی
۴۲	۲	۲-۳-۳ پروتکل های تعاملی (ترتیبی)
۴۳	۳	۳-۳-۳ قضیه ترکیب ترتیبی

۴۴	۴-۳ مکانیزم‌های پایه در LDP
۴۴	۱-۴-۳ پاسخ تصادفی دودویی (RR)
۴۶	۲-۴-۳ پاسخ تصادفی تعیین‌یافته (GRR)
۴۶	۳-۴-۳ مکانیزم‌های مبتنی بر کدگذاری یگانی (UE)
۴۸	۴-۴-۳ تحلیل مقایسه‌ای: چرا GRR در ابعاد بالا شکست می‌خورد؟
۴۹	۵-۴-۳ مکانیزم لاپلاس موضعی
۵۱	۵-۳ چالش سودمندی و هزینه عدم اعتماد
۵۱	۱-۵-۳ تعریف مسئله: تخمین میانگین دودویی
۵۲	۲-۵-۳ تحلیل در مدل مرکز (CDP)
۵۲	۳-۵-۳ تحلیل در مدل موضعی (LDP)
۵۲	۴-۵-۳ نتیجه‌گیری: شکاف کارایی
۵۴	۴ تحلیل‌های مبتنی بر انقباض و نرخ‌های مینی‌مکس
۵۴	۱-۴ مقدمه
۵۴	۲-۴ محramانگی به عنوان انقباض اطلاعاتی
۵۶	۱-۲-۴ انقباض در فاصله واریانس کل
۵۶	۳-۴ تحلیل نرخ‌های مینی‌مکس با استفاده از انقباض
۵۷	۴-۴ مطالعه موردي: تخمین میانگین
۵۷	۵-۴ محدودیت‌های تحلیل کلاسیک
۵۹	۵ همارزی LDP و انقباض E_γ -واگرایی
۵۹	۱-۵ مقدمه و انگیزه
۶۰	۲-۵ معرفی E_γ -واگرایی
۶۰	۱-۲-۵ خواص هندسی
۶۰	۳-۵ قضیه همارزی اصلی

۶۲	۴-۵ بهبود کران‌های انقباض
۶۲	۵-۵ تعمیم به محترمانگی تقریبی $((\alpha, \delta)\text{-LDP})$
۶۳	۶-۵ کاربرد در تخمین توزیع گستته
۶۳	۷-۵ انقباض قوی برای خانواده‌ی f -واگرایی‌ها
۶۳	۱-۷-۵ کران دقیق برای واگرایی کای-دو (χ^2)
۶۴	۲-۷-۵ تعمیم به سایر واگرایی‌ها
۶۵	۸-۵ نامساوی ون‌تریز خصوصی (Private van Trees Inequality)
۶۵	۹-۵ کاربردهای نوین و بهبود نرخ‌ها
۶۷	۶ نتیجه‌گیری
۶۸	مراجع
۷۱	واژه‌نامه
۷۲	آ مطالب تکمیلی

فهرست جداول

فهرست تصاویر

- ۲۰ ۱-۱ مدل محramانگی تفاضلی متتمرکز (CDP) با یک متصدی مورد اعتماد.
- ۲۱ ۱-۳ گذار از مدل متتمرکز به موضوعی؛ نویز به صورت محلی (Local) روی دستگاه کاربر اضافه می‌شود.

فصل ۱

مقدمه

در این بخش به توضیح مسئله‌ی محترمانگی تفاضلی و اهمیت آن می‌پردازیم. سپس ادبیات موضوع را شرح داده و مسئله را بیان می‌کنیم.

۱-۱ اهمیت داده‌ها و ضرورت حفظ حریم خصوصی

در دهه‌های اخیر، جهان شاهد رشد انفجاری در تولید و جمع‌آوری داده‌ها بوده است. پیشرفت‌های چشم‌گیر در فناوری‌های ذخیره‌سازی، محاسبات ابری و اینترنت اشیاء، منجر به انباشت حجم عظیمی از داده‌ها شده است که اغلب تحت عنوان کلان‌داده^۱ شناخته می‌شوند. این داده‌ها سوخت اصلی موتورهای تصمیم‌گیری مدرن و سیستم‌های هوشمند هستند. امروزه، الگوریتم‌های یادگیری ماشین^۲ و تحلیل داده^۳ با بهره‌گیری از این مخازن عظیم اطلاعاتی، قادرند الگوهای پیچیده‌ای را شناسایی کنند که در حوزه‌هایی نظری تشخیص پزشکی، بهینه‌سازی ترافیک شهری، توصیه‌گرهای تجاری و سیاست‌گذاری‌های کلان اقتصادی کاربرد حیاتی دارند.

با این حال، این استفاده‌ی گسترده از داده‌ها، نگرانی‌های جدی و فزاینده‌ای را در خصوص حریم خصوصی^۴ افراد به وجود آورده است. داده‌های خامی که برای آموزش مدل‌های هوشمند یا استخراج آماره‌ها استفاده می‌شوند، اغلب حاوی اطلاعات حساس^۵ و شخصی هستند. تاریخچه‌ی تراکنش‌های مالی، سوابق پزشکی، موقعیت‌های مکانی و حتی الگوهای جستجو در وب، همگی می‌توانند جزئیات دقیقی از زندگی

¹Big Data

²Machine Learning

³Data Analytics

⁴Privacy

⁵Sensitive Information

خصوصی افراد را فاش کنند. بنابراین، یک چالش اساسی شکل می‌گیرد: چگونه می‌توان از سودمندی^۶ آماری داده‌ها بهره برد، بدون آنکه حریم خصوصی مشارکت‌کنندگان در داده‌ها نقض شود؟

در سال‌های ابتدایی عصر اطلاعات، تصور عمومی بر این بود که حذف شناسه‌های صریح^۷ (مانند نام، کد ملی و شماره تلفن) برای محافظت از هویت افراد کافی است. این فرایند که گمنامسازی^۸ نامیده می‌شود، با این فرض انجام می‌شد که داده‌های باقی‌مانده قابلیت ردیابی به فرد خاصی را ندارند. اما پژوهش‌های متعددی نشان داده‌اند که این روش‌های سنتی در برابر حملات بازشناسایی^۹ به شدت آسیب‌پذیر هستند. در این نوع حملات، مهاجم با استفاده از اطلاعات جانبی^{۱۰} یا اتصال پایگاه‌داده‌های مختلف به یکدیگر، موفق به کشف هویت افراد در داده‌های به ظاهر گمنام می‌شود.

چندین رخداد مشهور در دو دهه‌ی گذشته، ناکارآمدی روش‌های سنتی گمنامسازی را اثبات کرده‌اند:

• **داده‌های پزشکی ماساچوست:** در یکی از اولین و مشهورترین موارد، لاتانیا سوئینی نشان داد که می‌توان با ترکیب داده‌های پزشکی گمنامسازی شده (که نام بیماران از آن حذف شده بود) با فهرست عمومی رأی‌دهندگان، هویت افراد را بازشناسایی کرد. او با استفاده از ترکیب تاریخ تولد، جنسیت و کد پستی (که به آن‌ها شبه‌شناسه^{۱۱} می‌گویند)، موفق شد پرونده پزشکی فرماندار وقت ایالت ماساچوست را شناسایی کند [۲۰].

• **مجموعه داده‌ی نتفلیکس^{۱۲}:** شرکت نتفلیکس مجموعه‌ای از امتیازهای کاربران به فیلم‌ها را منتشر کرد که در آن شناسه‌های کاربری با اعداد تصادفی جایگزین شده بودند. پژوهشگران نشان دادند که با استفاده از اطلاعات عمومی موجود در وبسایت IMDb و تطبیق الگوهای امتیازدهی، می‌توان هویت بسیاری از کاربران را با دقت بالا کشف کرد [۱۷].

• **داده‌های جستجوی AOL:** در سال ۲۰۰۶، شرکت AOL تاریخچه‌ی جستجوی هزاران کاربر خود را منتشر کرد. اگرچه نام کاربران حذف شده بود، اما تحلیل محتواهای جستجوها منجر به شناسایی هویت افراد شد (از جمله پرونده مشهور تلما آرنولد) که نشان داد حتی خود داده‌ها نیز می‌توانند به عنوان شناسه عمل کنند [۴].

این شواهد تجربی و نظری نشان می‌دهند که تعاریف هیوریستیک و روش‌های موردنی (مانند حذف ستون‌ها یا مخدوش‌سازی ساده) نمی‌توانند تضمین امنیتی پایداری ارائه دهنند. مهاجمان همواره می‌توانند

⁶Utility

⁷Explicit Identifiers

⁸Anonymization

⁹Re-identification Attacks

¹⁰Auxiliary Information

¹¹Quasi-identifier

¹²Netflix Prize Data

دانش پس زمینه‌ی پیش‌بینی نشده‌ای داشته باشد که مکانیزم‌های سنتی را دور بزند. در نتیجه، نیاز مبرمی به یک چارچوب ریاضی دقیق احساس شد که بتواند حریم خصوصی را به صورت کمی تعریف کرده و تضمین دهد که ریسک افشاء اطلاعات، مستقل از توان محاسباتی یا دانش جانبی مهاجم، همواره محدود باقی می‌ماند. این نیاز، زمینه‌ی را برای ظهور مفهوم محرمانگی تفاضلی فراهم کرد که در بخش‌های آتی به تفصیل به آن خواهیم پرداخت.

۱-۱-۱ محرمانگی تفاضلی (Differential Privacy)

در پاسخ به چالش‌های امنیتی و ناکارآمدی روش‌های سنتی گمنام‌سازی، دُورک و همکاران در سال ۲۰۰۶ مفهوم محرمانگی تفاضلی^{۱۳} را معرفی کردند [۱۰]. این چارچوب ریاضی دقیق، به جای تمرکز بر ویژگی‌های ظاهری داده‌ها (مانند حذف نام‌ها)، بر فرایند تولید خروجی تمرکز دارد و تضمین می‌کند که حضور یا عدم حضور یک فرد خاص در پایگاهداده، تأثیر ناچیزی بر خروجی نهایی الگوریتم داشته باشد.

پیش از آنکه به تعاریف صوری و ریاضی بپردازیم، ضروری است که درک عمیقی از چیستی محرمانگی و تمایز بین این آن با مفاهیم امنیتی کلاسیک پیدا کنیم. بسیاری از سوتفاهم‌ها در این حوزه ناشی از تمایز ندادن دو مفهوم امنیت داده (که قلمرو رمزنگاری^{۱۴} است) و محرمانگی داده (که هدف ماست) می‌باشد. رمزنگاری اساساً سازوکاری برای کنترل دسترسی^{۱۵} است و تضمین می‌کند که تنها افراد مجاز می‌توانند داده‌ها را ببینند؛ اما در برابر نشت اطلاعات از خروجی‌های مجاز سکوت می‌کند. تصور کنید یک پایگاهداده‌ی حساس پزشکی کاملاً رمزنگاری شده باشد و پژوهشگری مجاز، نتیجه‌ی یک تحلیل آماری ساده (مانند میانگین حقوق یا نرخ یک بیماری) را منتشر کند. رمزنگاری هیچ محافظتی در برابر استنتاج‌های ثانویه ارائه نمی‌دهد و مهاجم می‌تواند با ترکیب این خروجی مجاز با دانش پیشین^{۱۶} خود، اطلاعات خصوصی افراد را بازسازی کند. بنابراین، رمزنگاری شرط لازم است، اما برای حفظ محرمانگی کافی نیست؛ چرا که خود نتیجه‌ی تحلیل، حامل اطلاعات است.

در پاسخ به این چالش، دُورک مفهوم محرمانگی را با ایده‌ی امنیت معنایی^{۱۷} پیوند می‌زند. در این دیدگاه، هدف محرمانگی جلوگیری از یادگیری حقایق کلی درباره‌ی جامعه نیست، بلکه هدف محافظت از حقایق خاص مربوط به یک فرد مشخص است. فلسفه‌ی مرکزی این است که نتیجه‌ی هر تحلیلی باید تقریباً یکسان باشد، چه یک فرد خاص در آن مطالعه مشارکت کند و چه نکند. این تعریف، محرمانگی را به مفهوم ریسک گره می‌زند؛ به این معنا که مشارکت در یک پایگاهداده نباید باعث شود ریسک افشاء رازهای یک

¹³Differential Privacy

¹⁴Cryptography

¹⁵Access Control

¹⁶Auxiliary Knowledge

¹⁷Semantic Security

فرد به طور چشمگیری افزایش یابد.

برای مدل‌سازی این مفهوم، می‌توانیم از استعاره‌ی جهان‌های موازی استفاده کنیم. دو پایگاهداده همسایه^{۱۸} (\mathcal{D} و \mathcal{D}') را به عنوان دو جهان موازی در نظر بگیرید که در یکی، داده‌های کاربر x وجود دارد و در دیگری، این داده‌ها حذف یا تغییر یافته‌اند. هدف نهایی این است که از دیدگاه یک ناظر بیرونی (مهاجم)، این دو جهان غیرقابل تفکیک^{۱۹} باشند. اگر مکانیزم محروم‌گی بتواند کاری کند که مهاجم با مشاهده‌ی خروجی، نتواند تشخیص دهد که این خروجی از کدام جهان آمده است، آنگاه حریم خصوصی کاربر x حفظ شده است.

برای رسیدن به این هدف، ما از الگوریتم‌های تصادفی^{۲۰} بهره می‌بریم. این الگوریتم‌ها با تزریق نویز کنترل شده، توزیع خروجی‌ها را بین دو مجموعه‌داده‌ی همسایه چنان به هم نزدیک می‌کنند که تمایز قائل شدن میان آنها از نظر آماری ناممکن می‌شود.

چرا روش‌های قطعی شکست می‌خورند؟

دستیابی به هدف فوق با روش‌های قطعی^{۲۱} ممکن نیست. برای درک بهتر، یک حمله‌ی تفاضلی^{۲۲} کلاسیک را در نظر بگیرید. فرض کنید f تابعی قطعی است که میانگین درآمد n فرد در پایگاهداده را برمی‌گردد:

$$f(\mathcal{D}) = \frac{1}{n} \sum_{i=1}^n x_i$$

۱. میانگین درآمد n نفر حاضر در پایگاهداده (\mathcal{D}) .

۲. میانگین درآمد همان افراد، به جز فرد هدف k .

از آنجا که خروجی بدون نویز است، مهاجم با یک محاسبه‌ی ساده‌ی جبری $(x_k = n \cdot M_1 - (n-1) \cdot M_2)$ مقدار دقیق درآمد فرد k را به دست می‌آورد. این مثال نشان می‌دهد که هر تغییر کوچکی در ورودی یک تابع قطعی، به تغییری مشخص و قابل‌ردیابی در خروجی منجر می‌شود که بلاfacile دو جهان موازی را از هم تمایز می‌کند.

در واقع مثال میانگین را می‌توان به هر تابع قطعی $Z \rightarrow \mathcal{X}^n$: f تعمیم داد. فرض کنید مهاجم به دنبال بازیابی داده‌ی فرد k -ام (x_k) است. اگر سایر داده‌های موجود در پایگاهداده، یعنی $\mathcal{D}_{-k} = \{x_1, \dots, x_{k-1}, x_{k+1}, \dots, x_n\}$

¹⁸Neighboring Datasets

¹⁹Indistinguishable

²⁰Randomized Algorithms

²¹Deterministic

²²Differencing Attack

بدینانه محرمانگی تفاضلی استاندارد است)، تابع خروجی را می‌توان تنها بر حسب متغیر مجهول x_k به صورت $g(x) = f(x, \mathcal{D}_{-k})$ بازنویسی کرد.

اگر تابع g روی دامنه \mathcal{X} یکبهیک^{۲۳} (یا حتی در بازه‌ای مشخص وارونپذیر) باشد، محرمانگی به طور کامل از بین می‌رود؛ زیرا مهاجم با مشاهده خروجی z ، می‌تواند ورودی را به صورت $(z^{-1} = g^{-1}(z))$ بازیابی کند. حتی اگر g کاملاً وارونپذیر نباشد، مشاهده z فضای جستجوی مقادیر ممکن برای x_k را به شدت کاهش می‌دهد:

$$x_k \in \{x \in \mathcal{X} \mid g(x) = z\}$$

از دیدگاه نظریه اطلاعات، مشکل مکانیزم‌های قطعی این است که توزیع احتمال خروجی آن‌ها به ازای یک ورودی مشخص، یک جرم احتمالی^{۲۴} تک نقطه‌ای (تابع دلتای دیراک) است. اگر دو پایگاهداده همسایه‌ی \mathcal{D} و \mathcal{D}' چنان باشند که $f(\mathcal{D}') \neq f(\mathcal{D})$ ، آن‌گاه تکیه‌گاه^{۲۵} توزیع‌های خروجی کاملاً مجزا خواهد بود. در نتیجه، واگرایی کولبک-لایلر^{۲۶} بین آن‌ها بی‌نهایت می‌شود:

$$D_{KL}(\mathcal{M}(\mathcal{D}) \parallel \mathcal{M}(\mathcal{D}')) = \infty$$

این رابطه اثبات می‌کند که هیچ سطح محدودی از محرمانگی ($\infty < \epsilon$) با توابع قطعی غیرثابت قابل دستیابی نیست. بنابراین، همان‌طور که در ادبیات موضوع تأکید شده است [۱۱]، برای شکستن این وابستگی قطعی و ایجاد ابهام آماری، تصادفی‌سازی^{۲۷} در فرآیند مکانیزم الزامی است.

کاربردهای محرمانگی تفاضلی

این چارچوب ریاضی امروزه به استاندارد طلایی در تحلیل داده‌های حساس تبدیل شده و کاربردهای آن فراتر از آمارهای ساده رفته است. برخی از مهم‌ترین کاربردهای آن عبارتند از:

- **تخمین میانگین و مجموع^{۲۸}**: اساسی‌ترین کاربرد DP در محاسبه آماره‌های توصیفی است. سازمان‌های آماری (مانند اداره سرشماری آمریکا) از این روش برای انتشار میانگین درآمد، سن یا جمعیت مناطق استفاده می‌کنند، بدون آنکه داده‌های فردی شهروندان به خطر بیفتند.

- **انتشار هیستوگرام^{۲۹}**: بسیاری از تحلیل‌ها نیازمند دانستن توزیع داده‌ها هستند. DP اجازه می‌دهد

²³Injective

²⁴Probability Mass

²⁵Support

²⁶Kullback-Leibler Divergence

²⁷Randomization

²⁸Mean and Sum Estimation

²⁹Histogram Release

تا تعداد افراد در هر بازه (مثلاً گروههای سنی یا درآمدی) با دقت بالا منتشر شود، در حالی که نویز اضافه شده مانع از شناسایی افراد در گروههای کم جمعیت می‌شود.

• **یادگیری ماشین خصوصی^{۳۰}**: در آموزش مدل‌های عمیق، خطر به خاطر سپاری^{۳۱} داده‌های آموزشی وجود دارد. با استفاده از الگوریتم‌هایی نظیر DP-SGD، می‌توان مدل‌هایی آموزش داد که الگوهای کلی را یاد می‌گیرند اما قادر به بازتولید داده‌های آموزشی حساس (مانند تصاویر چهره یا متون خصوصی) نیستند.

• **سیستم‌های توصیه‌گر و داده‌های مکانی**: شرکت‌های فناوری از DP برای جمع‌آوری آمارهای رفتاری (مانند پربازدیدترین وب‌سایتها یا مکان‌های پرتردد) استفاده می‌کنند تا بدون ردیابی لحظه‌ای کاربران، کیفیت خدمات خود را بهبود بخشد (مانند مکانیزم RAPPOR در گوگل کروم).

این توضیحات، زیربنای اصلی تعاریف ریاضی دقیقی است که در فصل بعد به آن‌ها خواهیم پرداخت.

۲-۱-۱ محرمانگی تفاضلی موضعی (Local Differential Privacy)

اگرچه محرمانگی تفاضلی متمرکز (CDP) استاندارد طلایی حفاظت از داده‌ها محسوب می‌شود، اما پاشنه‌ی آشیل آن در فرضیه‌ی وجود یک متصدی مورد اعتماد^{۳۲} نهفته است که به تمام داده‌های خام دسترسی دارد. این مدل در دنیای واقعی با چالش‌های امنیتی و حقوقی جدی روبروست؛ چرا که تجربه نشان داده است اعتماد کامل به سرورهای مرکزی، حتی در صورت مدیریت توسط نهادهای بزرگ فناوری، همواره در معرض تهدید است. یکی از این خطرات، نفوذ‌های خارجی و سرقت انبوی داده‌هاست؛ به طوری که حتی پیشرفته‌ترین دیوارهای آتش^{۳۳} نیز در برابر حملات پیچیده آسیب‌پذیرند. در چنین شرایطی، اگر داده‌ها به صورت خام ذخیره شده باشند، نشت اطلاعاتی مانند آنچه در واقعه‌ی Equifax رخ داد، مکانیزم‌های محرمانگی تفاضلی مرکزی را عملأً بی‌فایده می‌کند؛ زیرا مهاجم با دور زدن مکانیزم، مستقیماً به مخزن داده‌های حساس دست می‌یابد [۲۱].

علاوه بر تهدیدهای خارجی، خطر سوءاستفاده‌های داخلی توسط کارمندان یا مدیران سیستم با دسترسی‌های سطح بالا نیز وجود دارد که امنیت داده‌ها را نه به ریاضیات، بلکه به اخلاق انسانی گره می‌زنند. از سوی دیگر، محدودیت‌های حقوقی و احصاریه‌های قضایی نیز متصدی را ملزم به افشاء اطلاعات می‌کند. در تمام این سناریوها، مدل متمرکز با یک نقطه شکست مرکزی^{۳۴} روبروست.

³⁰Private Machine Learning

³¹Memorization

³²Trusted Curator

³³Firewalls

³⁴Single Point of Failure

گذار به مدل موضعی، حذف نیاز به اعتماد

بنابراین، تنها راه تضمین قطعی حریم خصوصی، اتخاذ رویکردی است که در آن متصدی اساساً به داده‌های اصلی دسترسی نداشته باشد. این ضرورت، نقطه‌ی عزیمت ما از مدل متمرکز به سمت چارچوب محترمانگی تفاضلی موضعی (LDP) است که در آن فرآیند خصوصی‌سازی پیش از خروج داده از دستگاه کاربر انجام می‌شود.

در این معماری، مرز اعتماد از سرور مرکزی به دستگاه شخصی کاربر (موبایل یا لپ‌تاپ) منتقل می‌شود. پروتکل به گونه‌ای طراحی می‌شود که هیچ‌کس، نه نفوذگران، نه کارمندان کنجهکاو و نه حتی دولت‌ها، هرگز داده‌ی واقعی کاربر را مشاهده نکند. سرور تنها نسخه‌هایی مخدوش و نویزدار از داده‌ها را دریافت می‌کند که به تنها‌ی بی‌معنی هستند، اما در تجمعی با تعداد زیادی داده‌ی دیگر، الگوهای آماری دقیق را آشکار می‌سازند. این رویکرد، خطر نقض حریم خصوصی را بسیار کنترل می‌کند.

۲-۱ کارهای پیشین و مرور ادبیات

۲-۱-۱ آغازگرها: از پیمایش‌های آماری تا تعریف مدرن محترمانگی

اگرچه نگرانی پیرامون محترمانگی داده‌ها قدمتی به اندازه خود آمار دارد، اما فرمول‌بندی ریاضی دقیق آن دستاورد قرن بیست و یکم است. ادبیات کلاسیک این حوزه با تلاش برای کنترل افشاری آماری^{۳۵} آغاز شد، اما ناکارآمدی روش‌های مبتنی بر گمنامسازی در برابر دانش پس‌زمینه مهاجم، نیاز به یک تعریف معنایی قوی‌تر را ایجاد کرد.

نقطه عطف این تحول، معرفی مفهوم محترمانگی تفاضلی^{۳۶} توسط دُورک و همکاران بود [۱۰]. این تعریف، برخلاف روش‌های پیشین که بر ویژگی‌های داده تمرکز داشتند، بر ویژگی‌های مکانیزم پردازش داده تمرکز دارد. در مدل استاندارد (متمرکز)، یک مکانیزم تصادفی M دارای شرایط $\text{DP}-\epsilon$ است اگر برای هر دو پایگاه داده همسایه \mathcal{D} و \mathcal{D}' (که تنها در داده یک فرد متفاوت‌اند) و برای هر زیرمجموعه از خروجی‌ها $\mathcal{S} \subseteq \text{Range}(M)$ رابطه زیر برقرار باشد:

$$\Pr[M(\mathcal{D}) \in \mathcal{S}] \leq e^\epsilon \cdot \Pr[M(\mathcal{D}') \in \mathcal{S}] + \delta \quad (1-1)$$

³⁵Statistical Disclosure Control

³⁶Differential Privacy

که در آن ϵ پارامتری کلیدی به نام بودجه محرمانگی^{۳۷} است و δ احتمال شکست ناچیز مکانیزم را نشان می‌دهد [۱۱]. برای درک شهودی این مفهوم، می‌توان ϵ را به عنوان یک «پیچ تنظیم» برای کنترل توازن میان امنیت و مطلوبیت داده‌ها در نظر گرفت. این پارامتر تعیین می‌کند که خروجی مکانیزم تا چه حد اجازه دارد بین دو جهان موازی (جهانی با حضور داده‌ی شما و جهانی بدون آن) تمایز قائل شود:

- **مقادیر کوچک ϵ (محرمانگی قوی):** زمانی که $\epsilon \rightarrow 0$ ، توزیع‌های خروجی برای دو پایگاهداده همسایه تقریباً بر هم منطبق می‌شوند. در این حالت، مکانیزم مجبور است نویز بسیار زیادی به پاسخ اضافه کند تا تفاوت‌ها را بپوشاند. در نتیجه، مهاجم تقریباً هیچ توانی برای تشخیص حضور فرد ندارد، اما در مقابل، دقت آماری خروجی کاهش می‌یابد.
- **مقادیر بزرگ ϵ (محرمانگی ضعیف):** با افزایش ϵ ، مکانیزم آزادی عمل بیشتری دارد تا خروجی‌های متمایزتری تولید کند (نویز کمتر). این امر دقت تحلیل را افزایش می‌دهد، اما همزمان ریسک بازشناسایی فرد و نشت اطلاعات خصوصی نیز به صورت نمایی بالا می‌رود.

همان‌طور که در بخش قبل توضیح داده شد، پیاده‌سازی این تعریف نیازمند یک پیش‌فرض قوی است: وجود یک متصدی مورد اعتماد که تمام داده‌های خام را جمع‌آوری کرده و نویز را به صورت مرکزی اعمال کند. اما دیدیم که این مدل دارای نقطه ضعف‌هایی است. حذف این فرض و انتقال اعتماد از سرور به کاربر، منجر به شکل‌گیری مفهوم محرمانگی تفاضلی موضعی^{۳۸} (LDP) شد. اگرچه اصطلاح LDP و صورت‌بندی مدرن آن در سال‌های اخیر توسط پژوهشگرانی نظری کاسیسی‌سوانatan و دیگران تدوین شد [۱۵]، اما ریشه‌های عملی آن به دهه‌ها قبل باز می‌گردد.

تعریف ۱-۱ (محرمانگی تفاضلی موضعی (α, δ) -LDP) یک مکانیزم تصادفی $\mathcal{Z} \rightarrow \mathcal{X}$: \mathcal{M} : (تصادفی‌ساز موضعی) شرط «محرمانگی تفاضلی موضعی تقریبی» یا (α, δ) -LDP را برآورده می‌کند، اگر برای تمام جفت ورودی‌های ممکن $x, x' \in \mathcal{X}$ و هر زیرمجموعه‌ی خروجی $\mathcal{Z} \subseteq \mathcal{S}$ ، رابطه زیربرقرار باشد:

$$\Pr[\mathcal{M}(x) \in \mathcal{S}] \leq e^\alpha \cdot \Pr[\mathcal{M}(x') \in \mathcal{S}] + \delta \quad (2-1)$$

در این تعریف:

- α ، بودجه محرمانگی است که میزان شباهت توزیع‌های خروجی را کنترل می‌کند.
- δ ، احتمال ناچیز شکست مکانیزم در برقراری شرط محرمانگی است.

³⁷Privacy Budget

³⁸Local Differential Privacy

اگر $\delta = 0$ باشد، تعریف به حالت استاندارد یا «محرمانگی تفاضلی موضعی خالص» (α -LDP) باز می‌گردد.

مثال‌هایی از مکانیزم و کاربرد LDP

در واقع، ساده‌ترین و نخستین نمونه از یک مکانیزم LDP، روش «پاسخ تصادفی»^{۳۹} است که توسط وارنر در سال ۱۹۶۵ برای حذف سوگیری در نظرسنجی‌های حساس معرفی شد [۲۴]. وارنر این روش را نه برای حفاظت در برابر حملات سایبری، بلکه برای تشویق پاسخ‌دهندگان به صداقت در سوالات حساس (مانند مصرف مواد مخدر یا عقاید سیاسی خاص) طراحی کرد.

سازوکار کلاسیک این روش برای یک پرسش با پاسخ «بله/خیر» به صورت زیر است: فرض کنید از کاربر^{۴۰} خواسته می‌شود که ویژگی حساس $\{X_i \in \{0, 1\}$ را گزارش کند. کاربر به جای پاسخ مستقیم، طبق دستور العمل زیر عمل می‌کند:

۱. یک سکه را پرتاپ می‌کند. (می‌تواند سکه غیرمنصفانه^{۴۰} باشد)

۲. اگر سکه «شیر» آمد، پاسخ واقعی (X_i) را گزارش می‌کند.

۳. اگر سکه «خط» آمد، یک پاسخ تصادفی (با پرتاپ سکه‌ی دوم) تولید و گزارش می‌کند.

در این سناریو، حتی اگر سرور پاسخ «بله» را دریافت کند، با قطعیت نمی‌داند که آیا کاربر واقعاً دارای ویژگی X بوده است (شیر آمده) یا صرفاً به دلیل تصادف (خط آمدن سکه‌ی اول و شیر آمدن سکه‌ی دوم) این پاسخ را ارسال کرده است. با این حال، از آنجایی که احتمالات سکه‌ها مشخص است، سرور می‌تواند با جمع‌آوری تعداد زیادی از پاسخ‌ها (n بسیار بزرگ)، اثر نویز را به صورت آماری حذف کرده و توزیع واقعی جامعه را با خطأ تخمین بزند. به زبان ریاضی مدرن، اگر احتمال گزارش پاسخ واقعی p باشد، نسبت احتمال خروجی‌ها برای دو ورودی متفاوت x و x' به صورت زیر محدود می‌شود:

$$\frac{\Pr[\mathcal{M}(x) = z]}{\Pr[\mathcal{M}(x') = z]} \leq \frac{p}{1-p} \quad (3-1)$$

این رابطه دقیقاً منطبق بر تعریف α -LDP است و نشان می‌دهد که بودجه محرمانگی α چگونه مستقیماً از پارامترهای مکانیزم (p) مشتق می‌شود:

$$e^\alpha = \frac{p}{1-p} \quad \Rightarrow \quad \alpha = \ln\left(\frac{p}{1-p}\right) \quad (4-1)$$

³⁹Randomized Response (RR)

⁴⁰Unfair

این فرمول، تفسیر شهودی LDP را کامل می‌کند:

- اگر $0 / 5 \approx p$ (سکه کاملاً تصادفی)، آنگاه $0 \approx \alpha$ می‌شود. یعنی خروجی هیچ اطلاعاتی از ورودی ندارد (محرمانگی کامل، اما بدون فایده آماری).
- اگر $1 \rightarrow p$ (پاسخ تقریباً همیشه راست)، آنگاه $\infty \rightarrow \alpha$ می‌شود. یعنی داده‌ها دقیق هستند اما هیچ محرمانگی وجود ندارد.

بنابراین، کار وارنر را می‌توان سنگ بنای تاریخی این حوزه دانست که نشان داد چگونه می‌توان بدون اعتماد به گیرنده پیام، و با تنظیم دقیق پارامتر p (و در نتیجه α)، اطلاعات آماری مفیدی را مخابره کرد.

اما پاسخ تصادفی تنها راهکاری برای ایجاد محرمانگی در داده‌های دودویی است، و در کاربردهای مدرن با چالش دامنه‌ی بسیار بزرگ^{۴۱} روبروست. شرکت‌های بزرگ فناوری نیاز دارند داده‌هایی نظری «آدرس‌های اینترنتی بازدید شده» یا «کلمات جدید تایپ شده» را جمع‌آوری کنند که دامنه‌ی آنها^{۴۲} می‌تواند شامل میلیون‌ها حالت باشد. اعمال مستقیم RR در این حالات منجر به نویز بسیار زیاد و کاهش شدید سودمندی می‌شود. در ادامه، راهکارهای اتخاذ شده توسط بزرگ‌ترین شرکت‌های فناوری را مرور می‌کنیم:

- گوگل و پروتکل RAPPOR: در سال ۲۰۱۴، گوگل برای جمع‌آوری آمار تنظیمات مروگر کروم و شناسایی بدافزارها، پروتکل RAPPOR^{۴۳} را معرفی کرد [۲۲]. چالش اصلی گوگل، جمع‌آوری رشته‌های متنهای^{۴۴} بود. راه حل آنها ترکیب پاسخ تصادفی با فیلترهای بلوم^{۴۵} بود. در این روش، داده‌ی ورودی ابتدا به یک بردار بیتی (با استفاده از توابع درهم‌سان) نگاشت می‌شود و سپس پاسخ تصادفی روی تک‌تک بیت‌های این فیلتر اعمال می‌گردد. این معماری به گوگل اجازه داد تا بدون دانستن ورودی دقیق هر کاربر، الگوهای پرتکرار و ناهنجاری‌ها را در مقیاس میلیونی شناسایی کند.
- اپل و جمع‌آوری داده‌های دایره‌لغات: شرکت اپل از LDP برای بهبود کیبورد QuickType، شناسایی ایموجی‌های پرطرفدار و داده‌های سلامت در سیستم عامل‌های iOS و macOS استفاده می‌کند. مسئله‌ی اپل، مخابره‌ی کارآمد داده‌ها با حفظ حریم خصوصی بود. راه حل اپل استفاده از تکنیک‌های مبتنی بر طرح‌ریزی^{۴۶} و تبدیل‌های ریاضی مانند تبدیل هادامارد^{۴۷} است. این تبدیل‌ها به مکانیزم اجازه می‌دهند که اطلاعات را در ابعاد پایین‌تر فشرده کند تا هم بار ارتباطی کاهش یابد و هم واریانس تخمین‌گر در دامنه‌های بزرگ کنترل شود [۲۲].

⁴¹High-Dimensional Domain

⁴²Randomized Aggregatable Privacy-Preserving Ordinal Response

⁴³String

⁴⁴Bloom Filters

⁴⁵Sketching

⁴⁶Hadamard Transform

• مایکروسافت و داده‌های تله‌متري: مایکروسافت برای جمع‌آوری داده‌های تله‌متري ویندوز (مانند مدت زمان استفاده از برنامه‌ها) با چالش تخمين هیستوگرام‌های پیوسته روبرو بود. آن‌ها از مکانیزم‌هایی نظیر نمونه‌برداری هیستوگرام و روش‌های تکرارکننده برای بازسازی توزيع داده‌ها استفاده کردند. تمرکز اصلی در این‌جا، ایجاد تعادل بین دقت آماری در جمع‌آوری داده‌های سیستمی و عدم امکان بازناسایی رفتار یک کاربر خاص در طول زمان است.

این نمونه‌ها نشان می‌دهند که محترمانگی تفاضلی موضوعی (LDP) تنها یک مفهوم نظری نیست، بلکه یک ابزار حیاتی مهندسی است که با استفاده از تکنیک‌های پیشرفته‌ی آماری برای حل مسائل دنیا واقعی مقیاس‌دهی شده است.

۲-۲-۱ دسته‌بندی پروتکل‌های موضوعی: تعاملی و غیرتعاملی

برای بالا بردن دقت کارهای انجام‌شده لازم است به دسته‌بندی پروتکل‌های LDP بر اساس «معماری ارتباطی» اشاره کنیم. پژوهش‌های انجام شده در این حوزه، مکانیزم‌ها را به دو دسته‌ی کلی تقسیم می‌کنند:

۱. پروتکل‌های غیرتعاملی^{۴۷}: در این حالت، تمام کاربران به صورت همزمان و مستقل عمل می‌کنند. هر کاربر i مکانیزم M را تنها بر اساس داده‌ی خودش X_i اجرا کرده و پیام Z_i را به سرور می‌فرستد. هیچ ارتباطی بین کاربران وجود ندارد و سرور نیز هیچ بازخوردی به کاربران نمی‌دهد. به دلیل سادگی پیاده‌سازی و مقیاس‌پذیری بالا، اکثر پروتکل‌های صنعتی (مانند RAPPOR گوگل یا سیستم‌های اپل) در این دسته قرار می‌گیرند.

۲. پروتکل‌های تعاملی^{۴۸}: در این روش، کاربران به صورت متوالی با سرور ارتباط برقرار می‌کنند. کاربر i می‌تواند قبل از ارسال داده‌ی خود، خلاصه‌ای از داده‌های کاربران قبلی (Z_1, \dots, Z_{i-1}) را از سرور دریافت کند و نویز خود را هوشمندانه‌تر تنظیم نماید. اگرچه به نظر می‌رسد این آزادی عمل باید دقت را افزایش دهد، اما دوچی و همکاران در نتایج حیرت‌انگیزی نشان دادند که برای دسته‌ی بزرگی از توابع محدب (مانند تخمین میانگین)، پروتکل‌های تعاملی هیچ مزیتی نسبت به روش‌های غیرتعاملی ندارند و نرخ مینی‌مکس را بهبود نمی‌بخشند [۸، ۱۳].

⁴⁷Non-interactive / Simultaneous

⁴⁸Interactive / Sequential

۳-۲-۱ چالش سودمندی و موازنۀ دقت-محرمانگی

اگرچه حذف متصلی مرکزی در مدل LDP، تضمین‌های امنیتی بسیار قوی‌تری را فراهم می‌کند، اما این امنیت رایگان به دست نمی‌آید. چالش بنیادین در این رویکرد، کاهش چشم‌گیر سودمندی^{۴۹} داده‌ها یا همان دقت تحلیل‌های آماری است. این پدیده تحت عنوان **موازنۀ محرمانگی-دقت**^{۵۰} شناخته می‌شود.

برای درک شهودی این چالش، مقایسه نحوه اعمال نویز در دو مدل ضروری است:

- در مدل متمرکز (CDP): نویز تنها «یکبار» و پس از تجمعی داده‌ها به نتیجهنهایی اضافه می‌شود. از آنجا که مجموع (یا میانگین) داده‌ها حساسیت کمی دارد، مقدار نویز معمولاً مستقل از تعداد کاربران (n) و بسیار کوچک است.
- در مدل موضعی (LDP): نویز باید به «تک‌تک» داده‌های ورودی اضافه شود (پیش از آنکه از دستگاه کاربر خارج شوند). وقتی تحلیل‌گر قصد دارد میانگین این داده‌ها را محاسبه کند، واریانس نویزهای n کاربر با هم جمع می‌شود.

این انباست نویز باعث می‌شود که نسبت سیگنال به نویز^{۵۱} در مدل موضعی بسیار پایین‌تر از مدل متمرکز باشد. به بیان دیگر، برای دستیابی به همان سطح از دقت که در مدل متمرکز وجود دارد، در مدل LDP نیازمند تعداد بسیار بیشتری نمونه داده هستیم.

این مسئله در کاربردهای عملی بسیار حائز اهمیت است. برای مثال، اگر هدف تخمین فراوانی یک بیماری نادر باشد، نویز اضافه شده توسط مکانیزم‌های LDP ممکن است سیگنال اصلی را کاملاً بپوشاند. همین چالش بود که پژوهشگران را بر آن داشت تا به جای استفاده از روش‌های ساده (مثل وارنر)، به دنبال پاسخ این پرسش باشند که: «آیا می‌توان مکانیزم‌هایی طراحی کرد که با کمترین میزان نویز، بیشترین محرمانگی را فراهم کنند؟» و «حد نهایی این دقت کجاست؟» این پرسش‌ها زمینه را برای ورود تئوری‌های پیشرفته‌تر نظری «تخمین مینی‌مکس» فراهم کرد.

۳-۲-۲ نگاهی آماری به LDP: چارچوب مینی‌مکس و حدود بنیادین

پاسخ به پرسش بالا، مسیر پژوهش‌های این حوزه را به سمت نظریه مینی‌مکس آماری^{۵۲} تغییر داد. نقطه عطف این تحول، سلسله مقالات جریان‌ساز دوچی، جردن و وین‌رایت^{۵۳} بود [۸، ۹]. آن‌ها با صورت‌بندی

⁴⁹Utility

⁵⁰Privacy-Accuracy Trade-off

⁵¹Signal-to-Noise Ratio (SNR)

⁵²Statistical Minimax Theory

⁵³Duchi, Jordan, and Wainwright

مسئله در قالب نظریه اطلاعات، نشان دادند که هزینه محروم‌گی در مدل موضعی بسیار سنگین و غیرقابل اجتناب است.

در تحلیل مینی‌مکس، هدف یافتن «ریسک مینی‌مکس» (\mathfrak{M}_n) است؛ یعنی کمترین «زیان مورد انتظاری» (MSE) که بهترین تخمین‌گر ممکن در بدترین توزیع داده مرتكب می‌شود. دوچی و همکاران با استفاده از ابزارهایی نظری نامساوی فانو^{۵۴} و لم اسود^{۵۵} (که در فصل سوم به تفصیل بررسی خواهند شد)، ثابت کردند که رفتار مجانبی ریسک در مدل LDP تفاوتی بینایین با مدل مرکز دارد.

به طور مشخص، برای n کاربر و بودجه محروم‌گی α ، ریسک مینی‌مکس (واریانس خط) از رابطه زیر پیروی می‌کند:

$$\mathfrak{M}_{\text{LDP}} \asymp \frac{1}{n^\alpha} \quad , \quad \text{در حالی که} \quad \mathfrak{M}_{\text{CDP}} \asymp \frac{1}{n^{\frac{1}{2}\epsilon^2}} \quad (5-1)$$

این نتیجه که نرخ هم‌گرایی بهینه در مدل موضعی را تعیین می‌کند، حاوی دو پیام مهم است:

۱. کندی هم‌گرایی: در حالی که خطای مدل مرکز با سرعت $1/n$ کاهش می‌یابد، خطای مدل موضعی با سرعت بسیار کندر $\sqrt{n}/1$ کم می‌شود.

۲. اندازه نمونه مؤثر: ضریب α^2 نشان می‌دهد که هر نمونه داده‌ی خصوصی‌سازی شده، عملانه حاوی اطلاعاتی معادل با α^2 نمونه داده‌ی خام است (برای $1 < \alpha$). این یعنی برای جبران نویز α -LDP، حجم داده‌ها باید با ضریب $1/\alpha^2$ افزایش یابد.

پس از استقرار این چارچوب نظری، مرکز جامعه علمی بر طراحی مکانیزم‌های بهینه^{۵۶} قرار گرفت که بتوانند به این کران‌های نظری دست یابند. از جمله مهم‌ترین این تلاش‌ها می‌توان به معرفی مکانیزم‌های پله‌ای^{۵۷} توسط کایروز و همکاران [۱۳] و توسعه پروتکل‌های پیشرفته‌ای نظری کدگذاری یگانی^{۵۸} و هشینگ محلی بهینه^{۵۹} توسط وانگ و همکاران [۲۲] اشاره کرد. این روش‌ها تلاش می‌کنند با بهینه‌سازی ساختار نویز و استفاده از تکنیک‌های فشرده‌سازی اطلاعات، فاصله بین عملکرد عملی و حدود نظری مینی‌مکس را به حداقل برسانند.

⁵⁴Fano's Inequality

⁵⁵Assouad's Lemma

⁵⁶Optimal Mechanisms

⁵⁷Staircase Mechanisms

⁵⁸Unary Encoding (UE)

⁵⁹Optimal Local Hashing (OLH)

۳-۱ بیان مسئله و اهداف پژوهش

محرمانگی تفاضلی موضعی (LDP) به عنوان یک حوزه میانرشته‌ای، محل تلاقي «علوم کامپیوتر» (با تمرکز بر طراحی الگوریتم و امنیت) و «آمار ریاضی» (با تمرکز بر نظریه تخمین و مینیمکس) است. این ماهیت دوگانه، اگرچه باعث غنای ادبیات موضوع شده، اما منجر به پراکندگی قابل توجهی در روش‌ها و ابزارهای تحلیلی گشته است.

همان‌طور که در مرور ادبیات اشاره شد، چارچوب مینیمکس که توسط دوچی و همکاران [۸] پایه‌گذاری شده، نشان می‌دهد که اعمال محدودیت محرمانگی منجر به کاهش نرخ همگرایی در تخمین‌های آماری می‌شود. با این حال، اثبات این نتایج در مقالات مختلف با ابزارهای متفاوتی صورت گرفته است. برای مثال:

- در برخی مسائل تخمین چگالی، پژوهشگران عمدتاً از واگرایی کولبک-لایبلر (KL) و نامساوی فانو استفاده کرده‌اند.
- در مسائل آزمون فرض ساده، اغلب از فاصله‌ی تغییرات کل (TV) و لم لوکام بهره گرفته شده است.
- در تحلیل‌های اخیرتر، فاصله‌ی کای-دو (χ^2) به دلیل رفتار هموارتر در همسایگی صفر و ارتباط مستقیم با واریانس، مورد توجه قرار گرفته است.

در این پایان‌نامه تلاش شده است تا با گردآوری و بررسی جامع مطالعات پیشین، تحلیلی تطبیقی میان رویکردهای مختلف صورت گیرد و نتایج آن‌ها در چارچوبی منسجم و یک‌پارچه ارائه شود.

۱-۳-۱ رویکرد تحلیل: f -واگرایی‌ها به عنوان زبان مشترک

برای غلبه بر چالش پراکندگی و ایجاد یکپارچگی نظری، این پایان‌نامه پیشنهاد می‌کند که تمام تحلیل‌ها بر مبنای خانواده‌ی عمومی f -واگرایی‌ها^{۶۰} بازنویسی و تفسیر شوند. f -واگرایی‌ها (معرفی شده توسط سیسار^{۶۱})، کلاسی جامع از معیارهای فاصله بین دو توزیع احتمال P و Q هستند:

$$D_f(P\|Q) = \mathbb{E}_Q \left[f \left(\frac{dP}{dQ} \right) \right] \quad (6-1)$$

که در آن f یک تابع محدب با ویژگی $f(1) = 0$ است.

⁶⁰ f -divergences

⁶¹ Csiszár

انتخاب این رویکرد به ما اجازه می‌دهد تا «محرمانگی» را نه صرفاً به عنوان یک ویژگی الگوریتمی، بلکه به عنوان یک محدودیت هندسی تفسیر کنیم. در این دیدگاه، هر مکانیزم LDP مانند یک «کanal انقباضی»^{۶۲} عمل می‌کند که فاصله‌ی بین توزیع‌های ورودی را فشرده می‌سازد. هدف ما در این پژوهش، بررسی این است که چگونه ادبیات پیشرو، مفهوم «ضریب انقباض»^{۶۳} را برای f -واگرایی‌های مختلف محاسبه کرده و از آن برای استخراج کران‌های مینی‌مکس استفاده می‌کنند. این دیدگاه هندسی، پلی میان اثبات‌های پراکنده ایجاد می‌کند و نشان می‌دهد که انتخاب f مناسب، تابعی از هندسه‌ی مسئله است.

۲-۳-۱ رویکرد تحلیل: چارچوب انقباض f -واگرایی‌ها

برای غلبه بر چالش پراکنده‌ی مفاهیم و ارائه یک تحلیل منسجم، این پایان‌نامه بر مرور و تشریح رویکرد نوینی تمرکز دارد که در سال‌های اخیر توسط ** آسوده، علی‌اکبری و کالمون^{*} [۲] و ** آسوده و ژانگ^{*} [۳] توسعه یافته است. این پژوهشگران نشان داده‌اند که قیود محرمانگی تفاضلی موضعی (LDP) را می‌توان به صورت دقیق و ریاضی معادل با «خواص انقباضی»^{۶۴} خانواده‌ی f -واگرایی‌ها فرمول‌بندی کرد. به طور مشخص، در این رویکرد اثبات می‌شود که شرط LDP معادل است با کران‌دار بودن ضریب انقباض برای «واگرایی‌هاکی-استیک» (E_γ -divergence). همچنین، تحلیل‌های دقیق‌تر نشان می‌دهند که چگونه می‌توان بهترین کران‌های انقباض را برای واگرایی‌های مهمی نظیر χ^2 و KL استخراج کرد. این دیدگاه هندسی، هر مکانیزم محرمانگی را به مثابه‌ی یک کanal نویزی می‌بیند که فاصله بین توزیع‌های احتمالی ورودی را کاهش می‌دهد. در این پایان‌نامه، ما تلاش می‌کنیم تا با مطالعه‌ی دقیق این مراجع، نشان دهیم چگونه این ضرایب انقباض (η_f) محاسبه می‌شوند و چگونه می‌توان از آن‌ها برای بازتولید و بهبود کران‌های مینی‌مکس در مسائل تخمین و آزمون فرض استفاده کرد.

۳-۳-۱ اهداف و ساختار پژوهش

هدف اصلی این پایان‌نامه، ارائه‌ی یک «مرور تحلیلی و آموزشی» از ادبیات مدرن نظریه مینی‌مکس تحت محدودیت محرمانگی است. ما با محوریت قرار دادن کارهای انجام‌شده توسط محققان نامبرده، اهداف زیر را دنبال می‌کنیم:

۱. تبیین همارزی LDP و انقباض E_γ : مرور و بازنویسی اثبات‌های ریاضی که نشان می‌دهند

⁶²Contraction Channel

⁶³Contraction Coefficient

⁶⁴Contraction Properties

محرمانگی تفاضلی موضعی دقیقاً معادل با انقباض در واگرایی هاکی-استیک است. این بخش بر اساس نتایج [۲] تنظیم شده و پایه‌ای برای تعمیم نتایج به سایر واگرایی‌ها فراهم می‌کند.

۲. بررسی ضرایب انقباض برای واگرایی‌های χ^2 و KL : مطالعه‌ی کران‌های دقیق^{۶۵} برای ضریب انقباض مکانیزم‌های LDP تحت واگرایی‌های کای-دو و کولبک-لایبلر. این بخش با تمرکز بر نتایج [۳]^{۶۶}، نشان می‌دهد که چگونه می‌توان «نامساوی‌های پردازش داده قوی» را برای محیط‌های خصوصی استخراج کرد.

۳. یکپارچه‌سازی روش‌های کران پایین: تشریح اینکه چگونه ابزارهای انقباضی فوق، در ترکیب با متدهای کلاسیک آماری نظری «لوکام»، «فانو» و «اسود»، منجر به استخراج حدود بهینه برای خطای تخمین مینی‌مکس می‌شوند. هدف ما نشان دادن این موضوع است که چگونه این چارچوب واحد، نتایج پراکنده در ادبیات را پوشش می‌دهد.

۴. جمع‌بندی و مقایسه نتایج: انجام مروری ساختاریافته بر کاربردهای این چارچوب در مسائلی نظری «تخمین میانگین»، «تخمین چگالی» و «آزمون فرض»، و مقایسه نتایج حاصل از رویکرد انقباضی با سایر روش‌های موجود در ادبیات.

۴-۱ ساختار پایان‌نامه

ساختار ادامه‌ی این پایان‌نامه به شرح زیر سازمان‌دهی شده است:

در فصل دوم، مفاهیم بنیادی و ابزارهای ریاضی مورد نیاز برای تحلیل‌های نظری پیش رو معرفی می‌شوند. این فصل ابتدا به مرور تعاریف پایه در نظریه احتمال و اندازه می‌پردازد و سپس خانواده‌ی واگرایی‌های f (شامل واگرایی کولبک-لایبلر و فاصله تغییرات کل) را به عنوان ابزاری برای سنجش شباهت توزیع‌های احتمال تعریف می‌کند. در ادامه، مبانی آزمون فرض آماری و نامساوی‌های اطلاعاتی مهم نظری لم لی کم^{۶۷} و لم فانو^{۶۸} بررسی می‌شوند. بخش پایانی این فصل به معرفی مدل کلاسیک محرمانگی تفاضلی متمرکز (CDP) و ویژگی‌های آن اختصاص دارد.

فصل سوم به معرفی دقیق مدل محرمانگی تفاضلی موضعی (LDP) می‌پردازد. در این فصل، پس از ارائه تعریف و بررسی تفاوت‌های بنیادین آن با مدل متمرکز، مکانیزم‌های استاندارد این حوزه نظری پاسخ

⁶⁵Sharp Bounds

⁶⁶Strong Data Processing Inequalities (SDPI)

⁶⁷Le Cam's Lemma

⁶⁸Fano's Lemma

تصادفی⁶⁹ و خواص آن‌ها تشریح می‌شوند. هدف این فصل ایجاد درکی عمیق از محدودیت‌ها و الزامات طراحی مکانیزم در فضای موضعی است.

فصل چهارم به تحلیل کران‌های پایین خطر مینی‌مکس⁷⁰ در مسائل تخمین آماری تحت قید محروم‌گی اختصاص دارد. در این فصل نشان داده می‌شود که چگونه می‌توان با ترکیب ابزارهای نظریه اطلاعات و محدودیت‌های محروم‌گی، حدود بنیادین دقت تخمین‌گرها را تعیین کرد.

در فصل پنجم، چارچوب تحلیل خود را با استفاده از واگرایی‌های f تعمیم می‌دهیم. در این فصل ارتباط میان محروم‌گی تفاضلی موضعی و مفهوم ضریب انقباض⁷¹ در واگرایی‌ها بررسی شده و نتایج جدیدی در خصوص بھینگی مکانیزم‌ها ارائه می‌گردد.

در نهایت، فصل ششم به جمع‌بندی دستاوردها، نتیجه‌گیری کلی و ارائه پیشنهادهایی برای پژوهش‌های آتی اختصاص دارد.

⁶⁹Randomized Response

⁷⁰Minimax Risk

⁷¹Contraction Coefficient

فصل ۲

پیش‌نیازها

۱-۲ محرمانگی تفاضلی مت مرکز (CDP)

مفهوم محرمانگی تفاضلی^۱ یا به اختصار DP، اولین بار توسط دُورک و همکاران [۱۰] معرفی شد و به سرعت به استاندارد طلایی برای حفظ حریم خصوصی در تحلیل داده‌ها تبدیل گشت. این چارچوب، یک تعریف ریاضی قوی از حریم خصوصی ارائه می‌دهد که مبتنی بر پنهان‌سازی حضور یا عدم حضور یک فرد خاص در مجموعه‌داده است.

۱-۱-۲ مدل اعتماد و تعریف رسمی

در مدل مت مرکز^۲، فرض بر این است که یک متصدی مورد اعتماد^۳ وجود دارد. تمام افراد داده‌های خام و حساس خود را در اختیار این متصدی قرار می‌دهند (شکل ۱-۲ را ببینید). متصدی، مجموعه‌داده‌ی کامل D را در اختیار دارد. وظیفه‌ی متصدی این است که با اجرای یک مکانیزم تصادفی^۴ M بر روی مجموعه‌داده‌ی D ، نتایجی (مثالاً پاسخ به یک پرس‌وجو^۵) را به صورت عمومی منتشر کند، به طوری که اطلاعات حساس افراد فاش نشود.

تعریف ۱-۲ (جهان داده‌ها و پایگاه‌داده) مجموعه‌ی تمام مقادیر ممکن برای یک رکورد داده را «جهان

¹Differential Privacy

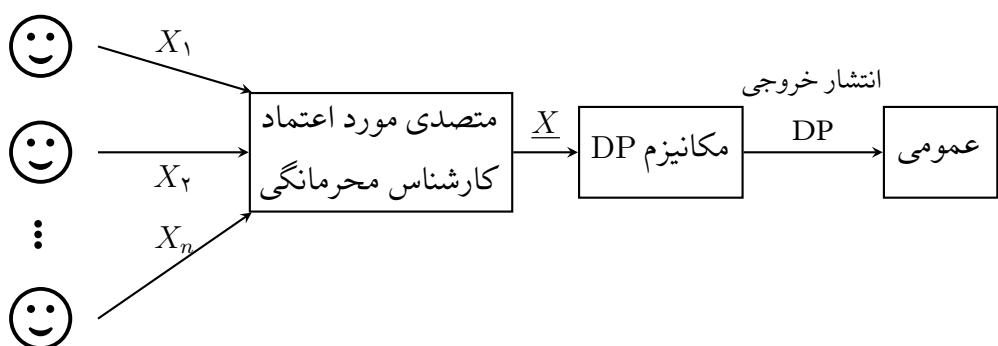
²Centralized

³Trusted Curator

⁴Randomized Mechanism

⁵Query

افراد (داده‌ها)



شکل ۱-۲: مدل محیانگی، تفاضلی، متمرکز (CDP) یا یک متصلی مورد اعتماد.

داده‌ها^۹ می‌نامیم و آن را با \mathcal{X} نمایش می‌دهیم. یک پایگاهداده \mathcal{D} مجموعه‌ای از رکوردهاست که اعضای آن از \mathcal{X} انتخاب شده‌اند. در ادبیات محترمانگی تفاضلی، پایگاهداده معمولاً به صورت یک بردار (هیستوگرام) $x \in \mathbb{N}^{|\mathcal{X}|}$ نمایش داده می‌شود که در آن هر مولفه x_i نشان‌دهنده تعداد تکرار عنصر i است. ام از \mathcal{X} در پایگاهداده است.

مثال ۱-۲ فرض کنید می خواهیم وضعیت اشتغال افراد را بررسی کنیم. در اینجا جهان داده‌ها برابر است با $\{بیکار, شاغل\} = \mathcal{X}$. اگر در یک پایگاه داده ۳ نفر شاغل و ۱ نفر بیکار باشند، نمایش هیستوگرامی پایگاه داده D به صورت پردازی خواهد بود:

$$\mathcal{D} = (\mathfrak{r}, \mathfrak{l})$$

تعريف ۲-۲ (الگوریتم تصادفی) یک الگوریتم (mekanizm) تصادفی M تابعی است که دامنه‌ی آن مجموعه‌ی تمام پایگاهداده‌های ممکن و برد آن مجموعه‌ی خروجی‌های ممکن \mathcal{R} است. برخلاف الگوریتم‌های قطعی، خروجی M برای یک ورودی ثابت D ، یک متغیر تصادفی است. به عبارت دیگر، M یک توزیع احتمال روی \mathcal{R} ایجاد می‌کند.

مثال ۲-۲ فرض کنید تابعی داریم که تعداد افراد بیمار را می‌شمارد. یک مکانیزم تصادفی ساده می‌تواند به این صورت باشد: «تعداد واقعی بیماران را بشمار و سپس نتیجه‌ی پرتاب یک سکه (۰ یا ۱) را به آن اضافه کن». در این حالت، خروجی، یا تعداد واقعی، بیماران است و یا یک عدد بیشتر از آن.

⁶Data Universe

تعريف ۳-۲ (فاصله و نرم‌های ℓ_p) برای سنجش میزان تفاوت دو پایگاهداده، از مفهوم نرم ℓ_p استفاده می‌شود. در حالت کلی برای $1 \geq p$ ، فاصله‌ی ℓ_p بین دو پایگاهداده‌ی \mathcal{D}_1 و \mathcal{D}_2 (با بردارهای تکرار متناظر) به صورت زیر تعریف می‌گردد:

$$\|\mathcal{D}_1 - \mathcal{D}_2\|_p = \left(\sum_{i=1}^{|\mathcal{X}|} |x_{1,i} - x_{2,i}|^p \right)^{1/p} \quad (1-2)$$

در ادبیات محترمانگی تفاضلی، نرم ℓ_1 (یا فاصله‌ی منتهن) به دلیل ارتباط مستقیم آن با تعداد رکوردها، معیار اصلی محسوب می‌شود. این فاصله دقیقاً تعداد رکوردهایی را می‌شمارد که باید تغییر کنند (اضافه یا حذف شوند) تا \mathcal{D}_2 به \mathcal{D}_1 تبدیل شود:

$$\|\mathcal{D}_1 - \mathcal{D}_2\|_1 = \sum_{i=1}^{|\mathcal{X}|} |x_{1,i} - x_{2,i}|$$

مثال ۳-۲ فرض کنید $(1, 0, 0) = \mathcal{D}_2$ باشند (یعنی در پایگاهداده دوم، یک نفر بیکار حذف شده است). فاصله‌ی ℓ_1 آن‌ها برابر است با:

$$\|\mathcal{D}_1 - \mathcal{D}_2\|_1 = |3 - 1| + |3 - 0| = 1$$

تعريف ۴-۲ (پایگاهداده‌های همسایه) دو پایگاهداده‌ی \mathcal{D}_1 و \mathcal{D}_2 را همسایه^۵ می‌گوییم (و با $\mathcal{D}_1 \sim \mathcal{D}_2$ نشان می‌دهیم) اگر فاصله‌ی ℓ_1 آن‌ها حداقل ۱ باشد:

$$\|\mathcal{D}_1 - \mathcal{D}_2\|_1 \leq 1$$

این شرط تضمین می‌کند که دو پایگاهداده تنها در بود و نبود مشخصات یک فرد خاص با هم تفاوت دارند.

ایده‌ی اصلی محترمانگی تفاضلی این است که خروجی مکانیزم برای دو مجموعه‌داده‌ی همسایه باید از نظر آماری «شبیه» باشد، به طوری که مهاجم نتواند تشخیص دهد ورودی واقعی کدام بوده است.

تعريف ۵-۲ (ε -محترمانگی تفاضلی (ε -DP)) یک مکانیزم تصادفی M با دامنه \mathcal{X}^n و برد \mathcal{R} ، ویژگی ε -محترمانگی تفاضلی را برآورده می‌سازد، اگر برای هر دو پایگاهداده‌ی همسایه‌ی \mathcal{D}_1 و \mathcal{D}_2 ($\mathcal{D}_1 \sim \mathcal{D}_2$) و برای هر زیرمجموعه از خروجی‌های ممکن $\mathcal{S} \subseteq \mathcal{R}$ (که در σ -جبر برد تعریف شده باشد)، داشته باشیم:

$$\mathbb{P}[M(\mathcal{D}_1) \in \mathcal{S}] \leq \exp(\varepsilon) \cdot \mathbb{P}[M(\mathcal{D}_2) \in \mathcal{S}] \quad (2-2)$$

در این نامساوی، پارامتر $\varepsilon \geq 0$ را بودجه‌ی محترمانگی^۶ می‌نامیم.

⁷Neighboring / Adjacent

⁸Privacy Budget

۲-۱-۲ تفسیر پارامترهای محربانگی

پارامتر ϵ نقش کنترل کننده‌ی توازن میان «محربانگی» و «سودمندی» را ایفا می‌کند:

- مقادیر کوچک ϵ (مثلاً $1 \leq \epsilon$) به معنای شباهت بسیار زیاد توزیع‌های خروجی است که منجر به محربانگی قوی‌تر اما خطای بیش‌تر (نویز بیش‌تر) می‌شود.
- مقادیر بزرگ ϵ اجازه‌ی تمایز بیش‌تر بین توزیع‌ها را می‌دهد که به معنای دقت بالاتر اما ریسک افشاری بیش‌تر است.
- اگر $\epsilon = 0$ باشد، خروجی مکانیزم باید کاملاً مستقل از ورودی باشد (امنیت کامل اما بدون هیچ‌گونه فایده‌ی آماری).

تعريف ۶-۲ DP -تقریبی یا (δ, ϵ) در بسیاری از موارد (مانند مکانیزم گوسی)، ارضای شرط ϵ خالص ممکن نیست. در این شرایط، از تعریف انعطاف‌پذیرتری به نام DP - ϵ استفاده می‌شود که اجازه‌ی یک احتمال شکست کوچک δ را می‌دهد:

$$\mathbb{P}[\mathcal{M}(\mathcal{D}_1) \in \mathcal{S}] \leq \exp(\epsilon) \cdot \mathbb{P}[\mathcal{M}(\mathcal{D}_2) \in \mathcal{S}] + \delta \quad (3-2)$$

پارامتر $[0, 1] \in \delta$ را معمولاً احتمال شکست^۹ یا احتمال نشت اطلاعات می‌نامند. تفسیر شهودی این است که مکانیزم با احتمال حداقل $\delta - 1$ ، تضمین DP - ϵ را رعایت می‌کند. در کاربردهای عملی، مقدار δ باید بسیار ناچیز (کمتر از معکوس چند جمله‌ای اندازه‌ی داده‌ها، مثلاً $1/n < \delta$) در نظر گرفته شود.

۳-۱-۲ تعاریف معادل و صورت‌بندی‌های جایگزین

برای تسهیل تحلیل‌های ریاضی و درک عمیق‌تر، می‌توان تعریف اصلی $DP-\epsilon$ را به صورت‌های همارز دیگری بیان کرد. در ادامه دو دیدگاه مهم « نقطه‌ای » و « واگرایی » را بررسی می‌کنیم.

۱. دیدگاه نقطه‌ای و چگالی احتمال (لم همارزی):

اگرچه تعریف اصلی بر روی زیرمجموعه‌ها بنا شده است، اما لم زیر نشان می‌دهد که کنترل نسبت احتمالات در تک‌تک نقاط برای برقراری شرط کافی است.

لم ۱-۲ (همارزی نقطه‌ای) یک مکانیزم M شرط $DP-\epsilon$ را بآورده می‌کند اگر و تنها اگر برای تمام همسایه‌های $D_2 \sim D_1$ شرایط زیر برقرار باشد:

⁹Failure Probability

- در فضای گسسته: برای هر خروجی $\mathcal{R} \in z$

$$\frac{\mathbb{P}[\mathcal{M}(\mathcal{D}_1) = z]}{\mathbb{P}[\mathcal{M}(\mathcal{D}_2) = z]} \leq e^\varepsilon \quad (4-2)$$

- در فضای پیوسته: با فرض وجود توابع چگالی $p(\cdot)$ و $q(\cdot)$ ، برای تمام $\mathcal{R} \in z$

$$p(z) \leq e^\varepsilon \cdot q(z) \quad (5-2)$$

اثبات. اثبات بر پایهی خاصیت جمع‌پذیری (در حالت گسسته) و خاصیت یکنواختی انTEGRAL (در حالت پیوسته روی میدان‌های σ -جبر بورل) استوار است. فرض کنید شرط نقطه‌ای برقرار باشد؛ برای هر زیرمجموعه‌ی بورلی $\mathcal{S} \subseteq \mathcal{R}$:

$$\mathbb{P}[\mathcal{M}(\mathcal{D}_1) \in \mathcal{S}] = \int_{\mathcal{S}} p(z) d\mu(z) \leq \int_{\mathcal{S}} e^\varepsilon q(z) d\mu(z) = e^\varepsilon \mathbb{P}[\mathcal{M}(\mathcal{D}_2) \in \mathcal{S}]$$

□ (در حالت گسسته، انTEGRAL با عملگر جمع جایگزین می‌شود).

نکته: این همارزی تنها برای $\delta = \varepsilon, \delta$ -DP صادق است. برای بررسی نقطه‌به‌ نقطه کافی نیست و شرط باید روی زیرمجموعه‌ها چک شود.

۲. تعریف مبتنی بر واگرایی ماکزیمم:

از دیدگاه نظریه اطلاعات، محترمانگی تفاضلی خالص محدودیتی بر روی «واگرایی ماکزیمم»^{۱۰} بین توزیع‌های خروجی است. واگرایی ماکزیمم به صورت $D_\infty(P||Q) = \sup_S \ln \frac{P(S)}{Q(S)}$ تعریف می‌شود. بنابراین تعریف ۵-۲ معادل است با:

$$\sup_{\mathcal{D}_1 \sim \mathcal{D}_2} D_\infty(\mathcal{M}(\mathcal{D}_1) \parallel \mathcal{M}(\mathcal{D}_2)) \leq \varepsilon \quad (6-2)$$

در بخش‌های بعدی با تعریف دقیق واگرایی آشنا خواهیم شد.

۴-۱-۲ مکانیزم‌های پایه

برای دست‌یابی به محترمانگی تفاضلی، باید به پاسخ دقیق پرس‌وجو «نویز»^{۱۱} اضافه کنیم. میزان نویز به حساسیت^{۱۲} پرس‌وجو بستگی دارد.

¹⁰Max Divergence

¹¹Noise

¹²Sensitivity

تعريف ۷-۲ (حساسیت سراسری ℓ_p) برای هر تابع پرس و جوی $f : \mathcal{X}^n \rightarrow \mathbb{R}^k$ که خروجی برداری دارد، «حساسیت سراسری ℓ_p »^{۱۳} که با $\Delta_{p,f}$ نمایش داده می‌شود، برابر است با بیشینه‌ی مقدار تغییرات خروجی تابع، به ازای تغییر تنها یک رکورد در ورودی. با استفاده از تعریف نرم ℓ_p (تعريف ۲-۱) داریم:

$$\Delta_p f = \max_{\mathcal{D}_1 \sim \mathcal{D}_2} \|f(\mathcal{D}_1) - f(\mathcal{D}_2)\|_p \quad (7-2)$$

که در آن ماکزیمم‌گیری روی تمام زوج پایگاه‌داده‌های همسایه ($\mathcal{D}_1 \sim \mathcal{D}_2$) انجام می‌شود.

در میان انواع حساسیت‌ها، دو مورد زیر به دلیل کاربردشان در مکانیزم‌های پایه، از اهمیت ویژه‌ای برخوردارند:

تعريف ۸-۲ (حساسیت ℓ_1 ، ℓ_2 و ℓ_∞) سه نوع حساسیت زیر بیشترین کاربرد را در طراحی مکانیزم‌های محترمانگی دارند:

۱. **حساسیت ℓ_1** ($\Delta_1 f$): این حساسیت برابر با ماکزیمم فاصله منتهن بین خروجی‌های است و پارامتر اصلی در مکانیزم لاپلاس می‌باشد:

$$\Delta_1 f = \max_{\mathcal{D}_1 \sim \mathcal{D}_2} \|f(\mathcal{D}_1) - f(\mathcal{D}_2)\|_1 \quad (8-2)$$

۲. **حساسیت ℓ_2** ($\Delta_2 f$): این حساسیت برابر با ماکزیمم فاصله اقلیدسی است و در مکانیزم گوسی کاربرد اساسی دارد. معمولاً استفاده از این حساسیت در ابعاد بالا منجر به خطای کمتری نسبت به ℓ_1 می‌شود:

$$\Delta_2 f = \max_{\mathcal{D}_1 \sim \mathcal{D}_2} \|f(\mathcal{D}_1) - f(\mathcal{D}_2)\|_2 \quad (9-2)$$

۳. **حساسیت ℓ_∞** ($\Delta_\infty f$): این حساسیت برابر با بیشینه‌ی تغییر در «تک‌تک مولفه‌های» خروجی است (نرم ماکزیمم). این معیار نشان می‌دهد که مقدار یک درایه خاص از خروجی چقدر می‌تواند تغییر کند:

$$\Delta_\infty f = \max_{\mathcal{D}_1 \sim \mathcal{D}_2} \|f(\mathcal{D}_1) - f(\mathcal{D}_2)\|_\infty \quad (10-2)$$

مثال ۴-۲ فرض کنید f یک تابع هیستوگرام شمارشی باشد (تعداد افراد در دسته‌های مجزا). اگر مشخصات یک فرد تغییر کند، او از یک دسته خارج (تغییر -1) و به دسته‌ی دیگر وارد (تغییر $+1$) می‌شود. سایر دسته‌ها ثابت می‌مانند (0). بردار تغییرات برابر است با $(0, \dots, +1, \dots, -1, \dots, 0)$. حال حساسیت‌ها را محاسبه می‌کنیم:

¹³ ℓ_p -Global Sensitivity

• حساسیت ℓ_1 : مجموع قدر مطلق تغییرات: $2 = |1| + |-1|$.

• حساسیت ℓ_2 : جذر مجموع مربعات: $\sqrt{2} = \sqrt{1^2 + (-1)^2}$.

• حساسیت ℓ_∞ : ماکزیمم قدر مطلق تغییرات: $1 = \max(|1|, |-1|, 0)$.

این مثال به وضوح رابطه $\Delta_\infty f \leq \Delta_2 f \leq \Delta_1 f$ را نشان می‌دهد.

انتخاب نوع حساسیت در طراحی مکانیزم، بستگی مستقیم به نوع نویز افزوده شده و ابعاد داده‌ها دارد. به طور خلاصه، حساسیت ℓ_1 برای کالیبره کردن مکانیزم لاپلاس و حساسیت ℓ_2 برای مکانیزم گوسی استفاده می‌شود.

۵-۱-۲ مکانیزم‌های بنیادی محترمانگی تفاضلی

در این بخش، سه مکانیزم اصلی را که بلوک‌های سازنده بسیاری از الگوریتم‌های پیچیده‌تر هستند، معرفی می‌کنیم.

مکانیزم لاپلاس

ساده‌ترین و پرکاربردترین روش برای توابع عددی، افزودن نویز از توزیع لاپلاس است. توزیع لاپلاس با پارامتر مقیاس b و میانگین μ دارای تابع چگالی احتمال $h(z) = \frac{1}{2b} \exp\left(-\frac{|z-\mu|}{b}\right)$ است.

قضیه‌ی ۲-۲ (محترمانگی مکانیزم لاپلاس) فرض کنید $f : \mathcal{X}^n \rightarrow \mathbb{R}^k$ یک تابع پرس‌وجو با حساسیت سراسری $\Delta_1 f$ باشد. مکانیزم لاپلاس که خروجی آن به صورت زیر تعریف می‌شود:

$$\mathcal{M}_{\text{Lap}}(\mathcal{D}) = f(\mathcal{D}) + (Y_1, \dots, Y_k) \quad (11-2)$$

که در آن $(\frac{\Delta_1 f}{\varepsilon}, Y_i)_{i=1}^{i.i.d.} \sim \text{Lap}(\frac{\Delta_1 f}{\varepsilon})$ را برآورده می‌کند.

اثبات. فرض کنید $\mathcal{D}_1 \sim \mathcal{D}_2$ دو پایگاه داده‌ی همسایه باشند و خروجی تابع f یک بردار k -بعدی باشد. نویز لاپلاس به هر مؤلفه به صورت مستقل اضافه می‌شود، بنابراین تابع چگالی احتمال توأم برابر با حاصل ضرب چگالی‌های مؤلفه‌هاست. با فرض $\frac{\Delta_1 f}{\varepsilon} = b$ ، نسبت چگالی احتمال را برای یک بردار خروجی دلخواه

z بررسی می‌کنیم:

$$\begin{aligned} \frac{p(z|\mathcal{D}_1)}{p(z|\mathcal{D}_2)} &= \frac{\prod_{i=1}^k \frac{1}{\sqrt{b}} \exp\left(-\frac{|z_i - f(\mathcal{D}_1)_i|}{b}\right)}{\prod_{i=1}^k \frac{1}{\sqrt{b}} \exp\left(-\frac{|z_i - f(\mathcal{D}_2)_i|}{b}\right)} \\ &= \prod_{i=1}^k \exp\left(\frac{|z_i - f(\mathcal{D}_2)_i| - |z_i - f(\mathcal{D}_1)_i|}{b}\right) \\ &= \exp\left(\frac{1}{b} \sum_{i=1}^k (|z_i - f(\mathcal{D}_2)_i| - |z_i - f(\mathcal{D}_1)_i|)\right) \end{aligned}$$

طبق نامساوی مثلثی ($|a| - |b| \leq |a - b|$) برای هر مؤلفه i داریم:

$$|z_i - f(\mathcal{D}_2)_i| - |z_i - f(\mathcal{D}_1)_i| \leq |f(\mathcal{D}_1)_i - f(\mathcal{D}_2)_i|$$

با اعمال این نامساوی در مجموع توان نمایی:

$$\sum_{i=1}^k (|z_i - f(\mathcal{D}_2)_i| - |z_i - f(\mathcal{D}_1)_i|) \leq \sum_{i=1}^k |f(\mathcal{D}_1)_i - f(\mathcal{D}_2)_i|$$

عبارت سمت راست دقیقاً برابر با نرم ℓ_1 تفاضل خروجی‌هاست:

$$\sum_{i=1}^k |f(\mathcal{D}_1)_i - f(\mathcal{D}_2)_i| = \|f(\mathcal{D}_1) - f(\mathcal{D}_2)\|_1$$

طبق تعریف حساسیت سراسری، می‌دانیم $\|f(\mathcal{D}_1) - f(\mathcal{D}_2)\|_1 \leq \Delta_1 f$. بنابراین:

$$\frac{p(z|\mathcal{D}_1)}{p(z|\mathcal{D}_2)} \leq \exp\left(\frac{\Delta_1 f}{b}\right) = \exp\left(\frac{\Delta_1 f}{\Delta_1 f/\varepsilon}\right) = e^\varepsilon$$

و حکم ثابت می‌شود. \square

مثال ۲-۵ (پرس‌وجوهای شمارشی)^{۱۴}، پرس‌وجوهایی شمارشی به فرم «چه تعداد از اعضای پایگاهداده ویژگی P را دارند؟» هستند. این نوع توابع بلوک‌های سازنده‌ی بسیاری از تحلیل‌های آماری و داده‌کاوی (مانند هیستوگرام‌ها) هستند [۱۱].

حالت تک پرس‌وجو: حساسیت یک پرس‌وجوی شمارشی دقیقاً ۱ است ($\Delta_1 f = 1$)؛ زیرا افزودن یا حذف یک فرد، نتیجه‌ی شمارش را حداقل ۱ واحد تغییر می‌دهد. بنابراین طبق قضیه ۲-۲، با افزودن نویز با مقیاس $\varepsilon/1$ (یعنی $(1/\varepsilon)$ Lap($1/\varepsilon$)) به پاسخ واقعی، محترمانگی $-DP(\varepsilon, 0)$ تضمین می‌شود.

حالت برداری (چند پرس‌وجو): فرض کنید لیستی از k پرس‌وجوی شمارشی $(f_1, \dots, f_k) = f$ داریم (یک پرس‌وجوی برداری). بدون داشتن اطلاعات اضافی درباره‌ی ارتباط پرس‌وجوهای f ، در بدترین حالت

¹⁴Counting Queries

یک فرد مشخص می‌تواند در تمام k شمارش تأثیر بگذارد. بنابراین حساسیت ℓ_1 کل بردار برابر با مجموع تغییرات، یعنی k خواهد بود ($f = \Delta_1 f = k$). در این حالت برای دست‌یابی به ϵ -DP، باید به هر پاسخ نویزی با مقیاس ϵ/k اضافه کنیم.

مکانیزم گوسی

زمانی که حساسیت ℓ_2 تابع بسیار کمتر از حساسیت ℓ_1 باشد (مثلًاً در پرس‌وجوهای برداری)، مکانیزم گوسی ترجیح داده می‌شود. این مکانیزم به جای نویز لابلس، نویز گوسی (نرمال) به خروجی اضافه می‌کند.

قضیه ۲-۳ (محرمانگی مکانیزم گوسی) فرض کنید $R^k \rightarrow \mathcal{X}^n : f$ تابعی با حساسیت ℓ_2 برابر با $\Delta_2 f$ باشد. مکانیزم گوسی با افزودن نویز $(\cdot, \sigma^2 \mathbf{I}_k) \sim \mathcal{N}(\cdot, \sigma^2 \mathbf{I}_k)$ به خروجی تعریف می‌شود:

$$\mathcal{M}_{\text{Gauss}}(\mathcal{D}) = f(\mathcal{D}) + \mathcal{N}(\cdot, \sigma^2 \mathbf{I}_k) \quad (12-2)$$

اگر $\epsilon \in (0, 1)$ باشد، با انتخاب انحراف معیار σ به صورت زیر، این مکانیزم شرط (ϵ, δ) -DP را برآورده می‌کند:

$$\sigma \geq \sqrt{2 \ln(1/25/\delta)} \cdot \frac{\Delta_2 f}{\epsilon} \quad (13-2)$$

اثبات. [طرح کلی] اثبات دقیق این قضیه نیازمند تحلیل «متغیر تصادفی زیان محرمانگی»¹⁵ است که جزئیات کامل آن در [11, Appendix A] موجود است. ایده اصلی این است که برخلاف توزیع لابلس، در توزیع گوسی نسبت $\frac{p(z)}{q(z)}$ کران‌دار نیست، اما احتمال رخداد مقادیری که این نسبت را بزرگ می‌کنند (نواحی دمی توزیع)، با δ محدود می‌شود. □

مثال ۲-۶ (انتشار آماره‌های چندگانه و اثر ابعاد) فرض کنید یک بیمارستان می‌خواهد میانگین d ویژگی حیاتی مختلف را منتشر کند. داده‌های هر بیمار را می‌توان به صورت یک بردار $v \in \mathbb{R}^d$ در نظر گرفت. اگر یک بیمار پرونده‌اش را تغییر دهد، در بدترین حالت تمام d ویژگی او می‌توانند از 0 به 1 تغییر کنند.

تحلیل حساسیت:

• حساسیت ℓ_1 : مجموع قدر مطلق تغییرات برابر است با d .

• حساسیت ℓ_2 : جذر مجموع مربعات تغییرات برابر است با \sqrt{d} .

¹⁵Privacy Loss Random Variable

مقایسه نویز: اگر تعداد ویژگی‌ها زیاد باشد (مثلًا $d = 100$):

- مکانیزم لاپلاس باید نویزی متناسب با $d = 100$ اضافه کند.

- مکانیزم گوسی نویزی متناسب با $\sqrt{100} = 10$ اضافه می‌کند.

این کاهش چشمگیر نویز (با ضریب \sqrt{d}) دلیل اصلی استفاده از مکانیزم گوسی در الگوریتم‌هایی نظریه یادگیری عمیق با محترمانگی تفاضلی (*DP-SGD*) است.

مکانیزم نمایی

مکانیزم‌های قبلی برای خروجی‌های عددی بودند. اگر خروجی یک «عضو» از یک مجموعه باشد، از مکانیزم نمایی استفاده می‌شود. این مکانیزم بر اساس یک تابع امتیاز^{۱۶} $q(\mathcal{D}, r)$ کار می‌کند که میزان «خوبی» خروجی r را می‌سنجد. حساسیت این تابع به صورت $\Delta q = \max_r \max_{\mathcal{D} \sim \mathcal{D}'} |q(\mathcal{D}, r) - q(\mathcal{D}', r)|$ تعریف می‌شود.

قضیه ۴-۲ (محترمانگی مکانیزم نمایی) مکانیزم نمایی، یک خروجی r از مجموعه ممکن \mathcal{R} را با احتمالی متناسب با امتیاز آن انتخاب می‌کند:

$$\mathbb{P}[\mathcal{M}_{\text{Exp}}(\mathcal{D}) = r] = \frac{\exp\left(\frac{\varepsilon \cdot q(\mathcal{D}, r)}{\gamma \Delta q}\right)}{\sum_{r' \in \mathcal{R}} \exp\left(\frac{\varepsilon \cdot q(\mathcal{D}, r')}{\gamma \Delta q}\right)} \quad (4-2)$$

این مکانیزم شرط $DP-\varepsilon$ -را برآورده می‌کند.

اثبات. فرض کنید $\mathcal{D}_1 \sim \mathcal{D}_2$. نسبت احتمالات برای یک خروجی ثابت r عبارت است از:

$$\frac{\mathbb{P}[\mathcal{M}(\mathcal{D}_1) = r]}{\mathbb{P}[\mathcal{M}(\mathcal{D}_2) = r]} = \frac{\exp\left(\frac{\varepsilon q(\mathcal{D}_1, r)}{\gamma \Delta q}\right)}{\exp\left(\frac{\varepsilon q(\mathcal{D}_2, r)}{\gamma \Delta q}\right)} \cdot \frac{\sum_{r'} \exp\left(\frac{\varepsilon q(\mathcal{D}_2, r')}{\gamma \Delta q}\right)}{\sum_{r'} \exp\left(\frac{\varepsilon q(\mathcal{D}_1, r')}{\gamma \Delta q}\right)}$$

ترم اول (صورت کسرها) با استفاده از خاصیت حساسیت q حداقل $e^{\varepsilon/2}$ است. ترم دوم (نسبت مخرج‌ها) نیز با استدلالی مشابه حداقل $e^{\varepsilon/2}$ خواهد بود. حاصل ضرب این دو مقدار حداقل e^ε می‌شود.

¹⁶Score Function

۶-۱-۲ ترکیب‌پذیری

در کاربردهای واقعی، معمولاً چندین پرس‌وجو روی یک پایگاهداده اجرا می‌شود. قضایای ترکیب‌پذیری^{۱۷} نشان می‌دهند که چگونه بودجه‌ی محرمانگی انباسته می‌شود.

قضیه‌ی ۵-۲ (ترکیب‌پذیری ساده) اگر k مکانیزم M_1, \dots, M_k به ترتیب دارای بودجه‌های $\varepsilon_1, \dots, \varepsilon_k$ باشند، اجرای متوالی آن‌ها روی یک پایگاهداده واحد، تضمین $-DP(\sum \varepsilon_i)$ را فراهم می‌کند [۱۱].

این کران خطی در بسیاری موارد بدینانه است. «قضیه ترکیب پیشرفت» نشان می‌دهد که با پذیرش اندکی احتمال شکست (δ' اضافه)، انباست بودجه بسیار کنتر (با نرخ \sqrt{k}) رشد می‌کند [۱۱].

قضیه‌ی ۶-۲ (ترکیب‌پذیری پیشرفت) برای هر $\varepsilon' > \delta'$ ، اجرای k مکانیزم که هر کدام $-DP(\varepsilon)$ هستند، دارای تضمین $-DP(\varepsilon', k\delta + \delta')$ است که در آن:

$$\varepsilon' \approx \varepsilon \sqrt{2k \ln(1/\delta')} + k\varepsilon(e^\varepsilon - 1) \quad (15-2)$$

برای مقادیر کوچک ε ، جمله دوم ناچیز است و بودجه کل تقریباً با $\sqrt{k}\varepsilon$ رشد می‌کند.

۷-۱-۲ محرمانگی گروهی

محرمانگی تفاضلی نه تنها از یک فرد، بلکه به صورت خودکار از گروههای کوچک نیز محافظت می‌کند [۱۱].

قضیه‌ی ۷-۲ (محرمانگی گروهی)^{۱۸} اگر دو پایگاهداده \mathcal{D}_1 و \mathcal{D}_2 در k رکورد متفاوت باشند (فاصله‌ی همسایگی k)، آنگاه هر مکانیزم $-DP(\varepsilon)$ برای آن‌ها تضمین $-DP(k\varepsilon)$ را ارائه می‌دهد:

$$\mathbb{P}[\mathcal{M}(\mathcal{D}_1) \in S] \leq e^{k\varepsilon} \mathbb{P}[\mathcal{M}(\mathcal{D}_2) \in S] \quad (16-2)$$

این خاصیت نشان می‌دهد که با بزرگ شدن گروه (k)، تضمین محرمانگی به صورت نمایی تضعیف می‌شود ($e^{k\varepsilon}$).

¹⁷Composition

۸-۱-۲ محدودیت مدل متتمرکز

با وجود تمام مزایا، مدل CDP یک نقطه‌ی ضعف اساسی دارد: نیاز به یک متصلی کاملاً مورد اعتماد. در بسیاری از سناریوهای دنیای واقعی (مانند جمع‌آوری داده از گوشی‌های هوشمند)، کاربران به سرور مرکزی اعتماد ندارند. این عدم اعتماد، ما را به سمت مدل جایگزین، یعنی «محرمانگی تفاضلی موضوعی» سوق می‌دهد. در فصل بعد با محرمانگی تفاضلی موضوعی و تعاریف و قضایای اساسی آن آشنا خواهیم شد.

۲-۲ f -واگرایی‌ها

در بخش‌های پیشین، مکانیزم‌های محرمانگی تفاضلی را ابزاری برای ایجاد «شباهت آماری» بین خروجی‌های دو پایگاهداده همسایه معرفی کردیم. برای کمی‌سازی دقیق این شباهت و اثبات کران‌های پایین در فصل‌های آینده، نیازمند معیاری هستیم که فاصله میان توزیع‌های احتمالی را در یک چارچوب عمومی بسنجد. این ابزار، خانواده f -واگرایی‌ها^{۱۹} است که نخستین بار توسط سیسر [۶] و علی و سیلوی [۱] معرفی شد.

۲-۲-۱ تعریف رسمی در فضای اندازه‌پذیر

برای ارائه تعریفی دقیق و مستقل از نوع متغیرهای تصادفی (پیوسته یا گسسته)، از زبان نظریه اندازه استفاده می‌کنیم. فرض کنید (Ω, \mathcal{F}) یک فضای اندازه‌پذیر^{۲۰} باشد و P و Q دو «اندازه احتمال»^{۲۱} تعریف شده روی این فضا باشند.

پیش از تعریف واگرایی، مفهوم «پیوستگی مطلق» که شرط وجود چگالی نسبت است را یادآوری می‌کنیم.

تعریف ۲-۹ (پیوستگی مطلق^{۲۲}) می‌گوییم اندازه P نسبت به Q مطلقاً پیوسته است و می‌نویسیم $Q \ll P$ ، اگر برای هر مجموعه اندازه‌پذیر $\mathcal{F} \in A \in \mathcal{F}$:

$$Q(A) = 0 \implies P(A) = 0 \quad (17-2)$$

این شرط تضمین می‌کند که هر رویدادی که تحت توزیع Q غیرممکن باشد، تحت P نیز غیرممکن است.

¹⁹ f -divergences

²⁰ Measurable Space

²¹ Probability Measures

اگر $Q \ll P$ باشد، بنابر قضیه رادون-نیکودیم^{۲۳}، تابعی اندازه‌پذیر و غیرمنفی روی Ω وجود دارد که «مشتق رادون-نیکودیم» P نسبت به Q نامیده می‌شود و با $\frac{dP}{dQ}$ نمایش داده می‌شود. این مشتق نقش همان نسبت درست‌نمایی^{۲۴} را در حالت کلی ایفا می‌کند.

تعريف ۱۰-۲ (f -واگرایی) فرض کنید P و Q دو اندازه احتمال روی (Ω, \mathcal{F}) باشند به طوری که $\ll P$ Q . برای هر تابع محدب^{۲۵} $\mathbb{R} \rightarrow (0, \infty)$: f با این شرط که $f(1) = 0$ ، f -واگرایی^{۲۶} P از Q به صورت امید ریاضی تابع f بر روی مشتق رادون-نیکودیم (تحت اندازه Q) تعریف می‌شود:

$$D_f(P\|Q) \triangleq \int_{\Omega} f\left(\frac{dP}{dQ}(\omega)\right) dQ(\omega) \quad (18-2)$$

یا به بیانی دیگر با استفاده از نماد امید ریاضی:

$$D_f(P\|Q) = \mathbb{E}_Q \left[f\left(\frac{dP}{dQ}\right) \right] \quad (19-2)$$

تفسیر اجزاء:

- تابع مولد f : تابع f تعیین‌کننده نوع هندسه و خواص واگرایی است. تحدب f شرطی حیاتی برای خوش‌رفتاری ریاضی این اندازه است.

- غیرمنفی بودن: با استفاده از نامساوی ینسن^{۲۶} و شرط محدب بودن f ، می‌توان نشان داد که واگرایی همواره نامنفی است:

$$D_f(P\|Q) = \mathbb{E}_Q \left[f\left(\frac{dP}{dQ}\right) \right] \geq f\left(\mathbb{E}_Q \left[\frac{dP}{dQ} \right]\right) = f(1) = 0 \quad (20-2)$$

تساوی $0 = D_f(P\|Q)$ برقرار است اگر و تنها اگر^{۲۷} $P = Q$ (در صورت اکیداً محدب بودن f).

در حالتهای خاص که فضای نمونه Ω گسسته یا پیوسته (اقلیدسی) باشد و چگالی‌های p و q نسبت به یک اندازه پایه (مانند شمارشی یا لبگ) وجود داشته باشند، مشتق رادون-نیکودیم به نسبت معمولی چگالی‌ها $\frac{p(x)}{q(x)}$ تبدیل می‌شود و تعریف انتگرالی بالا به فرم‌های آشنای زیر تقلیل می‌یابد:

$$D_f(P\|Q) = \int_{\mathcal{X}} q(x) f\left(\frac{p(x)}{q(x)}\right) dx \quad \text{یا} \quad \sum_{x \in \mathcal{X}} q(x) f\left(\frac{p(x)}{q(x)}\right) \quad (21-2)$$

²³Radon-Nikodym Theorem

²⁴Likelihood Ratio

²⁵Convex

²⁶Jensen's Inequality

تفاوت واگرایی با متر ریاضی: اگرچه در ادبیات موضوع، گاهی با اغماس از واژه‌ی «فاصله»^{۲۷} برای واگرایی‌ها استفاده می‌شود، اما باید توجه داشت که واگرایی‌ها لزوماً خواص یک متریک حقیقی را ندارند. یک تابع $d(P, Q)$ تنها در صورتی یک متر ریاضی است که علاوه بر غیرمنفی بودن و اصل همانی، دو شرط تقارن^{۲۸} ($d(P, Q) = d(Q, P)$) و نامساوی مثلث^{۲۹} ($d(P, R) \leq d(P, Q) + d(Q, R)$) را ارضاء کند.

بسیاری از واگرایی‌های معرفی شده در این بخش، به ویژه واگرایی کولبک-لایبلر (بخش ۱۲-۲)، این دو شرط را نقض می‌کنند. عدم تقارن در واگرایی‌ها دارای تفسیر آماری مهمی است؛ به عنوان مثال $KL(P\|Q)$ بیان‌گر میزان اطلاعات از دست رفته زمانی است که از توزیع Q برای مدل‌سازی توزیع واقعی P استفاده می‌کنیم. این مفهوم ماهیتی «جهت‌دار» دارد و با جابجایی جایگاه فرضیه و واقعیت تغییر می‌کند. با این حال، f -واگرایی‌ها همچنان خواص توپولوژیکی و هندسی قدرتمندی دارند که در فصل‌های آتی برای استخراج کران‌های پایین مینیممکن از آن‌ها بهره خواهیم برد.

۲-۲-۲ نمونه‌های مهم و توابع مولد

با انتخاب‌های متفاوت برای تابع مولد محدب f ، می‌توان طیف وسیعی از اندازه‌های فاصله را تولید کرد. در ادامه، مهم‌ترین نمونه‌ها را معرفی می‌کنیم. در تعاریف زیر، فرض می‌کنیم P و Q دو اندازه احتمال باشند که دارای چگالی (یا جرم) احتمال $p(x)$ و $q(x)$ نسبت به یک اندازه پایه هستند.

تعريف ۱۱-۲ (تغییرات کل) فاصله تغییرات کل^{۳۰}، شهودی‌ترین متریک برای سنجش تمایزپذیری دو توزیع است و بیان‌گر بیشترین تفاوت احتمالی است که دو توزیع می‌توانند روی یک پیشامد داشته باشند. تابع مولد آن $|f(t) - 1|$ است.

$$TV(P, Q) = \frac{1}{2} \int_{\mathcal{X}} |p(x) - q(x)| dx \quad (22-2)$$

$$= \sup_{A \subseteq \mathcal{X}} |P(A) - Q(A)| \quad (23-2)$$

این واگرایی ممکن است با نمادهایی مانند d_{TV} یا $\|\cdot\|_{TV}$ نیز نمایش داده شود.

تعريف ۱۲-۲ (کولبک-لایبلر) واگرایی کولبک-لایبلر^{۳۱}، معروف‌ترین واگرایی در نظریه اطلاعات که آنتروپی نسبی^{۳۲} نیز نامیده می‌شود. این معیار نامتقارن است و نقش اساسی در فشرده‌سازی داده‌ها و استنتاج

²⁷Distance

²⁸Symmetry

²⁹Triangle Inequality

³⁰Total Variation (TV)

³¹Kullback-Leibler (KL)

³²Relative Entropy

بیزی دارد. تابع مولد آن $f(t) = t \ln t$ است.

$$\text{KL}(P\|Q) = \int_{\mathcal{X}} p(x) \ln \left(\frac{p(x)}{q(x)} \right) dx \quad (24-2)$$

تعریف ۱۳-۲ (اطلاعات متقابل) اگر X و V دو متغیر تصادفی باشند، اطلاعات متقابل^{۳۳} بین آن‌ها به صورت امید ریاضی واگرایی KL بین توزیع شرطی و توزیع حاشیه‌ای تعریف می‌شود:

$$I(X; V) = \text{KL}(P_{X,V}\|P_X \otimes P_V) = \mathbb{E}_V [\text{KL}(P_{X|V}\|P_X)] \quad (25-2)$$

این معیار نقش کلیدی در نامساوی فانو و تحلیل کانال‌های اطلاعاتی ایفا می‌کند [۹].

تعریف ۱۴-۲ (کای-دو) واگرایی کای-دو^{۳۴}، اغلب برای تقریب‌زنی سایر فواصل (مانند KL) در همسایگی‌های کوچک استفاده می‌شود و به دلیل فرم مربعی، محاسبه آن معمولاً ساده‌تر است. تابع مولد آن^۲ $f(t) = (t - 1)^2$ است.

$$\chi^2(P\|Q) = \int_{\mathcal{X}} \frac{(p(x) - q(x))^2}{q(x)} dx \quad (26-2)$$

تعریف ۱۵-۲ (هلینگر-دو) فاصله هلینگر-دو^{۳۵}، تابع مولد آن^۲ $f(t) = (\sqrt{t} - 1)^2$ است. این فاصله به دلیل خواص ریاضی خوش‌رفتار (مانند متریک و کران‌دار بودن بین ۰ و ۲)، در نظریه برآورد^{۳۶} و استخراج کران‌های مینی‌مکس (مانند روش *Le Cam*) کاربرد فراوان دارد.

$$H^2(P, Q) = \int_{\mathcal{X}} \left(\sqrt{p(x)} - \sqrt{q(x)} \right)^2 dx \quad (27-2)$$

تعریف ۱۶-۲ (E_γ یا هاکی-استیک) واگرایی E_γ یا واگرایی هاکی-استیک^{۳۷}، ابزاری کلیدی در تحلیل‌های مدرن حریم خصوصی و آزمون‌های فرضیه است. تابع مولد آن برای پارامتر $\gamma \geq 0$ به صورت $f_\gamma(t) = [t - \gamma]_+ = \max \{0, t - \gamma\}$ است.

تعریف و صورت‌های معادل: تعریف اصلی بر اساس انگرال جرم اضافی نسبت درست‌نمایی است، اما صورت‌های معادل زیر بیان عملیاتی تری ارائه می‌دهند:

$$E_\gamma(P\|Q) = \int_{\mathcal{X}} \max \{0, p(x) - \gamma q(x)\} dx \quad (\tilde{28}-2)$$

$$= \sup_{A \subseteq \mathcal{X}} (P(A) - \gamma Q(A)) \quad (28-2)$$

$$= P(Z > \gamma) - \gamma Q(Z > \gamma) \quad \left(\text{که } Z = \frac{p(x)}{q(x)} \right) \quad (28-2)$$

³³Mutual Information

³⁴Chi-Squared (χ^2)

³⁵Squared Hellinger

³⁶Estimation Theory

³⁷Hockey-Stick Divergence

رابطه (۲۸-۲) نشان می‌دهد که این واگرایی بیان‌گر بیشینه‌ی تفاضل وزن‌دار احتمالات است که مستقیماً با موازنی خطای نوع اول و دوم در آزمون فرضیه مرتبط است.

نکات تحلیلی و تاریخی: نام‌گذاری توصیفی این واگرایی به «هاکی-استیک» که نخستین بار توسط ساسون و وردو [۱۹] پیشنهاد شد، برخاسته از شکل هندسی نمودار تابع مولد $f(t)$ است. نمادگذاری E_{e^ε} و تدوین نقش بنیادی آن، پیشتر توسط پولیانسکی و همکاران [۱۸] صورت گرفته بود.

کاربرد در حریم خصوصی: شرط محترمانگی تفاضلی تقریبی ($DP(\delta, \varepsilon)$) دقیقاً معادل است با اینکه برای هر دو دیتابیس همسایه، واگرایی هاکی-استیک خروجی‌ها از مقدار δ تجاوز نکند:

$$E_{e^\varepsilon}(P\|Q) \leq \delta \quad (29-2)$$

تعريف ۲-۱۷ (رنی) واگرایی رنی^{۳۸}، با پارامتر $(1, \infty)$ به صورت زیر تعریف می‌شود:

$$D_\alpha(P\|Q) = \frac{1}{\alpha - 1} \ln \left(\int_{\mathcal{X}} p(x)^\alpha q(x)^{1-\alpha} dx \right) \quad (30-2)$$

این واگرایی پای میان واگرایی KL (در حد $1 \rightarrow \alpha$) و واگرایی ماکزیمم (در حد $\infty \rightarrow \alpha$) است و در تحلیل ترکیب‌پذیری مکانیزم‌ها کاربرد دارد [۱۶].

تعريف ۲-۱۸ (ماکزیمم (D_∞)) این واگرایی متناظر با بدترین نسبت درست‌نمایی نقطه‌ای است و به عنوان حد واگرایی رنی به دست می‌آید:

$$D_\infty(P\|Q) = \lim_{\alpha \rightarrow \infty} D_\alpha(P\|Q) = \sup_{x \in \mathcal{X}} \ln \left(\frac{p(x)}{q(x)} \right) \quad (31-2)$$

کاربرد در حریم خصوصی: شرط $DP(\varepsilon)$ (خالص) دقیقاً معادل است با کران دار بودن این واگرایی توسط بودجه حریم خصوصی: $D_\infty(P\|Q) \leq \varepsilon$.

۳-۲-۲ خواص بنیادین و روابط بین f -واگرایی‌ها

خانواده f -واگرایی‌ها تنها مجموعه‌ای از فرمول‌های انتگرالی نیستند، بلکه دارای خواص ساختاری عمیقی هستند که آن‌ها را برای تحلیل سیستم‌های اطلاعاتی و حریم خصوصی ایده‌آل می‌سازد. در این بخش، سه ویژگی حیاتی این معیارها را بررسی می‌کنیم.

³⁸Rényi Divergence

نامساوی پردازش داده (DPI)

مهم‌ترین ویژگی f -واگرایی‌ها در نظریه اطلاعات، خاصیت یکنواختی^{۳۹} آن‌ها تحت پردازش است. این ویژگی بیان می‌کند که هیچ عملیات پردازشی روی داده‌ها (اعم از قطعی یا تصادفی) نمی‌تواند تمایزپذیری بین دو توزیع را افزایش دهد.

قضیه‌ی ۸-۲ (نامساوی پردازش داده^{۴۰}) فرض کنید P و Q دو توزیع احتمال روی فضای \mathcal{X} باشند و $\mathcal{X} \rightarrow \kappa$ یک هسته‌ی احتمالاتی (کانال مارکوف)^{۴۱} باشد که داده‌ها را از فضای \mathcal{X} به κ نگاشت می‌کند. اگر P_κ و Q_κ توزیع‌های خروجی پس از اعمال کرنل باشند، آنگاه برای هر f -واگرایی داریم:

$$D_f(P_\kappa \| Q_\kappa) \leq D_f(P \| Q) \quad (۳۲-۲)$$

تفسیر در حريم خصوصی: این قضیه تضمین می‌کند که اگر یک مهاجم نتواند دو دیتابیس را بر اساس خروجی مکانیزم از هم تشخیص دهد، با انجام هیچ‌گونه پس‌پردازشی^{۴۲} روی آن خروجی نیز قادر به بهبود توان تشخیص خود نخواهد بود. به عبارت دیگر، اطلاعات (و حريم خصوصی) با پردازش بیشتر، «خلق» یا «تخرب» نمی‌شود.

تحدب مشترک

تابع f -واگرایی نسبت به جفت توزیع‌های ورودی خود، محدب است.

قضیه‌ی ۹-۲ (تحدب مشترک^{۴۳}) نگاشت $(P, Q) \mapsto D_f(P \| Q)$ یک تابع محدب مشترک است. یعنی برای هر $\lambda \in [0, 1]$ و توزیع‌های P_1, P_2, Q_1, Q_2

$$D_f(\lambda P_1 + (1 - \lambda)P_2 \| \lambda Q_1 + (1 - \lambda)Q_2) \leq \lambda D_f(P_1 \| Q_1) + (1 - \lambda)D_f(P_2 \| Q_2) \quad (۳۳-۲)$$

این ویژگی در تحلیل مکانیزم‌هایی که ترکیبی از چند مکانیزم ساده‌تر هستند، بسیار کاربرد دارد.

روابط بین واگرایی‌ها

اگرچه انتخاب‌های مختلف f معیارهای متفاوتی تولید می‌کنند، اما این معیارها مستقل نیستند و می‌توان آن‌ها را با یکدیگر کران‌دار کرد.

³⁹Monotonicity

⁴¹Markov Kernel / Probability Kernel

⁴²Post-processing

- نامساوی پینسکر^{۴۴}: این نامساوی مشهور، ارتباط هندسه (فاصله تغییرات کل) و اطلاعات (واگرایی KL) را برقرار می‌کند و نشان می‌دهد که همگرایی در آنتروپی نسبی، همگرایی در L_1 را تضمین می‌کند:

$$TV(P, Q) \leq \sqrt{\frac{1}{2} KL(P\|Q)} \quad (34-2)$$

- رابطه هاکی-استیک و TV: می‌توان به سادگی دید واگرایی هاکی-استیک تعمیمی از فاصله تغییرات کل است. به طور مشخص، در نقطه $\gamma = 1$ این دو معیار برابر هستند:

$$E_1(P\|Q) = TV(P, Q) \quad (35-2)$$

این تساوی پل ارتباطی مهمی بین تعاریف $DP(\delta, \epsilon)$ و تحلیل‌های مبتنی بر فاصله تغییرات کل فراهم می‌کند.

۳-۲ مبانی آماری و کران‌های اطلاعاتی

در بخش‌های پیشین، ابزارهای سنجش فاصله بین توزیع‌ها (مانند f -واگرایی‌ها) را در بخش ۲-۲ معرفی کردیم. در این بخش، به معرفی چارچوب «نظریه تصمیم آماری»^{۴۵} می‌پردازیم. هدف ما ایجاد پلی مستحکم میان مفاهیم انتزاعی فاصله و مسئله‌ی عملیاتی تخمین پارامتر است. تعاریف و لمحاتی ارائه شده در این بخش، ابزار اصلی برای اثبات کران‌های پایین مینی‌مکس در فصل‌های آینده خواهد بود.

۱-۳-۲ نظریه تصمیم و ریسک مینی‌مکس

فرض کنید مدل آماری ما شامل فضای نمونه \mathcal{X} و خانواده‌ای از توزیع‌های احتمال $\{P_\theta : \theta \in \Theta\} = \mathcal{P}$ باشد که توسط فضای پارامتر Θ اندیس‌گذاری شده‌اند. داده‌های مشاهده شده $X^n = (X_1, \dots, X_n) \in \mathcal{X}^n$ میان متغیرهای تصادفی مستقلی هستند که از توزیع ناشناخته P_θ نمونه‌برداری شده‌اند.

یک «تخمین‌گر»^{۴۶}، تابعی اندازه‌پذیر به صورت $\hat{\theta} : \mathcal{X}^n \rightarrow \hat{\Theta}$ است که بر اساس مشاهدات، تقریبی از پارامتر واقعی ارائه می‌دهد. برای سنجش کیفیت این تقریب، از یک متریک (یا شبهمتریک) $\rho : \Theta \times \Theta \rightarrow \mathbb{R}_{\geq 0}$ بر روی فضای پارامتر استفاده می‌کنیم. تابع زیان معمولاً تابعی صعودی از این متریک است:

$$L(\hat{\theta}(X^n), \theta) = \Phi(\rho(\hat{\theta}(X^n), \theta)) \quad (36-2)$$

⁴⁴Pinsker's Inequality

⁴⁵Statistical Decision Theory

⁴⁶Estimator

که در آن Φ تابعی صعودی و غیرمنفی است (مانند $t = \hat{\theta}$ برای خطای میانگین مربعات).⁴⁷

«ریسک»^{۴۸} یک تخمین‌گر در نقطه θ ، برابر با امید ریاضی زیان تحت توزیع P_θ تعریف می‌شود:

$$R(\hat{\theta}, \theta) = \mathbb{E}_{X^n \sim P_\theta^n} [\Phi(\rho(\hat{\theta}(X^n), \theta))] \quad (37-2)$$

در تحلیل مینی‌مکس، ما بدترین عملکرد ممکن یک تخمین‌گر را در سراسر فضای پارامتر در نظر می‌گیریم.

تعریف ۱۹-۲ (ریسک مینی‌مکس) ریسک مینی‌مکس $\mathfrak{M}_n(\Theta)$ برای خانواده \mathcal{P} و متريک ρ ، برابر است با کمینه‌ی بیشینه‌ی ریسک:

$$\mathfrak{M}_n(\Theta, \Phi \circ \rho) = \inf_{\hat{\theta}} \sup_{\theta \in \Theta} \mathbb{E}_{P_\theta^n} [\Phi(\rho(\hat{\theta}(X^n), \theta))] \quad (38-2)$$

که در آن اينفييم بر روی تمامی تخمین‌گرهای اندازه‌پذیر $\hat{\theta}$ گرفته می‌شود و سوپریم روی تمام پارامترهای عضو خانواده‌ی Θ .

۲-۳-۲ تقلیل به آزمون فرض (روش بسته‌بندی)

محاسبه مستقیم مقدار (۳۸-۲) دشوار است. استراتژی استاندارد ما برای غلبه بر این دشواری، «تبديل فضای پيوسته پارامتر به يك مجموعه گسيسته» است. به عبارت ديگر، مسئله‌ی «تخمين» را به مسئله‌ی «آزمون فرض چندگزینه‌ای» تقلیل می‌دهیم.

این فرآيند بر پایه اين شهود استوار است که هر تخمین‌گر دقیق، باید بتواند بین پارامترهایی که فاصله‌ی تقریباً زیادی از هم دارند، تمایز قائل شود. برای رسمی‌سازی این ایده، از مفهوم «بسته‌بندی» استفاده می‌کنیم.

تعریف ۲۰-۲ (مجموعه بسته‌بندی)^{۴۹} مجموعه‌ی متناهی $\Theta = \{\theta_1, \dots, \theta_M\} \subset \mathcal{V}$ یک 2δ -بسته‌بندی برای فضای (ρ, Θ) نامیده می‌شود اگر اعضای آن حداقل به اندازه 2δ از يك ديگر فاصله داشته باشند:

$$\min_{i \neq j} \rho(\theta_i, \theta_j) \geq 2\delta \quad (39-2)$$

نکته کلیدی در این است که اگر تخمین‌گر $\hat{\theta}$ به پارامتر واقعی θ_v نزدیک باشد ($\delta < \rho(\hat{\theta}, \theta_v)$)، آنگاه به دليل نامساوی مثلث، فاصله آن از سایر نقاط شبکه بيش از δ خواهد بود. بنابراین، قوع خطای آزمون

⁴⁷Risk

فرضیه، مستلزم وقوع خطای تخمین بزرگ است. با استفاده از مفاهیم فاصله که در بخش ۲-۲ دیدیم و ترکیب آن با نامساوی مارکوف، به قضیه‌ی زیر می‌رسیم:

قضیه‌ی ۱۰-۲ (کران پایین عمومی) فرض کنید $\{\theta_1, \dots, \theta_M\}$ یک 2δ -بسته‌بندی برای Θ باشد. آنگاه ریسک مینی‌مکس به خطای آزمون فرض محدود می‌شود:

$$\mathfrak{M}_n(\Theta) \geq \Phi(\delta) \cdot \inf_{\hat{\theta}} \sup_{\theta \in \mathcal{V}} \Pr_{P_{\theta}^n} \left(\rho(\hat{\theta}, \theta) \geq \delta \right) \quad (40-2)$$

$$\geq \Phi(\delta) \cdot \inf_{\psi} \bar{P}_{err}(\psi) \quad (41-2)$$

که در آن $\bar{P}_{err}(\psi) = \frac{1}{M} \sum_{v=1}^M P_{\theta_v}^n(\psi(X^n) \neq v)$ میانگین احتمال خطا روی فرضیه‌های گسسته است و ψ آزمون‌گری است که سعی در بازیافت اندیس v دارد.

۳-۳-۲ نامساوی‌های کران پایین

اکنون که مسئله را به آزمون فرض روی M نقطه تقلیل دادیم، برای اثبات کران‌های پایین نهایی نیاز به ابزارهایی داریم که \bar{P}_{err} را از پایین محدود کنند. سه روش اصلی که بر پایه f -واگرایی‌ها بنا شده‌اند عبارتند از:

قضیه‌ی ۱۱-۲ (نامساوی لو کم^{۴۹}) این روش معمولاً برای آزمون بین دو توزیع P_1 و P_2 ($M = 2$) استفاده می‌شود و برای «کران‌های محلی» حول یک نقطه مناسب است.

$$\inf_{\psi} \bar{P}_{err}(\psi) \geq \frac{1}{2} (1 - \|P_1^n - P_2^n\|_{TV}) \quad (42-2)$$

تفسیر: این نامساوی بیان می‌کند که اگر فاصله TV بین دو توزیع کم باشد، همپوشانی آن‌ها زیاد است و هیچ آزمون‌گری نمی‌تواند با خطای ناچیز آن‌ها را تفکیک کند.

قضیه‌ی ۱۲-۲ (نامساوی فانو^{۵۰}) زمانی که پارامتر مورد نظر متعلق به مجموعه‌ای بزرگ‌تر V باشد ($M = |V| > 2$)، نامساوی فانو کران پایین قوی‌تری ارائه می‌دهد:

$$\inf_{\psi} \bar{P}_{err}(\psi) \geq 1 - \frac{I(X^n; V) + \log 2}{\log M} \quad (43-2)$$

که در آن $I(X^n; V)$ اطلاعات متقابل بین داده‌ها و اندیس پارامتر است.

تفسیر: نامساوی فانو مسئله خطای اطلاعات متقابل $I(X^n; V)$ گره می‌زند. اگر داده‌ها حاوی اطلاعات کافی درباره اندیس واقعی V نباشند (ظرفیت کانال نسبت به تعداد فرضیه‌ها M کم باشد)، خطای اجتناب‌ناپذیر است.

لم ۱۳-۲ (لم اسود^{۵۱}) این لم ابزاری قدرتمند برای فضاهای پارامتر با ابعاد بالا (مانند $\{1, \dots, 1\}^d$) است. قدرت لم اسود در شکستن یک مسئله d -بعدی دشوار به d مسئله ۱-بعدی مستقل است.

$$\mathfrak{M}_n(\Theta) \geq \frac{\delta}{2} \sum_{j=1}^d \left[1 - \|M_{+j}^n - M_{-j}^n\|_{TV} \right] \quad (44-2)$$

که در آن M_{+j}^n و M_{-j}^n توزیع‌های مخلوط حاشیه‌ای هستند (میانگین توزیع‌هایی که بیت زام آن‌ها به ترتیب $+1$ و -1 است). اگر در هر بعد تمایز قائل شدن سخت باشد، مجموع خطاهای با تعداد ابعاد d جمع شده و کران محکمی می‌سازد.

فصل ۳

محرمانگی تفاضلی موضعی

۱-۳ مقدمه

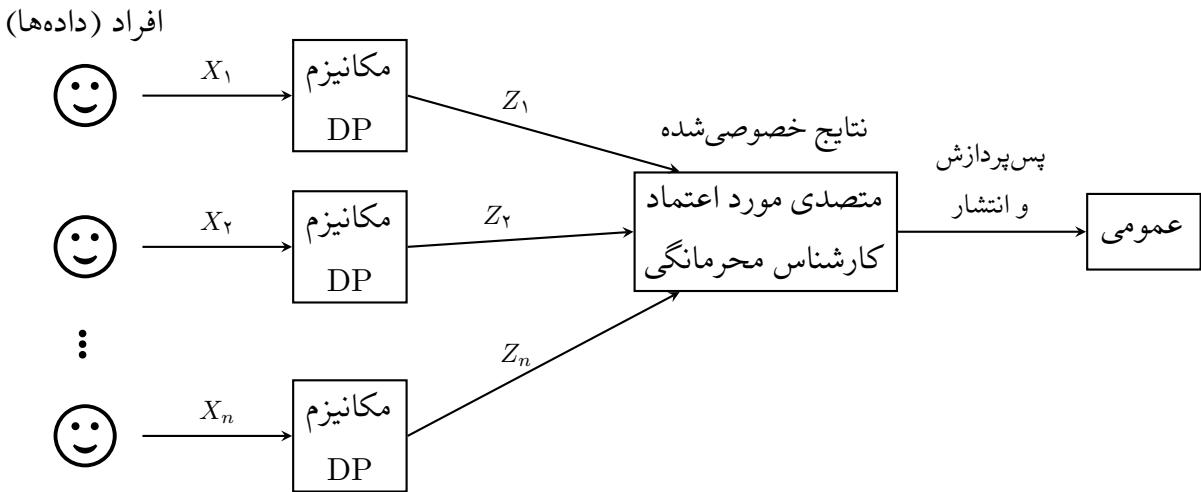
در فصل پیشین (۲)، مفاهیم بنیادی نظریه اندازه و مدل محرمانگی تفاضلی مت مرکز (CDP) را بررسی کردیم. همان‌طور که در بخش ۱-۲ مشاهده شد، مدل مت مرکز (CDP) بر فرض وجود یک متصلی مورد اعتماد استوار است که به داده‌های خام تمامی کاربران دسترسی دارد ($M : \mathcal{X}^n \rightarrow \mathcal{R}$). اگرچه این مدل دقیق آماری بالایی را فراهم می‌کند، اما ذخیره‌سازی مت مرکز داده‌ها یک «نقطه شکست مرکزی» ایجاد می‌کند؛ به این معنا که نفوذ به سرور یا خیانت متصلی، حریم خصوصی تمامی کاربران را به خطر می‌اندازد. برای مثال در بسیاری از کاربردهای مدرن، مانند جمع‌آوری داده‌های تله‌متري مرورگرها یا اپلیکیشن‌های موبایل، اعتماد به سرور مرکزی خطرات امنیتی و چالش‌های حقوقی را به همراه دارد.

در پاسخ به این چالش، مدل «محرمانگی تفاضلی موضعی»^۱ یا به اختصار LDP پارادایم اعتماد را تغییر می‌دهد. در این مدل، هیچ موجودیتی (حتی سرور) به داده‌ی خام X_i دسترسی ندارد؛ بلکه هر کاربر به صورت مستقل مکانیزم تصادفی M_i را روی داده‌ی خود اجرا کرده و تنها خروجی نویزدار Z_i را منتشر می‌کند (شکل ۱-۲).

۲-۳ تعاریف رسمی و مدل‌های محاسباتی

در مدل موضعی، مجموعه‌ای از n کاربر وجود دارند که هر کدام داده‌ای خصوصی $X_i \in \mathcal{X}$ در اختیار دارند. برخلاف مدل مت مرکز که شرط محرمانگی روی «پایگاه داده‌های همسایه» تعریف می‌شد، در این جا

¹Local Differential Privacy



شکل ۱-۳: گذار از مدل متمرکز به موضعی؛ نویز به صورت محلی (Local) روی دستگاه کاربر اضافه می‌شود.

شرط محترمانگی باید برای «هر جفت ورودی ممکن» در دامنه برقرار باشد تا تمایز قائل شدن بین مقادیر مختلف ورودی برای مهاجم دشوار گردد.

تعريف ۱-۳ (تصادفی‌ساز موضعی^۲) یک مکانیزم تصادفی $\mathcal{Z} \rightarrow \mathcal{M} : \mathcal{X}$ را یک تصادفی‌ساز موضعی می‌نامیم که ورودی $x \in \mathcal{X}$ را دریافت کرده و خروجی $z \in \mathcal{Z}$ را بر اساس توزیع احتمال شرطی $Q(z|x)$ تولید می‌کند.

۱-۲-۳ تعریف ریاضی LDP

هسته‌ی اصلی این مدل، تضمین این نکته است که توزیع‌های خروجی برای هر دو ورودی متمايز، از نظر آماری بسیار به هم نزدیک باشند.

تعريف ۲-۳ (α -LDP) یک مکانیزم تصادفی \mathcal{M} ، α -LDP است، اگر برای تمام جفت ورودی‌های $x, x' \in \mathcal{X}$ و برای هر رویداد خروجی $\mathcal{Z} \subseteq \mathcal{S}$ (در σ -جبر برد) داشته باشیم:

$$\sup_{x, x' \in \mathcal{X}} \sup_{\mathcal{S} \subseteq \mathcal{Z}} \frac{\mathbb{P}[\mathcal{M}(x) \in \mathcal{S}]}{\mathbb{P}[\mathcal{M}(x') \in \mathcal{S}]} \leq e^\alpha \quad (1-3)$$

نکته: در متون آماری این حوزه (مانند [A]), معمولاً از پارامتر α برای بودجه‌ی محترمانگی موضعی استفاده می‌شود تا تمایز آن با پارامتر ϵ در مدل متمرکز مشخص گردد. ما نیز در این فصل و فصول بعدی از این نمادگذاری پیروی می‌کنیم.

این تعریف را می‌توان با استفاده از مفهوم «واگرایی ماکزیمم» (D_∞) که پیش‌تر معرفی شد، به صورت فشرده‌تری بیان کرد. شرط (۱-۳) دقیقاً معادل است با:

$$\sup_{x, x' \in \mathcal{X}} D_\infty(Q(\cdot|x) \| Q(\cdot|x')) \leq \alpha \quad (2-3)$$

این رابطه نشان می‌دهد که α -LDP محدودیتی سخت‌گیرانه بر روی «نسبت درست‌نمایی»^۳ توزیع‌های خروجی اعمال می‌کند و تضمین می‌دهد که مشاهده‌ی خروجی z ، اطلاعات اندکی درباره‌ی ورودی x افشا می‌کند.

۲-۲-۳ محرمانگی تقریبی

مشابه مدل متمرکز، در برخی کاربردها نیاز است که تعریف α -LDP را تضعیف کنیم تا اجازه‌ی یک احتمال شکست ناچیز^۴ داده شود. این حالت معمولاً زمانی رخ می‌دهد که دامنه یا برد مکانیزم نامتناهی باشد (مانند مکانیزم گوسی).

تعریف ۳-۳ (α, δ)-LDP یک مکانیزم \mathcal{M} دارای محرمانگی تفاضلی موضعی تقریبی است اگر برای تمام ورودی‌های $x, x' \in \mathcal{X}$ و تمام زیرمجموعه‌های خروجی $Z \subseteq S$ داشته باشیم:

$$\mathbb{P}[\mathcal{M}(x) \in S] \leq e^\alpha \cdot \mathbb{P}[\mathcal{M}(x') \in S] + \delta \quad (3-3)$$

بدیهی است که اگر $\delta = 0$ باشد، این تعریف به حالت α -LDP خالص باز می‌گردد [۲۲].

۳-۳ پروتکل‌های تعاملی و خواص ترکیب

برای تحلیل دقیق حدود مینی‌مکس و درک محدودیت‌های بنیادین LDP، نیازمند مدل‌سازی دقیق نحوه تعامل کاربران با سرور (یا جمع‌آورنده داده) هستیم. دوچی و همکاران [۸] پروتکل‌های موضعی را بر اساس ساختار وابستگی آماری خروجی‌ها به دو دسته‌ی کلی تقسیم می‌کنند: غیرتعاملی و تعاملی.

۱-۳-۳ پروتکل‌های غیرتعاملی

در پروتکل‌های غیرتعاملی^۵، تمام کاربران $n = 1, \dots, i$ مکانیزم‌های خود را به صورت همزمان و مستقل از یک‌دیگر اجرا می‌کنند. اگر i -خروجی کاربر i -ام باشد، توزیع آن تنها به داده‌ی خصوصی X_i وابسته است

³Likelihood Ratio

⁴Non-interactive

و هیچ وابستگی‌ای به خروجی سایر کاربران ندارد. به بیان ریاضی، توزیع مشترک خروجی‌ها به صورت حاصل ضرب توزیع‌های حاشیه‌ای فاکتور می‌شود:

$$\mathbb{P}(Z_1, \dots, Z_n | X_1, \dots, X_n) = \prod_{i=1}^n Q_i(Z_i | X_i) \quad (4-3)$$

بسیاری از پیاده‌سازی‌های صنعتی فعلی، از جمله RAPPOR گوگل [۱۲]، در این دسته قرار می‌گیرند.

۲-۳-۳ پروتکل‌های تعاملی (ترتیبی)

در پروتکل‌های تعاملی^۵، کاربران به نوبت داده‌های خود را ارسال می‌کنند و مکانیزم کاربر i -ام می‌تواند به خروجی‌های مشاهده شده از کاربران پیشین (Z_1, \dots, Z_{i-1}) وابسته باشد. این مدل، آزادی عمل بیشتری را برای طراحی الگوریتم‌های تطبیقی فراهم می‌کند.

از دیدگاه آنالیز ریاضی، این فرآیند با استفاده از «کرنل‌های احتمالاتی»^۶ مدل‌سازی می‌شود. فرض کنید $Z_{1:i-1} = (Z_1, \dots, Z_{i-1})$ بردار خروجی‌های پیشین باشد که σ -فیلد \mathcal{F}_{i-1} را تولید می‌کند. مکانیزم کاربر i -ام، یک کرنل احتمالاتی Q_i است که خروجی $Z_i \in \mathcal{Z}$ را مشروط بر داده‌ی خصوصی X_i و تاریخچه‌ی عمومی $Z_{1:i-1}$ تولید می‌کند:

$$Z_i \sim Q_i(dz_i | x_i, z_{1:i-1}) \quad (5-3)$$

شرط اساسی محترمانگی در اینجا این است که با شرط‌سازی روی X_i و $Z_{1:i-1}$ ، متغیر Z_i باید از سایر داده‌های خصوصی $X_{j \neq i}$ مستقل باشد (شرط مارکوفی). این ساختار به پروتکل اجازه می‌دهد تا پارامترهای پرس‌وجو را به صورت پویا بر اساس اطلاعات کسب شده از کاربران قبلی تنظیم کند.

۳-۳-۳ قضیه ترکیب ترتیبی

یکی از ویژگی‌های بنیادین LDP، پایداری آن در برابر ترکیب است. اگر یک پروتکل شامل چندین مرحله‌ی تعاملی باشد، بودجه‌های محترمانگی با یک‌دیگر جمع می‌شوند. قضیه‌ی زیر، کران بالای محترمانگی را برای یک پروتکل ترتیبی بیان می‌کند [۸].

قضیه ۱-۳ (ترکیب ترتیبی)^۷ فرض کنید در یک پروتکل تعاملی، برای هر کاربر $\{1, \dots, n\}$ و به ازای هر تاریخچه‌ی ممکن^۸ $Z^{i-1} \in \mathcal{Z}^{i-1}$ ، مکانیزم $(Q_i(\cdot | \cdot), z_{1:i-1})$ دارای خاصیت LDP_{α_i} نسبت به

⁵Interactive / Sequential

⁶Probability Kernels

ورو دی x_i باشد. آنگاه توزیع مشترک کل خروجی ها (Z_1, \dots, Z_n)، دارای محترمانگی تفاضلی موضعی با بودجه مجموع است:

$$\alpha_{total} = \sum_{i=1}^n \alpha_i \quad (6-3)$$

اثبات. اثبات بر پایه خاصیت زنجیره ای و اگرایی ماکزیمم (D_∞) یا تجزیه نسبت های درست نمایی استوار است. اگر P و P' دو توزیع احتمال روی دنباله خروجی ها Z^n باشند که ناشی از دو دنباله ورودی x^n و x'^n هستند، نسبت احتمال توانم به حاصل ضرب نسبت های شرطی تجزیه می شود:

$$\frac{P(z^n)}{P'(z^n)} = \prod_{i=1}^n \frac{Q_i(z_i|x_i, z_{1:i-1})}{Q_i(z_i|x'_i, z_{1:i-1})}$$

از آنجا که هر گام طبق فرض با e^{α_i} کران دار است، کل حاصل ضرب با $e^{\sum \alpha_i}$ کران دار خواهد بود. \square

۴-۳ مکانیزم های پایه در LDP

در این بخش، مکانیزم های بنیادین LDP را با رویکردی آماری تحلیل می کنیم. هدف اصلی در طراحی این مکانیزم ها، یافتن نگاشتی تصادفی است که علاوه بر اراضی شرط محترمانگی، «خطای تخمین» (که معمولاً با واریانس سنجیده می شود) را کمینه کند. فرض بنیادی در تمام این مکانیزم ها این است که برای بازیابی اطلاعات آماری (مانند هیستوگرام)، از یک «تخمین گر ناریب»^۸ معکوس استفاده می شود.

۱-۴-۳ پاسخ تصادفی دودویی (RR)

پایه ای ترین مکانیزم α -LDP، پاسخ تصادفی^۹ (RR) برای دامنه دودویی $\{0, 1\}^x$ است. این مکانیزم را می توان به صورت یک کانال متقارن دودویی مدل سازی کرد که ورودی x را با احتمال p حفظ کرده و با احتمال $p - 1$ قرینه می کند:

$$\mathbb{P}[y = z|x] = \begin{cases} p & \text{if } z = x \\ 1 - p & \text{if } z \neq x \end{cases} \quad (7-3)$$

اثبات α -LDP: برای اینکه این مکانیزم شرط α -LDP را برآورده کند، طبق تعریف ۲-۳ باید نسبت درست نمایی برای هر دو ورودی متمایز x' و x و هر خروجی ممکن y ، با e^α کران دار شود. بدترین حالت

⁸Unbiased Estimator

⁹Randomized Response

زمانی رخ می‌دهد که صورت کسر بیشترین احتمال (p) و مخرج کسر کمترین احتمال ($p - 1$) باشد:

$$\sup_{y \in \{0, 1\}} \frac{\mathbb{P}[y|x]}{\mathbb{P}[y|x']} = \frac{p}{1-p} \leq e^\alpha \quad (8-3)$$

با حل این نامساوی برای p (و با فرض $1/2 > p$ برای بی معنی نشدن نتیجه)، مقدار بهینه احتمال حفظ پاسخ برای بودجه α به دست می‌آید:

$$p = \frac{e^\alpha}{e^\alpha + 1} \quad (9-3)$$

تحلیل واریانس: برای تحلیل دقیق خطا، ابتدا تخمین‌گر نااریب را استخراج می‌کنیم. اگر $\{0, 1\}$ $y \in \{0, 1\}$ خروجی مکانیزم باشد، هدف یافتن تابعی $\hat{f}(y) = x$ است که $\mathbb{E}_{\hat{f}(y)} = x$ باشد.

лем ۲-۳ (واریانس پاسخ تصادفی) برای مکانیزم RR با پارامتر p ، تخمین‌گر نااریب ورودی x به صورت زیر است:

$$\hat{x} = \frac{y - (1 - p)}{2p - 1} \quad (10-3)$$

و واریانس این تخمین‌گر بر حسب بودجه محترمانگی α برابر است با:

$$\text{Var}[\hat{x}] = \frac{e^\alpha}{(e^\alpha - 1)^2} \quad (11-3)$$

اثبات. ابتدا نااریبی را بررسی می‌کنیم. امید ریاضی y برابر است با:

$$\mathbb{E}_y = p \cdot x + (1 - p)(1 - x) = (2p - 1)x + (1 - p)$$

با جایگذاری در معادله تخمین‌گر:

$$\mathbb{E}_{\hat{x}} = \frac{\mathbb{E}_y - (1 - p)}{2p - 1} = \frac{(2p - 1)x}{2p - 1} = x$$

برای محاسبه واریانس، چون y یک متغیر برنولی است، واریانس آن $(p - 1)p$ می‌شود. با اعمال خواص واریانس ($\text{Var}[aY + b] = a^2 \text{Var}[Y]$) داریم:

$$\text{Var}[\hat{x}] = \frac{\text{Var}[y]}{(2p - 1)^2} = \frac{p(1 - p)}{(2p - 1)^2}$$

حال با جایگذاری $p = \frac{e^\alpha}{e^\alpha + 1}$ در رابطه بالا:

$$\text{Var}[\hat{x}] = \frac{\frac{e^\alpha}{(e^\alpha + 1)^2}}{\left(\frac{e^\alpha - 1}{e^\alpha + 1} - 1\right)^2} = \frac{\frac{e^\alpha}{(e^\alpha + 1)^2}}{\left(\frac{e^\alpha - 1}{e^\alpha + 1}\right)^2} = \frac{e^\alpha}{(e^\alpha - 1)^2}$$

□

۲-۴-۳ پاسخ تصادفی تعمیم‌یافته (GRR)

پاسخ تصادفی تعمیم‌یافته^{۱۰}، برای دامنه‌های گسسته با $k > 2$ عنصر ($\mathcal{X} = \{1, \dots, k\}$)، به عنوان تعمیم مستقیم RR معرفی می‌شود. این مکانیزم را می‌توان با یک «ماتریس گذار»^{۱۱} تصادفی $Q \in [0, 1]^{k \times k}$ توصیف کرد.

تعریف ۴-۳ (ماتریس احتمال GRR) در مکانیزم GRR، ماتریس احتمال شرطی Q که درایه (i, j) آن برابر با $\mathbb{P}[z = j | x = i]$ است، به صورت زیر تعریف می‌شود:

$$Q = \begin{pmatrix} p & q & \dots & q \\ q & p & \dots & q \\ \vdots & \vdots & \ddots & \vdots \\ q & q & \dots & p \end{pmatrix}_{k \times k} \quad (12-3)$$

که در آن p احتمال گزارش صادقانه و q احتمال گزارش هر یک از $1 - k$ گزینه‌ی دیگر است.

به صورت مشابه RR می‌توان نشان داد که مقادیر بهینه برای ارضای شرط α -LDP عبارتند از:

$$p = \frac{e^\alpha}{e^\alpha + k - 1}, \quad q = \frac{1}{e^\alpha + k - 1} \quad (13-3)$$

برای تخمین فراوانی یک آیتم خاص $v \in \mathcal{X}$ ، از تخمین‌گر ناریب $\hat{c}_v = \frac{\mathbb{I}(z=v)-q}{p-q}$ استفاده می‌شود. با تحلیلی مشابه لم^{۱۲}، واریانس این تخمین‌گر برابر خواهد بود با:

$$\text{Var}_{GRR} = \frac{p(1-p)}{(p-q)^2} = \frac{(e^\alpha)(k-1) + (k-1)^2}{(e^\alpha - 1)^2} \approx \mathcal{O}(k) \quad (14-3)$$

این رابطه نشان می‌دهد که واریانس GRR وابستگی خطی به اندازه دامنه k دارد که نقطه ضعف این روش در ابعاد بالاست.

۳-۴-۳ مکانیزم‌های مبتنی بر کدگذاری یگانی (UE)

برای غلبه بر مشکل کاهش دقت GRR در دامنه‌های بزرگ، خانواده‌ای از مکانیزم‌ها تحت عنوان «کدگذاری یگانی»^{۱۳} توسعه یافته‌اند. این رویکرد اساس پروتکل مشهور RAPPOR گوگل را تشکیل می‌دهد [۱۴، ۲۲].

¹⁰Generalized Randomized Response

¹¹Transition Matrix

¹²Unary Encoding (UE)

تعريف ۵-۳ (کدگذاری یگانی) در این روش، فرآیند خصوصی‌سازی طی دو مرحله انجام می‌شود:

۱. **کدگذاری قطعی:** ورودی $\{1, \dots, k\}^k$ به یک بردار بیتی $v \in \{0, 1\}^k$ تبدیل می‌شود که تنها در موقعیت x برابر با ۱ و در سایر جاهای ۰ است (*One-hot encoding*).

۲. **اختلال^{۱۳} مستقل:** هر بیت این بردار به صورت مستقل با استفاده از یک مکانیزم باینری معکوس می‌شود. اگر v_i بیت i -ام بردار کدگذاری شده باشد، خروجی z_i به صورت زیر تولید می‌شود:

$$\mathbb{P}[z_i = 1] = \begin{cases} p & \text{if } v_i = 1 \\ q & \text{if } v_i = 0 \end{cases} \quad (15-3)$$

مثال ۱-۳ فرض کنید دامنه شامل ۴ آیتم باشد ($\mathcal{X} = \{1, 2, 3, 4\}$) و ورودی کاربر $x = 2$ باشد.

۱. بردار کدگذاری شده: $v = [0, 0, 1, 0]$

۲. اعمال نویز: هر بیت مستقل پرتاب می‌شود. ممکن است خروجی نهایی $[0, 1, 1, 0] = z$ شود (بیت سوم از ۰ به ۱ تغییر کرده است).

اثبات α -LDP: برای بررسی شرط α -LDP، نسبت احتمال خروجی برداری $(z_1, \dots, z_k) = z$ را برای دو ورودی متمایز x و x' محاسبه می‌کنیم. بردارهای متناظر v و v' تنها در دو موقعیت تفاوت دارند: موقعیت x (که $v_x = 1, v'_x = 0$) و موقعیت x' (که $v_{x'} = 0, v'_{x'} = 1$). در سایر موقعیت‌ها ($j \neq x, x'$) بیت‌ها یکسان و برابر صفر هستند و در نسبت احتمالات ساده می‌شوند. از آنجا که بیت‌ها مستقل هستند:

$$\frac{\mathbb{P}[z|x]}{\mathbb{P}[z|x']} = \frac{\mathbb{P}[z_x|v_x = 1] \cdot \mathbb{P}[z_{x'}|v_{x'} = 0]}{\mathbb{P}[z_x|v'_x = 0] \cdot \mathbb{P}[z_{x'}|v'_{x'} = 1]} \quad (16-3)$$

بیشینه‌ی این کسر زمانی رخ می‌دهد که صورت کسر ماکزیمم و مخرج مینیمم شود؛ یعنی زمانی که $z_x = 1$ (حفظ بیت ۱) و $z_{x'} = 0$ (حفظ بیت ۰) باشد. در این حالت:

$$\frac{\mathbb{P}[z|x]}{\mathbb{P}[z|x']} \leq \frac{p}{q} \cdot \frac{1-q}{1-p} = \frac{p(1-q)}{q(1-p)} \quad (17-3)$$

بنابراین شرط α -LDP معادل است با:

$$\alpha = \ln \left(\frac{p(1-q)}{q(1-p)} \right) \quad (18-3)$$

¹³Perturbation

لم ۳-۳ (تحلیل واریانس UE) در پروتکل‌های UE، واریانس تخمین فراوانی برای هر آیتم، تنها به پارامترهای p و q وابسته است و از رابطه زیر پیروی می‌کند:

$$\text{Var}_{UE} = \frac{q(1-q)}{(p-q)^2} \quad (19-3)$$

(نکته: این واریانس برای حالتی است که ورودی واقعی کاربر آن آیتم نباشد، که در دامنه‌های بزرگ حالت غالب است).

دو استراتژی اصلی برای تنظیم p و q بر اساس رابطه (۱۸-۳) وجود دارد:

۱. کدگذاری یگانی متقارن (SUE): در این روش $1 + q = p$ در نظر گرفته می‌شود. با جایگذاری در شرط α -LDP، مقادیر بهینه عبارتند از $p = \frac{1}{e^{\alpha/2} + 1}$ و $q = \frac{e^{\alpha/2}}{e^{\alpha/2} + 1}$. واریانس در این حالت برابر است با:

$$\text{Var}_{SUE} = \frac{e^{\alpha/2}}{(e^{\alpha/2} - 1)^2} \quad (20-3)$$

۲. کدگذاری یگانی بهینه (OUE): وانگ و همکاران [۲۲] نشان دادند که برای کمینه‌سازی واریانس در دامنه‌های بزرگ، باید اطلاعات بیت‌های ۱ (سیگنال) حفظ شود ($p = 1/2$) و نویز روی بیت‌های ۰ (که اکثر بردار را تشکیل می‌دهند) کنترل شود ($q = \frac{1}{e^\alpha + 1}$). واریانس حاصل برابر است با:

$$\text{Var}_{OUE} = \frac{4e^\alpha}{(e^\alpha - 1)^2} \quad (21-3)$$

۴-۴-۳ تحلیل مقایسه‌ای: چرا GRR در ابعاد بالا شکست می‌خورد؟

یکی از مهم‌ترین نتایج نظری در ادبیات LDP، مقایسه رفتار معجانبی GRR و OUE نسبت به اندازه دامنه k است.

مثال ۲-۳ (ناکارآمدی GRR در دامنه‌های بزرگ) فرض کنید می‌خواهیم کلمات پرکاربرد را از یک لغت‌نامه با $k = 100,000$ کلمه استخراج کنیم.

- در مکانیزم GRR، طبق رابطه (۱۴-۳)، واریانس تقریباً با k رشد می‌کند:

$$\text{Var}_{GRR} \approx \frac{k}{(e^\alpha - 1)^2}$$

به عبارتی، نویز اضافه شده متناسب با کل اندازه دیکشنری است که سیگنال کلمات نادر را کاملاً محروم می‌کند.

- در مکانیزم OUE ، واریانس مستقل از k است:

$$\text{Var}_{OUE} = \frac{4e^\alpha}{(e^\alpha - 1)^2}$$

این استقلال از k باعث می‌شود که خانواده UE گزینه‌ی برتر برای دامنه‌های بزرگ باشند. با این حال، OUE هزینه مخابراتی بالایی دارد (ارسال بردار با طول k). برای رفع این مشکل، نسخه بهبودیافته‌ای به نام «درهم‌سازی موضعی بجهینه^{۱۴}» توسط وانگ و همکاران [۲۳] معرفی شده است. این روش با استفاده از توابع درهم‌ساز، ورودی را فشرده کرده و بدون افزایش واریانس، هزینه مخابراتی را کاهش می‌دهد.

۵-۴-۳ مکانیزم لاپلاس موضعی

برای داده‌های عددی پیوسته، رویکرد استاندارد تعمیم مکانیزم لاپلاس از مدل متمرکز به مدل موضعی است. فرض کنید دامنه ورودی یک بازه‌ی کران دار $\mathbb{R} \subset \mathcal{X}$ باشد. بدون کاستن از کلیت^{۱۵}، فرض می‌کنیم داده‌ها با یک تبدیل خطی به بازه‌ی $[1, -1]$ نگاشت شده‌اند. در مدل موضعی، شرط محترمانگی باید برای هر جفت ورودی $x, x' \in \mathcal{X}$ برابر با قطر دامنه است. در این صورت Δ ، بیشترین مقدار ممکن را خواهد داشت:

$$\Delta = \sup_{x, x' \in [-1, 1]} |x - x'| = |1 - (-1)| = 2 \quad (22-3)$$

تعريف ۳-۶ (مکانیزم لاپلاس موضعی) مکانیزم \mathcal{M}_{Lap} ورودی نرمالایز شده $[1, -1] \in x$ را دریافت کرده و خروجی z را طبق رابطه زیر تولید می‌کند:

$$z = x + \eta, \quad \eta \sim \text{Lap}\left(\frac{\Delta}{\alpha}\right) = \text{Lap}\left(\frac{2}{\alpha}\right) \quad (23-3)$$

تابع چگالی احتمال (PDF) خروجی برای ورودی x به صورت زیر است:

$$f(z|x) = \frac{\alpha}{2} \exp\left(-\frac{\alpha|z-x|}{2}\right) \quad (24-3)$$

اثبات α -LDP: برای هر دو ورودی x, x' و هر خروجی z ، نسبت چگالی‌ها عبارت است از:

$$\frac{f(z|x)}{f(z|x')} = \frac{\exp\left(-\frac{\alpha}{2}|z-x|\right)}{\exp\left(-\frac{\alpha}{2}|z-x'|\right)} \quad (25-3)$$

$$= \exp\left(\frac{\alpha}{2}(|z-x'| - |z-x|)\right) \quad (26-3)$$

¹⁴Optimized Local Hashing (OLH)

¹⁵Without Loss of Generality

طبق نامساوی مثلثی معکوس ($|a| - |b| \leq |a - b|$):

$$|z - x'| - |z - x| \leq |(z - x') - (z - x)| = |x - x'| \leq 2$$

بنابراین نسبت احتمال با $\exp\left(\frac{\alpha}{2} \cdot 2\right) = e^\alpha$ کران دار می‌شود.

مثال ۳-۳ فرض کنید می‌خواهیم دمای بدن یک بیمار را گزارش کنیم. اگر دامنه تغییرات دما $[35, 42]$ درجه باشد، طول بازه $7 = 42 - 35$ است. اگر بدون نرم‌السازی از لایپلاس استفاده کنیم، باید نویزی متناسب با $\frac{7}{\alpha}$ اضافه کنیم. اما در روش استاندارد، ابتدا دما را به $[1, 1] -$ نگاشت می‌کنیم (که حساسیت ۲ شود)، نویز با مقیاس $\frac{2}{\alpha}$ اضافه می‌کنیم و در سمت سرور مجدد نتیجه را به مقیاس اصلی بر می‌گردانیم. حال اگر بخواهیم دمای بدن یک بیمار را که به بازه $[1, 1] -$ نرم‌الایز شده است، با بودجه $\alpha = 1$ منتشر کنیم. اگر مقدار واقعی $x = 0/5$ باشد:

- مقیاس نویز برابر است با $b = \frac{2}{1} = 2$.

- یک نمونه تصادفی ممکن است $z = -0/7 = -0.5 + 1/2$ باشد.

- واریانس خطای برابر است با $s^2 = 2b^2 = 2 \cdot 1^2 = 2$. این واریانس برای یک مقدار در بازه $[1, 1] -$ بسیار زیاد است و نشان می‌دهد که LDP برای داده‌های عددی تک بعدی خطای زیادی تحمیل می‌کند مگر اینکه n (تعداد کاربران) بسیار زیاد باشد.

چالش ابعاد بالا (نفرین ابعاد)

چرا در ابعاد بالا ($d > 1$) از مکانیزم لایپلاس استفاده نمی‌شود؟ فرض کنید ورودی کاربر یک بردار $x \in \mathbb{R}^d$ باشد که در توپ واحد اقلیدسی قرار دارد ($\|x\|_2 \leq 1$).

مشکل بنیادین این است که مکانیزم لایپلاس متنکی بر حساسیت در فضای ℓ_1 است، در حالی که هندسه فضای برداری اقلیدسی منطبق بر ℓ_2 می‌باشد. برای پوشش دادن توپ واحد ℓ_2 با نویز لایپلاس، باید حساسیت ℓ_1 را در بدترین حالت در نظر بگیریم. می‌دانیم برای هر بردار با نرم اقلیدسی ۱، نرم ℓ_1 می‌تواند تا \sqrt{d} رشد کند. بنابراین قطر دامنه در متر ℓ_1 برابر است با:

$$\Delta_{\ell_1} = \sup_{x, x' \in B_{\ell_1}} \|x - x'\|_1 \leq \sqrt{d} \cdot \sup \|x - x'\|_2 = \sqrt{d} \quad (27-3)$$

برای تأمین α -LDP، باید به هر مؤلفه نویزی مستقل با مقیاس $\frac{2\sqrt{d}}{\alpha}$ اضافه کنیم. در نتیجه:

$$\bullet \text{ واریانس خطای خطا در هر بُعد: } 2 \times \left(\frac{\sqrt{d}}{\alpha} \right)^2 = \frac{8d}{\alpha^2}$$

$$\bullet \text{ خطای میانگین مربعات کل } ^{16} \text{ برای } d \text{ بُعد: } d \times \frac{8d}{\alpha^2} = \frac{8d^2}{\alpha^2}$$

این نرخ رشد $O(d^2)$ برای خطای خطا، بسیار ناکارآمد است. دوچی و همکاران [A] ثابت کردند که حد پایین نظری مینی‌مکس برای این مسئله $O(d)$ است. به همین دلیل، در ابعاد بالا از مکانیزم‌های پیشرفته‌تری مانند «توزیع برنولی چندبعدی» یا «نمونه‌برداری هایپرکیوب» استفاده می‌شود که با هندسه فضای سازگارترند.

مقایسه با مدل متمرکز: در مثال ۲-۶ فصل قبل دیدیم که در مدل متمرکز، مکانیزم لایپلاس با افزایش ابعاد (d) دچار افت کارایی می‌شود و نویز با ضریب d رشد می‌کند (که با استفاده از مکانیزم گوسی به \sqrt{d} کاهش می‌یابد). اما در مدل موضوعی، این پدیده بسیار شدیدتر است. در اینجا نه تنها نویز با d رشد می‌کند، بلکه به دلیل عدم تمرکز و جمع شدن خطاهای تک‌تک کاربران، خطای نهایی (MSE) با d^2 افزایش می‌یابد. به همین دلیل، راهکارهای ساده‌ی مدل متمرکز (مانند افزودن نویز به هر بعد) در مدل موضوعی تقریباً بلااستفاده هستند.

۵-۳ چالش سودمندی و هزینه عدم اعتماد

همان‌طور که دیدیم، مدل LDP گلوگاه اعتماد به سرور مرکزی را حذف می‌کند. اما این افزایش امنیت بدون هزینه نیست. در این بخش، با یک تحلیل دقیق ریاضی نشان می‌دهیم که حذف متصدی مورد اعتماد منجر به کاهش شدید دقت آماری (سودمندی) می‌شود. برای این منظور، ساده‌ترین مسئله آماری یعنی «تخمین میانگین جامعه» را در دو مدل متمرکز و موضوعی مقایسه می‌کنیم.

۱-۵-۳ تعریف مسئله: تخمین میانگین دودویی

فرض کنید n کاربر وجود دارند و هر کاربر i دارای یک بیت خصوصی $\{0, 1\} \in X_i$ است. هدف تخمین‌گر، محاسبه‌ی میانگین واقعی جامعه است:

$$p = \frac{1}{n} \sum_{i=1}^n X_i \quad (28-3)$$

معیار ارزیابی ما، خطای میانگین مربعات تخمین‌گر \hat{p} خواهد بود:

$$\text{MSE}(\hat{p}) = \mathbb{E} [(\hat{p} - p)^2] = \text{Var}[\hat{p}] + (\text{Bias}[\hat{p}])^2 \quad (29-3)$$

¹⁶Mean Squared Error (MSE)

ما در هر دو مدل از تخمین‌گرهای نااریب ($Bias = 0$) استفاده می‌کنیم، بنابراین خطأ صرفاً ناشی از واریانس نویز تزریق شده است.

۲-۵-۳ تحلیل در مدل متمرکز (CDP)

در مدل متمرکز با بودجه محروم‌گی $\text{DP}-\varepsilon$ ، متصلی به تمام X_i ‌ها دسترسی دارد. او ابتدا مقدار دقیق مجموع $\sum X_i$ را محاسبه می‌کند. چون تغییر یک بیت حداقل مجموع را 1 واحد تغییر می‌دهد، حساسیت سراسری برابر با $1 = \Delta$ است. طبق مکانیزم لاپلاس، نویزی با مقیاس $1/\varepsilon$ به مجموع اضافه شده و سپس بر n تقسیم می‌شود تا میانگین به دست آید:

$$\hat{p}_{CDP} = \frac{1}{n} \left(\sum_{i=1}^n X_i + \eta \right), \quad \eta \sim \text{Lap}(1/\varepsilon) \quad (30-3)$$

خطای این تخمین‌گر برابر است با:

$$\text{MSE}_{CDP} = \text{Var} \left[\frac{\eta}{n} \right] = \frac{1}{n^2} \text{Var}[\eta] = \frac{1}{n^2} \cdot \frac{2}{\varepsilon^2} = \mathcal{O} \left(\frac{1}{n^2 \varepsilon^2} \right) \quad (31-3)$$

این رابطه نشان می‌دهد که در مدل متمرکز، خطأ با سرعت $1/n$ به سمت صفر میل می‌کند (یا انحراف معیار با سرعت $1/n$).

۳-۵-۳ تحلیل در مدل موضعی (LDP)

در مدل موضعی با محدودیت LDP، هیچ‌کس به X_i ‌های خام دسترسی ندارد. هر کاربر به صورت مستقل مکانیزم پاسخ تصادفی (RR) را روی داده خود اجرا می‌کند و \hat{X}_i را گزارش می‌دهد. طبق نتایج بخش ۱-۴-۳، واریانس تخمین‌گر هر کاربر برای α ‌های کوچک ($1 < \alpha$) تقریباً برابر است با:

$$\text{Var}[\hat{X}_i] \approx \frac{1}{\alpha^2} \quad (32-3)$$

متصلی برای تخمین میانگین کل، میانگین گزارش‌های دریافتی را محاسبه می‌کند: $\hat{p}_{LDP} = \frac{1}{n} \sum_{i=1}^n \hat{X}_i$. از آنجا که نویز کاربران مستقل از یکدیگر است، واریانس مجموع برابر با مجموع واریانس‌هاست:

$$\text{MSE}_{LDP} = \text{Var} \left[\frac{1}{n} \sum_{i=1}^n \hat{X}_i \right] = \frac{1}{n^2} \sum_{i=1}^n \text{Var}[\hat{X}_i] = \frac{1}{n^2} \cdot n \cdot \mathcal{O} \left(\frac{1}{\alpha^2} \right) = \mathcal{O} \left(\frac{1}{n \alpha^2} \right) \quad (33-3)$$

در اینجا خطأ با سرعت $1/\sqrt{n}$ به سمت صفر میل می‌کند.

۴-۵-۳ نتیجه‌گیری: شکاف کارایی

با مقایسه روابط (۳۱-۳) و (۳۲-۳)، تفاوت بین این دو مدل آشکار می‌شود (با فرض ثابت بودن بودجه‌های محرمانگی $\alpha \approx \varepsilon$):

- مدل متتمرکز: نرخ همگرایی خطأ $\mathcal{O}(1/n)$ است.

- مدل موضعی: نرخ همگرایی خطأ $\mathcal{O}(1/\sqrt{n})$ است.

این تفاوت در نرخ همگرایی پیامد بسیار مهمی در حجم نمونه^{۱۷} مورد نیاز دارد. برای رسیدن به یک دقت ثابت مشخص (مثلًاً خطای τ ، تعداد کاربران مورد نیاز در هر مدل عبارت است از:

$$n_{CDP} \propto \frac{1}{\tau}, \quad n_{LDP} \propto \frac{1}{\tau^2} \quad (34-3)$$

بنابراین رابطه بین حجم داده مورد نیاز در دو مدل به صورت زیر است:

$$n_{LDP} \approx \mathcal{O}(n_{CDP}^2) \quad (35-3)$$

این رابطه که در ادبیات موضوع به «هزینه عدم اعتماد» شهرت دارد، نشان می‌دهد که مدل موضعی برای رسیدن به دقتی مشابه مدل متتمرکز، نیازمند داده‌های بسیار بیشتری است. برای مثال، اگر در مدل متتمرکز با ۱,۰۰۰ کاربر به دقت مطلوبی برسیم، در مدل موضعی برای همان دقت به ۱,۰۰۰,۰۰۰ کاربر نیاز خواهیم داشت [۱۴، ۸].

همین شکاف عظیم است که انگیزه اصلی فصل‌های آینده‌ی این پایان‌نامه را شکل می‌دهد: «چگونه می‌توان با استفاده از تحلیل‌های دقیق‌تر (مانند واگرایی‌های f) و الگوریتم‌های بهینه، ثابت‌های پنهان در این حدود را بهبود بخشد؟»

¹⁷Sample Complexity

فصل ۴

تحلیل‌های مبتنی بر انقباض و نرخ‌های مینی‌مکس

۱-۴ مقدمه

در فصل پیشین، تعاریف پایه محرمانگی تفاضلی موضعی (LDP) و مکانیزم‌های ابتدایی آن را بررسی کردیم. همان‌طور که دیدیم، چالش اصلی در مدل موضعی، کاهش شدید نسبت سیگنال به نویز است. برای تحلیل دقیق این پدیده و یافتن حدود نهایی دقت آماری، نیازمند ابزارهای قوی‌تری هستیم.

در این فصل، به بررسی چارچوب نظری استانداردی می‌پردازیم که توسط دوچی و همکاران [۸] توسعه داده شده است. ایده مرکزی این چارچوب، نگاه به مکانیزم‌های محرمانگی به عنوان «عملگرهای انقباضی»^۱ است. به بیان شهودی، اعمال شرط LDP باعث می‌شود که توزیع‌های خروجی $(x|M)$ و $(x'|M)$ بسیار به یکدیگر شبیه شوند، حتی اگر ورودی‌های x و x' کاملاً متفاوت باشند.

ما نشان خواهیم داد که چگونه می‌توان این شباهت اجباری را با استفاده از نامساوی‌های پردازش داده و f -واگرایی‌ها (به‌ویژه واگرایی کولبک-لایلر) مدل‌سازی کرد و از آن برای اثبات نرخ‌های مینی‌مکس در مسائل تخمین آماری استفاده نمود [۸].

۲-۴ محرمانگی به عنوان انقباض اطلاعاتی

یکی از ویژگی‌های بنیادین نظریه اطلاعات، «نامساوی پردازش داده»^۲ است که بیان می‌کند پردازش روی داده‌ها (بدون دسترسی به منبع اصلی) نمی‌تواند اطلاعات متقابل را افزایش دهد. در زمینه محرمانگی، ما

¹Contraction Operators

²Data Processing Inequality

با نسخه قوی‌تری از این مفهوم سروکار داریم که به آن «نامساوی قوی پردازش داده»^۳ می‌گویند [۳].

فرض کنید M یک مکانیزم $\text{LDP}-\alpha$ -بашد. هدف ما یافتن کرانی برای واگرایی بین توزیع‌های خروجی بر حسب واگرایی ورودی‌هاست. دوچی و همکاران نشان دادند که مکانیزم‌های موضعی باعث انقباض شدید در واگرایی KL می‌شوند.

قضیه ۱-۴ (انقباض KL در مکانیزم‌های موضعی) فرض کنید M یک مکانیزم $\text{LDP}-\alpha$ -باشد. برای هر دو ورودی $x, x' \in \mathcal{X}$, واگرایی کولبک-لایلر بین توزیع‌های خروجی متناظر $M(\cdot|x)$ و $M(\cdot|x')$ با رابطه زیر محدود می‌شود:

$$D_{KL}(M(\cdot|x) \| M(\cdot|x')) \leq 4(e^\alpha - 1)^2 \quad (1-4)$$

به طور دقیق‌تر، اگر $1 \leq \alpha$ باشد، این کران به صورت $O(\alpha^2)$ رفتار می‌کند [۱].

اثبات. برای اثبات دقیق این قضیه، از تعریف واگرایی KL شروع می‌کنیم. فرض کنید $(z|x)$ و $(z|x')$ چگالی‌های احتمال خروجی باشند. طبق تعریف $\text{LDP}-\alpha$ -می‌دانیم که برای هر $z \in \mathcal{Z}$:

$$e^{-\alpha} \leq \frac{q(z|x)}{q(z|x')} \leq e^\alpha \quad (2-4)$$

این شرط تضمین می‌کند که نسبت درست‌نمایی‌ها حول عدد ۱ محدود است. با بسط تیلور تابع $\log t$ حول $t = 1$ و استفاده از خواص تحدب، می‌توان نشان داد که:

$$D_{KL}(P \| Q) = \int p(z) \log \frac{p(z)}{q(z)} dz \quad (3-4)$$

$$\leq \int p(z) \left(\frac{p(z)}{q(z)} - 1 + \frac{1}{2} \left(\frac{p(z)}{q(z)} - 1 \right)^2 \right) dz \quad (4-4)$$

با اعمال کران‌های $\text{LDP}-\alpha$ -بر روی نسبت p/q ، جمله درجه اول صفر می‌شود و جمله درجه دوم ضریب $(1 - e^\alpha)^2$ را تولید می‌کند. جزئیات کامل این محاسبات در لم ۱ مقاله [۱] آمده است. نکته کلیدی این است که برای α کوچک، فاصله KL به صورت مربعی با α کاهش می‌یابد. \square

این قضیه ابزار بسیار قدرتمندی است. به جای اینکه مستقیماً با تعریف دشوار $\text{LDP}-\alpha$ -کار کنیم، می‌توانیم از این کران ساده در نامساوی‌هایی مثل فانو استفاده کنیم. همچنین مطالعات جدیدتر نشان داده‌اند که این انقباض را می‌توان با استفاده از معیارهای دیگری نظیر اطلاعات متقابل [۵] یا واگرایی E_γ [۲] نیز بیان کرد که در فصل بعد به آن می‌پردازیم.

³Strong Data Processing Inequality (SDPI)

۴-۲-۱ انقباض در فاصله واریانس کل

علاوه بر KL، کران مشابهی برای فاصله واریانس کل (TV) نیز ارائه شده است که در استفاده از روش «لم لو کم^۴» کاربرد دارد [۸]:

قضیه‌ی ۴-۲ (انقباض TV) تحت شرایط مشابه، برای هر مکانیزم α -LDP:

$$\|\mathcal{M}(\cdot|x) - \mathcal{M}(\cdot|x')\|_{TV} \leq \min\{1, e^\alpha - 1\} \cdot \|x - x'\|. \quad (5-4)$$

(در اینجا $\|x - x'\|$ نشان‌دهنده فاصله همینگ یا متريک مجزا روی ورودی است). برای α کوچک، اين رابطه بيان می‌کند که فاصله آماری خروجي‌ها نمی‌تواند بيشتر از $O(\alpha)$ باشد.

۳-۴ تحليل نرخ‌های ميني‌مكس با استفاده از انقباض

حال که ابزار انقباض را در اختیار داریم، می‌توانیم استراتژی کلی اثبات حدود پایین^۵ در مدل موضعی را صورت‌بندی کنیم. این استراتژی که توسط دوچی [۸] و بعدها با جزئیات بیشتر در [۹] بسط داده شد، شامل سه گام است:

۱. تقلیل به آزمون فرض: تبدیل مسئله تخمین پارامتر θ به مسئله تشخیص اندیس V در یک مجموعه متناهی (استفاده از LM فانو یا اسود).

۲. کران‌دار کردن اطلاعات متقابل: استفاده از خاصیت انقباض α -LDP برای محدود کردن اطلاعاتی که نمونه‌های مشاهده شده Z_1, \dots, Z_n درباره اندیس V می‌دهند [۵].

۳. محاسبه ريسک نهايی: ترکيب نتایج برای رسيدن به کران پایين خطای تخمین.

مهم‌ترین گام، گام دوم است. طبق نامساوی قوى پردازش داده برای مدل موضعی، داریم:

$$I(V; Z^n) \leq \sum_{i=1}^n I(V; Z_i) \leq n \cdot \alpha^2 \cdot C \quad (6-4)$$

که در آن C ثابتی است که به هندسه مسئله بستگی دارد. این رابطه نشان می‌دهد که اطلاعات موثر با نرخ $n\alpha^2$ رشد می‌کند، نه n . این همان دليلی است که «اندازه نمونه موثر» در مدل موضعی برابر با $n\alpha^2$ در نظر گرفته می‌شود.

⁴Le Cam

⁵Lower Bounds

۴-۴ مطالعه موردی: تخمین میانگین

برای نمایش قدرت این چارچوب، مسئله کلاسیک تخمین میانگین را در نظر می‌گیریم. فرض کنید هر کاربر i برداری $X_i \in [-1, 1]^d$ دارد و هدف تخمین میانگین جامعه $\mu = \mathbb{E}_X$ است. معیار خطا را «میانگین مربعات خطای مدل» (MSE) در نظر می‌گیریم.

قضیه ۳-۴ (کران پایین تخمین میانگین) برای هر مکانیزم $LDP-\alpha$ -هر تخمین گرفته، ماکسیمم خطای مورد انتظار با رابطه زیر محدود می‌شود [۱]:

$$\inf_{\hat{\mu}, \mathcal{M}} \sup_P \mathbb{E}_{\|\hat{\mu} - \mu\|^2} \geq \Omega \left(\frac{d}{n \min\{\alpha, \alpha^2\}} \right) \quad (7-4)$$

تحلیل اثبات: برای اثبات این کران، از لم اسود استفاده می‌کنیم. فضای پارامتر را به صورت یک ابرمکعب $\{-1, 1\}^d$ گسترش می‌کنیم. طبق لم اسود، خطای مجموع فاصله‌های TV بین توزیع‌های شرطی مرتبط است. با استفاده از قضیه انقباض ۱-۴ و نامساوی پینسکر، می‌دانیم که:

$$\|\mathcal{M}(\cdot|x) - \mathcal{M}(\cdot|x')\|_{TV}^2 \leq \frac{1}{\alpha} D_{KL}(\mathcal{M}(\cdot|x) || \mathcal{M}(\cdot|x')) \leq O(\alpha^2) \quad (8-4)$$

بنابراین فاصله TV حداکثر از مرتبه α است. با جایگذاری این مقدار در لم اسود، کران پایین $\frac{1}{n\alpha^2}$ حاصل می‌شود.

این نتیجه نشان می‌دهد که برای رسیدن به خطای کم در مدل موضعی، تعداد داده‌ها باید متناسب با α^2/α افزایش یابد، که هزینه‌ی بسیار سنگین‌تری نسبت به مدل متغیر (که متناسب با $1/\varepsilon$ است) دارد.

۵-۴ محدودیت‌های تحلیل کلاسیک

با وجود موفقیت چارچوب دوچی در اثبات نرخ‌های مینی‌مکس بهینه برای α ‌های کوچک (رزیم محربمانگی بالا)، این روش در رزیم α ‌های بزرگ (محربمانگی پایین) دچار ضعف است.

همان‌طور که در رابطه (۱-۴) دیدیم، کران انقباض KL با ضریب $(1 - e^\alpha)^2$ رشد می‌کند. زمانی که α بزرگ باشد، این کران به سرعت به بینهایت می‌کند و اطلاعاتی فراتر از کران بدیهی به ما نمی‌دهد. این در حالی است که به طور شهودی، حتی با α بزرگ، مکانیزم همچنان باید مقداری انقباض ایجاد کند.

این محدودیت ناشی از ذات واگرایی KL است که رفتار دنباله‌های توزیع را با حساسیت زیادی وزن دهدی می‌کند. برای رفع این مشکل و به دست آوردن تحلیل‌های دقیق‌تر^۶ که در تمام بازه‌های α معتبر باشند، نیازمند

⁶Tight

معیار هندسی متفاوتی هستیم. این نیاز، انگیزه اصلی معرفی واگرایی‌های جدید مانند f – واگرایی‌های خاص (نظیر E_γ) است [۲، ۳] که در فصل آینده به تفصیل به آن خواهیم پرداخت.

فصل ۵

همارزی LDP و انقباض E_γ -واگرایی

۱-۵ مقدمه و انگیزه

در فصل پیشین، دیدیم که چگونه دوچی و همکاران [۱] از واگرایی کولبک-لایلر (KL) برای تحلیل محترمانگی تفاضلی موضعی استفاده کردند. اگرچه کرانهای آنها برای رژیم‌های محترمانگی بالا (α کوچک) بسیار کارآمد هستند، اما در رژیم‌های α متوسط و بزرگ، دقت خود را از دست می‌دهند.

مشکل اصلی در آنجاست که واگرایی KL متريک «بومی» برای تعريف α -LDP- α نیست. تعريف α -LDP (معادله $??$) مبنی بر نسبت احتمالات است، در حالی که KL مبنی بر لگاريتم نسبت‌هاست. اين نامخوانی باعث می‌شود که در تبدیل شرایط α -LDP به کرانهای KL، اطلاعاتی از دست برود (lossy conversion).

در اين فصل، نشان می‌دهيم که يك معيار واگرایی دیگر به نام E_γ -واگرایی وجود دارد که دقیقاً ساختار هندسى α -LDP را تسخیر می‌کند. ما ثابت خواهیم کرد که شرط E_γ -واگرایی معادل صفر شدن سایر واگرایی‌ها است. سپس از اين همارزی برای استخراج کرانهای انقباض دقیق^۱ برای E_γ -واگرایی (برای $e^\alpha = \gamma$) است. سپس از اين همارزی برای استخراج کرانهای انقباض دقیق^۲.

¹Tight

۲-۵ معرفی E_γ -واگرایی

-واگرایی یکی از اعضای کمتر شناخته شدهی خانواده f -واگرایی هاست که در نظریه اطلاعات برای مقایسه نسبت درست نمایی توزیع‌ها کاربرد دارد.

تعريف ۱-۵ (-واگرایی) فرض کنید P و Q دو توزیع احتمال باشند و $1 \geq \gamma \geq 0$ یک عدد حقیقی باشد.
-واگرایی بین P و Q به صورت زیر تعریف می‌شود:

$$E_\gamma(P||Q) = \sup_{\mathcal{S} \in \sigma(\mathcal{X})} (P(\mathcal{S}) - \gamma Q(\mathcal{S})) \quad (1-5)$$

این تعریف را می‌توان به صورت بسطه‌ی زیر نیز نوشت:

$$E_\gamma(P||Q) = \int_{\mathcal{X}} \max\{\cdot, p(x) - \gamma q(x)\} d\mu(x) \quad (2-5)$$

که در آن p و q توابع چگالی احتمال هستند.

۱-۲-۵ خواص هندسی

این واگرایی خواص جالبی دارد که آن را برای تحلیل محروم‌نگی ایده‌آل می‌کند:

- ارتباط با فاصله واریانس کل: اگر $\gamma = 1$ باشد، داریم:

$$E_1(P||Q) = \sup_{\mathcal{S}} (P(\mathcal{S}) - Q(\mathcal{S})) = \|P - Q\|_{TV} \quad (3-5)$$

بنابراین E_γ تعمیمی از فاصله TV است.

- غیرمنفی بودن: همواره $E_\gamma(P||Q) \geq 0$ نیست. در واقع، اگر نسبت $p(x)/q(x)$ همواره کمتر از γ باشد، این مقدار صفر می‌شود. دقیقاً همین ویژگی است که آن را به α -LDP-مرتبه می‌کند.

۳-۵ قضیه همارزی اصلی

اکنون به مهم‌ترین نتیجه‌ی نظری این پایان‌نامه می‌رسیم: اثبات اینکه α -LDP-چیزی جز محدودیت بر روی -واگرایی نیست.

قضیه‌ی ۱-۵ (همارزی- LDP_{α} و E_{γ}) یک مکانیزم \mathcal{M} در شرط LDP_{α} -صدق می‌کند اگر و تنها اگر برای تمام جفت ورودی‌های $x, x' \in \mathcal{X}$

$$E_{e^{\alpha}}(\mathcal{M}(\cdot|x)||\mathcal{M}(\cdot|x')) = 0 \quad (4-5)$$

اثبات. اثبات را در دو جهت انجام می‌دهیم.

جهت اول (\Rightarrow): فرض کنید \mathcal{M} خاصیت LDP_{α} -دارد. طبق تعریف ۲-۳، برای هر زیرمجموعه خروجی $\mathcal{S} \subseteq \mathcal{Z}$ و هر $x, x' \in \mathcal{S}$:

$$\Pr[\mathcal{M}(x) \in \mathcal{S}] \leq e^{\alpha} \Pr[\mathcal{M}(x') \in \mathcal{S}] \quad (5-5)$$

این نامساوی را می‌توان به صورت زیر بازنویسی کرد:

$$\Pr[\mathcal{M}(x) \in \mathcal{S}] - e^{\alpha} \Pr[\mathcal{M}(x') \in \mathcal{S}] \leq 0 \quad (6-5)$$

از آنجایی که این رابطه برای تمام \mathcal{S} ‌ها برقرار است، سوپریمم آن نیز باید کوچکتر یا مساوی صفر باشد. اما طبق تعریف E_{γ} در معادله ۱-۵، این سوپریمم دقیقاً همان $E_{e^{\alpha}}$ است. چون E_{γ} نمی‌تواند منفی باشد (با انتخاب $\emptyset = \mathcal{S}$ مقدار حداقل صفر است)، پس حتماً برابر صفر است.

جهت دوم (\Leftarrow): فرض کنید $\Pr[\mathcal{M}(x) \in \mathcal{S}] - e^{\alpha} \Pr[\mathcal{M}(x') \in \mathcal{S}] \leq 0$. طبق تعریف سوپریمم، برای هر مجموعه دلخواه \mathcal{S} :

$$\Pr[\mathcal{M}(x) \in \mathcal{S}] - e^{\alpha} \Pr[\mathcal{M}(x') \in \mathcal{S}] \leq 0 \quad (7-5)$$

که بلافارسله نتیجه می‌دهد:

$$\frac{\Pr[\mathcal{M}(x) \in \mathcal{S}]}{\Pr[\mathcal{M}(x') \in \mathcal{S}]} \leq e^{\alpha} \quad (8-5)$$

□ این دقیقاً همان تعریف LDP_{α} -است.

این قضیه ساده اما بنیادین، یک تفسیر هندسی دقیق از محرمانگی ارائه می‌دهد: LDP_{α} -یعنی توزیع‌های خروجی چنان به هم نزدیک باشند که هیچ بخشی از دامنه نتواند نسبت درست‌نمایی بیشتر از e^{α} ایجاد کند.

۴-۵ بهبود کران‌های انقباض

در فصل ۳ دیدیم که دوچی [۱] کران زیر را برای انقباض KL ارائه کرد:

$$D_{KL}(\mathcal{M}(\cdot|x) \parallel \mathcal{M}(\cdot|x')) \leq 4(e^\alpha - 1)^2 \quad (9-5)$$

حال با استفاده از چارچوب E_γ ، می‌توانیم کران‌های بسیار دقیق‌تری استخراج کنیم. آسوده و همکاران [۲] نشان داده‌اند که اگر شرط $E_{e^\alpha} = 0$ برقرار باشد، می‌توان کران‌های انقباض برای سایر f -واگرایی‌ها را از طریق بهینه‌سازی محدب به دست آورد.

قضیه‌ی ۲-۵ (کران دقیق انقباض KL) اگر \mathcal{M} یک مکانیزم α -LDP باشد، آنگاه:

$$D_{KL}(\mathcal{M}(\cdot|x) \parallel \mathcal{M}(\cdot|x')) \leq \frac{e^\alpha - 1}{e^\alpha + 1} \cdot (e^\alpha - 1) \quad (10-5)$$

برای مقادیر کوچک α (رژیم محروم‌گی بالا)، این کران به $\alpha^2/2$ میل می‌کند که 4 برابر کوچکتر (بهتر) از کران دوچی است.

تحلیل مقایسه‌ای: باید رفتار دو کران را در $\alpha \rightarrow 0$ بررسی کنیم:

- کران دوچی: $4(e^\alpha - 1)^2 \approx 4\alpha^2$

- کران مبتنی بر E_γ : $\frac{e^\alpha - 1}{e^\alpha + 1} \approx \tanh(\alpha/2) \approx \alpha/2 \approx \frac{\alpha}{2} \cdot \alpha = \frac{\alpha^2}{2}$

این بهبود ضریب ثابت (از 4 به 0.5) در تحلیل‌های مینی‌مکس بسیار حیاتی است و نشان می‌دهد که «اندازه نمونه موثر» واقعی می‌تواند تا ۸ برابر بهتر از چیزی باشد که آنالیزهای قبلی نشان می‌دادند.

۵-۵ تعمیم به محروم‌گی تقریبی (α, δ) -LDP

یکی دیگر از قدرت‌های چارچوب E_γ ، توانایی آن در توصیف ساده‌ی محروم‌گی تقریبی است. یادآوری می‌کنیم که (α, δ) -LDP شرط زیر را دارد:

$$\Pr[\mathcal{M}(x) \in \mathcal{S}] \leq e^\alpha \Pr[\mathcal{M}(x') \in \mathcal{S}] + \delta \quad (11-5)$$

با بازنویسی این رابطه داریم:

$$\sup_{\mathcal{S}} (\Pr[\mathcal{M}(x) \in \mathcal{S}] - e^\alpha \Pr[\mathcal{M}(x') \in \mathcal{S}]) \leq \delta \quad (12-5)$$

که دقیقاً معادل است با:

$$E_{e^\alpha}(\mathcal{M}(\cdot|x)||\mathcal{M}(\cdot|x')) \leq \delta \quad (13-5)$$

نتیجه‌ی ۳-۵ محرمانگی تقریبی $LDP_{\alpha, \delta}$ - E_{e^α} -واگرایی توزیع‌های خروجی به مقدار δ است. این نتیجه نشان می‌دهد که E_γ -واگرایی طبیعی‌ترین زبان برای صحبت درباره محرمانگی تفاضلی (چه خالص و چه تقریبی) است.

۶-۵ کاربرد در تخمین توزیع گستته

برای نشان دادن کاربرد عملی این نتایج، مسئله تخمین توزیع احتمال روی یک دامنه k -تایی را در نظر بگیرید. با استفاده از تکنیک‌های انقباض E_γ ، می‌توان نشان داد که نرخ مینی‌مکس برای این مسئله تحت شرط α -LDP برابر است با:

$$\mathfrak{M}_n \asymp \frac{k}{n(e^\alpha - 1)^2} \quad (14-5)$$

در حالی که استفاده از تکنیک‌های کلاسیک (دوچی)، جمله‌ای به صورت $\frac{k}{n\alpha^2}$ را پیشنهاد می‌کرد. تفاوت این دو عبارت در رژیم α بزرگ (محرمانگی کم) آشکار می‌شود؛ جایی که $(1 - e^\alpha)^2$ به صورت نمایی رشد می‌کند و نشان می‌دهد که دقت می‌تواند بسیار سریع‌تر از پیش‌بینی‌های قبلی بهبود یابد.

۷-۵ انقباض قوی برای خانواده‌ی f -واگرایی‌ها

تا اینجا دیدیم که شرط α -LDP معادل صفر شدن E_{e^α} -واگرایی است. یک پرسش طبیعی و بسیار مهم این است: آیا این شرط بر روی سایر معیارهای فاصله (مثل χ^2 یا هلینجر) نیز انقباض ایجاد می‌کند؟ پاسخ مثبت است. در مقاله‌ی اخیر آسوده و ژانگ [۳]، نشان داده شده است که مکانیزم‌های موضعی خاصیت «انقباض قوی» را برای طیف وسیعی از واگرایی‌ها به ارمغان می‌آورند.

۱-۷-۵ کران دقیق برای واگرایی کای-دو (χ^2)

یکی از مهم‌ترین نتایج این پژوهش، ارائه‌ی یک ضریب انقباض دقیق برای واگرایی χ^2 است. اهمیت این واگرایی در آن است که کار با آن در محاسبات واریانس و کران‌های مینی‌مکس بسیار ساده‌تر از KL است.

قضیه‌ی ۴-۵ (انقباض χ^2) فرض کنید M یک مکانیزم α -LDP باشد. برای هر دو توزیع ورودی P و Q ، واگرایی کای-دو بین توزیع‌های خروجی با رابطه زیر محدود می‌شود:

$$\chi^2(MP||MQ) \leq \eta_\alpha \cdot \chi^2(P||Q) \quad (15-5)$$

که در آن η_α ضریب انقباض بهینه است و برابر است با:

$$\eta_\alpha = \left(\frac{e^\alpha - 1}{e^\alpha + 1} \right)^2 \quad (16-5)$$

تحلیل مجانبی: برای مقادیر کوچک α (رژیم محترمانگی بالا)، داریم:

$$\eta_\alpha \approx \left(\frac{1 + \alpha - 1}{1 + \alpha + 1} \right)^2 \approx \left(\frac{\alpha}{2} \right)^2 = \frac{\alpha^2}{4} \quad (17-5)$$

این نتیجه بسیار قابل توجه است. یادآوری می‌کنیم که کران‌های کلاسیک دوچی (فصل ۳) ضریبی از مرتبه $O(\alpha^2)$ داشتند، اما ضریب $1/4$ در اینجا نشان‌دهنده‌ی یک انقباض بسیار شدیدتر است. این ضریب دقیقاً با ضریب انقباض «پاسخ تصادفی دودویی» برای واریانس مطابقت دارد و نشان می‌دهد که این کران برای کل کلاس مکانیزم‌های α -LDP «تایت» (Tight) است.

۲-۷-۵ تعمیم به سایر واگرایی‌ها

نویسنده‌گان در [۳] نشان داده‌اند که این ضریب انقباض η_α تنها مختص χ^2 نیست، بلکه برای خانواده‌ای از واگرایی‌ها که خاصیت «تحدب مشترک» دارند (شامل فاصله هلینجر مجدد H^2 و واگرایی KL) نیز صادق است.

نتیجه‌ی ۵-۵ برای هر مکانیزم α -LDP، کران‌های زیر برقرار هستند:

$$D_{KL}(MP||MQ) \leq \eta_\alpha \cdot D_{KL}(P||Q) \quad (18-5)$$

$$H^2(MP, MQ) \leq \eta_\alpha \cdot H^2(P, Q) \quad (19-5)$$

این یکسان‌سازی ضرایب انقباض، تحلیل مکانیزم‌های پیچیده را بسیار ساده می‌کند؛ زیرا کافیست فقط ضریب η_α را محاسبه کنیم.

۸-۵ نامساوی ونتریز خصوصی (Inequality Private van Trees)

اکثر تحلیل‌های موجود در ادبیات α -LDP (مانند کارهای دوچی)، بر روی «ریسک مینی‌مکس» (بدترین حالت) تمرکز دارند. اما در بسیاری از کاربردهای مدرن، ما به تحلیل‌های بیزی (Bayesian) علاقه‌مندیم، جایی که پارامتر مجهول θ دارای یک توزیع پیشین $(\theta) \pi$ است.

نامساوی ونتریز (van Trees) ابزاری کلاسیک برای کران دار کردن خطای بیزی بر اساس «اطلاعات فیشر» است. آسوده و ژانگ^۳ [۳] نسخه‌ی خصوصی شده‌ی این نامساوی را ارائه کردند که ابزاری نوین در جعبه‌ابزار تحلیل محروم‌گی محسوب می‌شود.

قضیه‌ی ۶-۵ (نامساوی ونتریز موضعی) فرض کنید می‌خواهیم پارامتر θ را از روی مشاهدات Z^n که خروجی یک مکانیزم α -LDP-هستند، تخمین بزنیم. اگر $\hat{\theta}$ هر تخمین‌گر دلخواهی باشد، آنگاه میانگین مربعات خطای بیزی^۴ دارای کران پایین زیر است:

$$\mathbb{E}_{(\hat{\theta}-\theta)^2} \geq \frac{1}{\mathbb{E}_{\mathcal{I}(\theta)} + \mathcal{I}_{prior}(\pi)} \quad (20-5)$$

نکته‌ی کلیدی اینجاست که در نسخه خصوصی، اطلاعات فیشر مشاهدات $((\mathcal{I}(\theta))$ با ضریب انقباض تضعیف می‌شود:

$$\mathcal{I}_{priv}(\theta) \leq \eta_\alpha \cdot \mathcal{I}_{orig}(\theta) \quad (21-5)$$

که در آن \mathcal{I}_{orig} اطلاعات فیشر داده‌های خام است.

تفسیر: این نامساوی به زبان ساده می‌گوید: «در دنیای α -LDP، هر بیت اطلاعات فیشر که از داده‌ها می‌گیرید، به اندازه‌ی $\alpha^2/4 \approx \eta_\alpha$ تضعیف می‌شود.» این نتیجه، اثبات حدود پایین برای مسائل تخمین پارامتر را بسیار ساده می‌کند. به جای درگیر شدن بالمهای پیچیده‌ی اسود یا فانو، کافیست اطلاعات فیشر مسئله‌ی اصلی را محاسبه کنیم و در ضریب η_α ضرب کنیم.

۹-۵ کاربردهای نوین و بهبود نرخ‌ها

استفاده از کران‌های انقباض قوی (بخش ۵-۵^۵) و نامساوی ونتریز خصوصی (بخش ۵-۵^۶) منجر به بهبود نتایج در مسائل کلاسیک می‌شود.

²Bayesian Mean Square Error

به عنوان مثال، در مسئله‌ی تخمین چگالی غیرپارامتری برای کلاس توزیع‌های هموار (کلاس هولدر با پارامتر β)، استفاده از این ابزارهای جدید نشان می‌دهد که نرخ خطای بهینه دقیقاً برابر است با:

$$R_{opt} \asymp \left(\frac{1}{n\alpha^2} \right)^{\frac{1}{1/\beta + 1}} \quad (22-5)$$

اگرچه مرتبه‌ی کلی نرخ همگرایی مشابه نتایج دوچی است، اما ضرایب ثابت بهبود یافته‌اند و مهم‌تر از آن، اثبات با استفاده از انقباض^۲ χ بسیار کوتاه‌تر و مستقیم‌تر از روش‌های مبتنی بر KL است. این امر نشان‌دهنده‌ی برتری رویکرد مبتنی بر E_γ و انقباض قوی در تحلیل سیستم‌های محربمانگی تفاضلی است.

فصل ٦

نتیجہ گیری

Bibliography

- [1] S. M. Ali and S. D. Silvey. A general class of coefficients of divergence of one distribution from another. *Journal of the Royal Statistical Society: Series B (Methodological)*, 28(1):131–142, 1966.
- [2] Shahab Asoodeh, Maryam Aliakbarpour, and Flavio P. Calmon. Local differential privacy is equivalent to contraction of an f -divergence. In *2021 IEEE International Symposium on Information Theory (ISIT)*, page 545–550. IEEE Press, 2021.
- [3] Shahab Asoodeh and Huanyu Zhang. Contraction of locally differentially private mechanisms. *IEEE Journal on Selected Areas in Information Theory*, 5:385–395, 2024.
- [4] Michael Barbaro and Tom Zeller. A face is exposed for aol searcher no. 4417749. *New York Times*, 01 2006.
- [5] Leighton Pate Barnes, Wei Ning Chen, and Ayfer Özgür. Fisher information under local differential privacy. *IEEE Journal on Selected Areas in Information Theory*, 1:645–659, 2020.
- [6] Imre Csiszár. Eine informationstheoretische ungleichung und ihre anwendung auf den beweis der ergodizität von markoffschen ketten. *A Magyar Tudományos Akadémia Matematikai Kutató Intézetének Közleményei*, 8(1-2):85–108, 1963.
- [7] Paul Cuff and Lanqing Yu. Differential privacy as a mutual information constraint. In *Proceedings of the ACM Conference on Computer and Communications Security*, pages 43–54, 2016.
- [8] John C. Duchi, Michael I. Jordan, and Martin J. Wainwright. Local privacy and statistical minimax rates. In *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*, pages 429–438, 2013.

- [9] John C Duchi, Michael I Jordan, and Martin J Wainwright. Minimax optimal procedures for locally private estimation. *Journal of the American Statistical Association*, 113(521):182–201, 2018.
- [10] Cynthia Dwork. Differential privacy. In *International colloquium on automata, languages, and programming*, pages 1–12. Springer, 2006.
- [11] Cynthia Dwork, Aaron Roth, et al. The algorithmic foundations of differential privacy. *Foundations and trends® in theoretical computer science*, 9(3–4):211–407, 2014.
- [12] Úlfar Erlingsson, Vasyl Pihur, and Aleksandra Korolova. Rappor: Randomized aggregatable privacy-preserving ordinal response. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS ’14, page 1054–1067, New York, NY, USA, 2014. Association for Computing Machinery.
- [13] Peter Kairouz, Sewoong Oh, and Pramod Viswanath. Extremal mechanisms for local differential privacy. *J. Mach. Learn. Res.*, 17(1):492–542, January 2016.
- [14] Gautam Kamath. CS860: Algorithms for private data analysis – lecture 17: Local differential privacy. Lecture Notes, University of Waterloo, 2020. <http://www.gautamkamath.com/CS860notes/lec17.pdf> (Accessed: 2026-02-14).
- [15] Shiva Prasad Kasiviswanathan, Homin K. Lee, Kobbi Nissim, Sofya Raskhodnikova, and Adam Smith. What can we learn privately? In *2008 49th Annual IEEE Symposium on Foundations of Computer Science*, pages 531–540, 2008.
- [16] Ilya Mironov. Rényi differential privacy. In *2017 IEEE 30th computer security foundations symposium (CSF)*, pages 263–275. IEEE, 2017.
- [17] Arvind Narayanan and Vitaly Shmatikov. Robust de-anonymization of large sparse datasets. In *2008 IEEE Symposium on Security and Privacy (sp 2008)*, pages 111–125, 2008.
- [18] Yury Polyanskiy, H. Vincent Poor, and Sergio Verdú. Channel coding rate in the finite blocklength regime. *IEEE Trans. Inf. Theor.*, 56(5):2307–2359, May 2010.
- [19] Igal Sason and Sergio Verdu. f -divergence inequalities. *IEEE Trans. Inf. Theor.*, 62(11):5973–6006, November 2016.
- [20] Latanya Sweeney. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05):557–570, 2002.

- [21] U.S. House of Representatives Committee on Oversight and Government Reform. The equifax data breach. Majority staff report, U.S. House of Representatives, December 2018.
- [22] Teng Wang, Xuefeng Zhang, Jingyu Feng, and Xinyu Yang. A comprehensive survey on local differential privacy toward data statistics and analysis. *Sensors*, 20:1–48, 2020.
- [23] Tianhao Wang, Jeremiah Blocki, Ninghui Li, and Somesh Jha. Locally differentially private protocols for frequency estimation. In *Proceedings of the 26th USENIX Conference on Security Symposium*, SEC’17, page 729–745, USA, 2017. USENIX Association.
- [24] Stanley L Warner. Randomized response: A survey technique for eliminating evasive answer bias. *Journal of the American statistical association*, 60(309):63–69, 1965.

واژه‌نامه

الف

ز

ب

س

پ

ش

پرس‌وجو Query
پایگاه‌داده Database

ص

ت

غ

ج

ف

ح

ق

خ

ک

د

گ

داده Data
دودوبی Binary

ل

ر

م

Divergence واگرایی Set مجموعه

Trusted Curator متصلی مورد اعتماد

Randomized Mechanism مکانیزم تصادفی

Differential Privacy محرمانگی تفاضلی

Absolutely Continuous مطلقاً پیوسته

هـ

Ajacent همسایه

Adjacency همسایگی

ى**ن**

پیوست آ

مطالب تكميلی

Abstract

We present a standard template for typesetting theses in Persian. The template is based on the XE_PA_HPersian package for the L_AT_EX typesetting system. This write-up shows a sample usage of this template.

Keywords: Thesis, Typesetting, Template, XE_PA_HPersian



Sharif University of Technology

Department of Mathematics

M.Sc. Thesis

Information-Theoretic Analysis of Local Differential Privacy and its Statistical Applications

By:

Firoozeh Abrishami

Supervisor:

Dr. Javad Ebrahimi Boroujeni

March 2026