



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

جناب آقای دکتر جواد ابراهیمی بروجنبی

۱۴۰۴ بهمن

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: جناب آقای دکتر جواد امضاء:

ابراهیمی 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 محرمانگی تفاضلی موضعی و کاربردهای آماری آن

استاد راهنما: جناب آقای دکتر جواد ابراهیمی استاد مشاور: استاد مشاور
بروجنی

این جانب فیروزه ابریشمی اظهار می‌دارم:

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 اختراع 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.

استاد راهنما: جناب آقای دکتر جواد ابراهیمی بروجنی نگارنده: فیروزه ابریشمی

تاریخ:

امضاء:

سپاس

از استاد عزیزم که با کمک‌ها و راهنمایی‌های بی‌دریغشان، مرا در به سرانجام رساندن این پایان‌نامه یاری داده‌اند، تشکر و قدردانی می‌کنم. همچنین از همکاران عزیزی که با راهنمایی‌های خود در بهبود نگارش این نوشتار سهیم بوده‌اند، صمیمانه سپاس‌گزارم.

چکیده

کلیدواژه‌ها:

فهرست مطالب

۱	مقدمه	۱
۲	۱-۱ اهمیت موضوع	۲
۲	۲-۱ ادبیات موضوع	۲
۲	۳-۱ اهداف پژوهش	۲
۲	۴-۱ ساختار پایان نامه	۲
۲	پیش نیازها	۳
۲	۱-۱-۱ محرمانگی تفاضلی متمرکز (CDP)	۳
۲	۱-۱-۲ مدل اعتماد و تعریف رسمی	۳
۲	۲-۱-۱ مکانیزم های پایه در CDP	۵
۲	۲-۱-۲ خواص کلیدی محرمانگی تفاضلی	۶
۲	۴-۱-۱ محدودیت مدل متمرکز	۶
۲	۴-۱-۲ محرمانگی تفاضلی موضعی	۶
۲	۱-۲-۱ مقدمه و گذار از مدل متمرکز	۷
۲	۱-۲-۲ تعاریف رسمی و مدل های محاسباتی	۸
۲	۳-۲-۱ مکانیزم های پایه در α -LDP	۱۰
۲	۳-۲-۲ چالش سودمندی در مدل موضعی	۱۳
۲	۴-۲-۱ f-واگرایی ها	۱۳

۱۳	۱-۳-۲ تعریف f -واگرایی
۱۴	۲-۳-۲ نمونه‌های مهم f -واگرایی
۱۵	۳-۳-۲ ارتباط f -واگرایی‌ها با یکدیگر
۱۵	۴-۲ مبانی آماری و نظریه اطلاعات
۱۵	۱-۴-۲ معیارهای فاصله اطلاعاتی
۱۶	۲-۴-۲ ریسک مینیماکس
۱۷	۲-۵ آزمون فرض آماری و روش تقلیل
۱۷	۱-۵-۲ آزمون فرض دودویی
۱۷	۲-۵-۲ تقلیل تخمین به آزمون (روش بسته‌بندی)
۱۸	۳-۵-۲ نامساوی‌های کران پایین
۲۰	۳ تحلیل‌های مبتنی بر انقباض و نرخ‌های مینیماکس
۲۰	۱-۳ مقدمه
۲۰	۲-۳ محramانگی به عنوان انقباض اطلاعاتی
۲۲	۱-۲-۳ انقباض در فاصله واریانس کل
۲۲	۳-۳ تحلیل نرخ‌های مینیماکس با استفاده از انقباض
۲۳	۴-۳ مطالعه موردي: تخمین میانگین
۲۳	۵-۳ محدودیت‌های تحلیل کلاسیک
۲۵	۴ همارزی α-LDP و انقباض E_γ-واگرایی
۲۵	۱-۴ مقدمه و انگیزه
۲۶	۲-۴ معرفی E_γ -واگرایی
۲۶	۱-۲-۴ خواص هندسی
۲۶	۳-۴ قضیه همارزی اصلی
۲۸	۴-۴ بهبود کران‌های انقباض

۲۸	۵-۴ تعمیم به محرومانگی تقریبی $((\alpha, \delta)\text{-LDP})$
۲۹	۶-۴ کاربرد در تخمین توزیع گسته
۲۹	۷-۴ انقباض قوی برای خانواده f -واگرایی‌ها
۲۹	۱-۷-۴ کران دقیق برای واگرایی کای-دو (χ^2)
۳۰	۲-۷-۴ تعمیم به سایر واگرایی‌ها
۳۱	۸-۴ نامساوی ونتریز خصوصی (Private van Trees Inequality)
۳۱	۹-۴ کاربردهای نوین و بهبود نرخ‌ها
۳۲	۵ نتیجه‌گیری
۳۴	مراجع
۳۶	واژه‌نامه
۳۸	آ مطالب تکمیلی

فهرست جداول

فهرست تصاویر

- ۱-۲ مدل محضانگی تفاضلی متمرکز با یک متصلی مورد اعتماد.

۲-۲ مدل محضانگی تفاضلی موضعی (α -LDP). نویز به صورت موضعی روی دستگاه کاربر اضافه می‌شود.

۴

۷

فصل ۱

مقدمه

۱-۱ اهمیت موضوع

۲-۱ ادبیات موضوع

۳-۱ اهداف پژوهش

۴-۱ ساختار پایان نامه

فصل ۲

پیش‌نیازها

۱-۲ محرمانگی تفاضلی متمرکز (CDP)

مفهوم محرمانگی تفاضلی یا به اختصار DP-ع، اولین بار توسط دُورک و همکاران^[۱] 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 مجموعه داده است.

۱-۱ مدل اعتماد و تعریف رسمی

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

برای تعریف رسمی محرمانگی تفاضلی، ابتدا باید مفهوم «همسایگی» مجموعه داده‌ها را تعریف کنیم.

تعریف ۱-۲ (مجموعه داده‌ای همسایه) دو مجموعه داده‌ی D_1 و D_2 را همسایه^[۵] می‌گوییم (و با ~

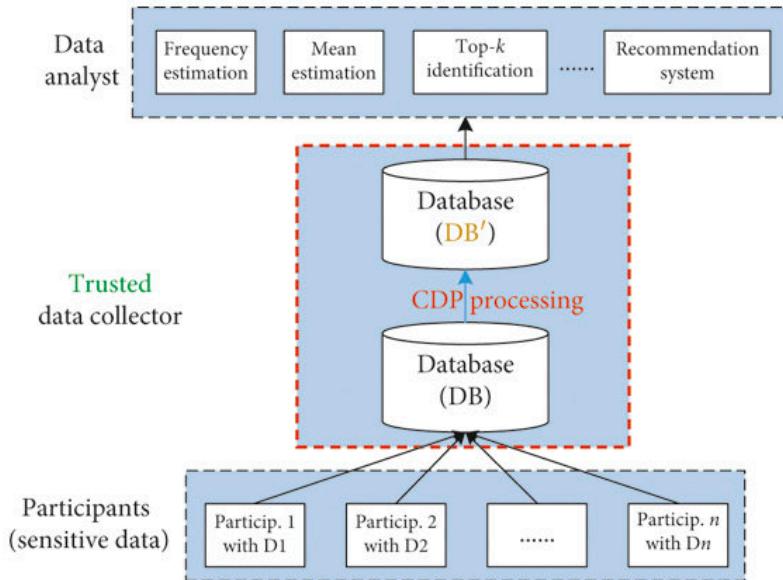
¹Centralized

²Trusted Curator

³randomized mechanism

⁴Query

⁵Adjacent



شکل ۱-۲: مدل محترمانگی تفاضلی متتمرکز با یک متتصدی مورد اعتماد.

D_2 نشان می‌دهیم) اگر تنها در یک رکورد با یکدیگر تفاوت داشته باشند. (یعنی D_2 از افزودن یا حذف یک رکورد به D_1 به دست آید).

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

تعریف ۲-۲ (ε -محترمانگی تفاضلی (ε -DP)) یک مکانیزم تصادفی M ، تعریف ε -محترمانگی تفاضلی^۶ را برآورده می‌سازد، اگر برای هر دو مجموعه داده‌ی همسایه‌ی D_1 و D_2 و برای هر زیرمجموعه S از خروجی‌های ممکن ($\text{Range}(M)$)، داشته باشیم:

$$\Pr[M(D_1) \in S] \leq \exp(\varepsilon) \cdot \Pr[M(D_2) \in S] \quad (1-2)$$

گاهی اوقات، یک تعریف انعطاف‌پذیرتر به نام (ε, δ) -DP نیز استفاده می‌شود که اجازه‌ی یک احتمال شکست کوچک δ را می‌دهد:

$$\Pr[M(D_1) \in S] \leq \exp(\varepsilon) \cdot \Pr[M(D_2) \in S] + \delta \quad (2-2)$$

⁶ ε -Differential Privacy

۲-۱-۲ مکانیزم‌های پایه در CDP

برای دستیابی به ϵ -DP، باید به پاسخ دقیق پرس‌وجو «نویز»^۴ اضافه کنیم. میزان نویز به حساسیت^۵ پرس‌وجو بستگی دارد.

تعريف ۲-۳ (حساسیت سراسری) برای یک تابع f ، حساسیت سراسری $\ell_1(f)$ و $\ell_2(f)$ به صورت زیر تعریف می‌شوند:

$$\Delta_1 f = \max_{\mathcal{D}_1 \sim \mathcal{D}_r} \|f(\mathcal{D}_1) - f(\mathcal{D}_r)\|_1 \quad (3-2)$$

$$\Delta_2 f = \max_{\mathcal{D}_1 \sim \mathcal{D}_r} \|f(\mathcal{D}_1) - f(\mathcal{D}_r)\|_2 \quad (4-2)$$

سه مکانیزم اساسی برای دستیابی به CDP عبارتند از:

- **مکانیزم لاپلاس**^۶: برای توابع عددی، با افزودن نویز از توزیع لاپلاس متناسب با حساسیت ℓ_1 ، می‌توان به ϵ -DP دست یافت:

$$\mathcal{M}(\mathcal{D}) = f(\mathcal{D}) + \text{Lap}\left(\frac{\Delta_1 f}{\epsilon}\right) \quad (5-2)$$

- **مکانیزم گوسی**^۷: این مکانیزم اغلب زمانی استفاده می‌شود که حساسیت ℓ_2 تابع کمتر از حساسیت ℓ_1 باشد. در اینجا نویز از توزیع نرمال (گوسی) افزوده می‌شود:

$$\mathcal{M}(\mathcal{D}) = f(\mathcal{D}) + \mathcal{N}(0, \sigma^2) \quad (6-2)$$

که در آن $\sigma \geq \sqrt{2 \ln(1/25/\delta)} \cdot \frac{\Delta_2 f}{\epsilon}$ است. برخلاف مکانیزم لاپلاس، این مکانیزم تنها ϵ -DP می‌باشد. در اینجا نویز از توزیع نرمال (گوسی) افزوده می‌شود.

- **مکانیزم نمایی**^۸: برای خروجی‌های غیرعددی (دسته‌ای)، از یک «تابع امتیاز» $q(\mathcal{D}, r)$ استفاده می‌شود. این مکانیزم خروجی r را با احتمالی متناسب با امتیاز آن برمی‌گرداند:

$$\Pr[\mathcal{M}(\mathcal{D}) = r] \propto \exp\left(\frac{\epsilon \cdot q(\mathcal{D}, r)}{2 \Delta q}\right) \quad (7-2)$$

⁷Noise

⁸Sensitivity

⁹The Laplace Mechanism

¹⁰The Gaussian Mechanism

¹¹The Exponential Mechanism

۳-۱-۲ خواص کلیدی محرمانگی تفاضلی

قدرت چارچوب DP در خواص ترکیبی آن نهفته است:

• مصنونیت در برابر پسپردازش^{۱۲}: انجام هرگونه محاسبات بر روی خروجی یک مکانیزم DP- ϵ (بدون دسترسی مجدد به داده‌های اصلی)، نمی‌تواند سطح محرمانگی را کاهش دهد.

• ترکیب‌پذیری^{۱۳}: اگر چندین مکانیزم DP- ϵ_i را اجرا کیم، بودجه‌های محرمانگی جمع می‌شوند.

– ترکیب‌پذیری پایه‌ای: اجرای k مکانیزم $DP\sum \epsilon_i$ - منجر به $DP\sum \epsilon_i$ - می‌شود.

– ترکیب‌پذیری پیشرفته: با پذیرش یک δ کوچک، می‌توان نشان داد که بودجه کل با نرخ \sqrt{k} رشد می‌کند (نه k).

• محرمانگی گروهی^{۱۴}: محرمانگی تفاضلی به طور طبیعی برای گروه‌هایی از افراد نیز صادق است. اگر دو پایگاه داده در k رکورد با هم متفاوت باشند، تضمین محرمانگی به صورت $k\epsilon$ -DP برقرار خواهد بود. این یعنی با افزایش اندازه گروه، تضمین محرمانگی به صورت خطی تضعیف می‌شود.

۴-۱-۲ محدودیت مدل مت مرکز

با وجود تمام مزایا، مدل CDP یک نقطه‌ی ضعف اساسی دارد: نیاز به یک متصدی 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 موضعی» سوق می‌دهد.

۲-۲ محرمانگی تفاضلی موضعی

در فصل گذشته، مبانی نظری حریم خصوصی مت مرکز (CDP) و ابزارهای آماری لازم برای تحلیل آن را مرور کردیم. در این فصل، به طور اختصاصی به چارچوب محرمانگی تفاضلی موضعی^{۱۵} (α -LDP) می‌پردازیم. این مدل، که امروزه در سیستم‌های توزیع شده و جمع‌آوری داده‌های بزرگ مقیاس کاربرد فراوان دارد، پارادایم اعتماد را از «سرور مرکزی» به «کاربر نهایی» تغییر می‌دهد.

¹²Post-processing Immunity

¹³Composition

¹⁴Group Privacy

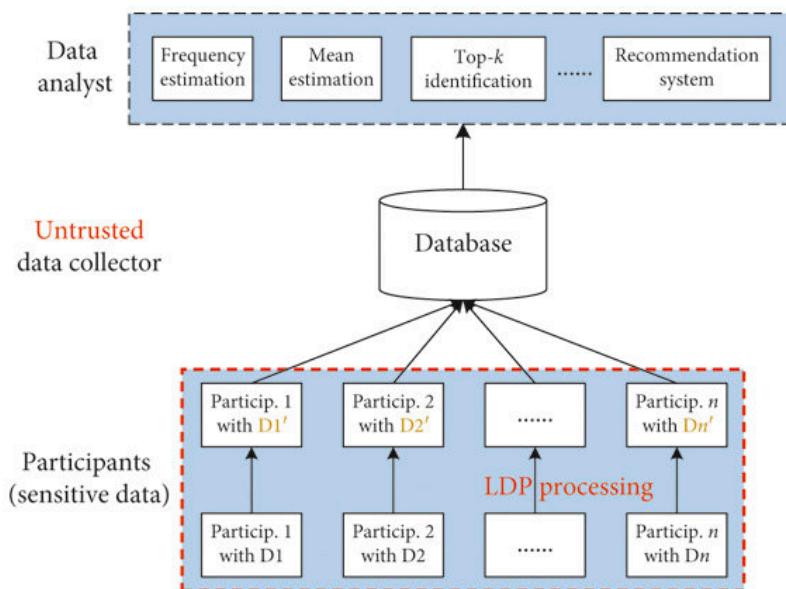
¹⁵Local Differential Privacy (LDP)

۱-۲-۲ مقدمه و گذار از مدل متمرکز

همان طور که در بخش ۱-۲ دیدیم، مدل متمرکز نیازمند وجود یک متصلی مورد اعتماد^{۱۶} است که به داده‌های خام دسترسی داشته باشد. اگرچه این مدل دقیق آماری بالایی را فراهم می‌کند، اما در دنیای واقعی با چالش‌های امنیتی و حقوقی جدی روبروست:

- نقطه شکست مرکزی^{۱۷}: سرور مرکزی هدف جذابی برای مهاجمان است. نشت اطلاعات از سرور (چه بر اثر هک و چه بر اثر خطای انسانی) حریم خصوصی تمام کاربران را به خطر می‌اندازد.
- عدم اعتماد کاربران: در بسیاری از کاربردها (مانند جمع‌آوری داده‌های پزشکی یا تاریخچه مرورگر)، کاربران تمایلی ندارند داده‌های حساس خود را حتی به یک سرور «مطمئن» بسپارند.

در پاسخ به این چالش‌ها، مدل محترمانگی تفاضلی موضوعی مطرح شد. در α -LDP، فرآیند خصوصی‌سازی (افزودن نویز) به سمت کلاینت (کاربر) منتقل می‌شود. به این معنا که داده‌ها قبل از ترک دستگاه کاربر، نویزدار می‌شوند و سرور تنها به داده‌های بنام و نویزدار دسترسی دارد (شکل ۲-۲).



شکل ۲-۲: مدل محترمانگی تفاضلی موضوعی (α -LDP). نویز به صورت موضوعی روی دستگاه کاربر اضافه می‌شود.

این رویکرد توسط شرکت‌های بزرگ فناوری برای جمع‌آوری داده‌های تله‌متري پذیرفته شده است. برای مثال، گوگل از مکانیزم RAPPOR در مرورگر کروم، و اپل و مایکروسافت از روش‌های مشابهی برای جمع‌آوری داده‌های آماری از سیستم‌عامل‌های خود استفاده می‌کنند.

¹⁶Trusted Curator

¹⁷Single Point of Failure

۲-۲-۲ تعاریف رسمی و مدل‌های محاسباتی

در مدل موضعی، ما n کاربر داریم که هر کدام یک داده‌ی خصوصی X_i از دامنه \mathcal{X} در اختیار دارند. هر کاربر به طور مستقل یک الگوریتم تصادفی (مکانیزم) را اجرا می‌کند و خروجی Z_i را منتشر می‌کند.

α -LDP تعریف

هسته‌ی اصلی این مدل، «تصادفی‌ساز موضعی» است.

تعریف ۴-۲ (تصادفی‌ساز موضعی^{۱۸}) یک مکانیزم تصادفی $Z : \mathcal{M} \rightarrow \mathcal{Z}$ را یک تصادفی‌ساز موضعی می‌نامیم که ورودی $x \in \mathcal{X}$ را می‌گیرد و خروجی $z \in \mathcal{Z}$ را براساس توزیع احتمال شرطی $Q(z|x)$ تولید می‌کند.

شرط محترمانگی در اینجا تضمین می‌کند که با مشاهده‌ی خروجی z ، تمایز قائل شدن بین هر دو ورودی اولیه x و x' دشوار باشد. تفاوت کلیدی این تعریف با مدل متمرکز در این است که در CDP ما دو پایگاه داده‌ی همسایه را مقایسه می‌کردیم، اما در اینجا هر دو مقدار ورودی ممکن مقایسه می‌شوند.

تعریف ۵-۲ (α -محترمانگی تفاضلی موضعی) یک مکانیزم M دارای α -محترمانگی تفاضلی موضعی است اگر برای تمام جفت ورودی‌های $x, x' \in \mathcal{X}$ و هر زیرمجموعه از خروجی‌ها $S \subseteq \mathcal{Z}$ داشته باشیم:

$$\sup_S \frac{\Pr[M(x) \in S]}{\Pr[M(x') \in S]} \leq e^\alpha \quad (8-2)$$

(نکته: در متون آماری مانند [۲] معمولاً از پارامتر α به جای ϵ برای نمایش بودجه حریم خصوصی موضعی استفاده می‌شود تا تمایز آن با مدل متمرکز مشخص باشد. ما نیز در این فصل و فصول بعدی از این نمادگذاری پیروی می‌کنیم).

این تعریف معادل شرط زیر بر روی واگرایی ماقزیم (D_∞) بین توزیع‌های شرطی است:

$$\sup_{x, x' \in \mathcal{X}} D_\infty(Q(\cdot|x) || Q(\cdot|x')) \leq \alpha \quad (9-2)$$

تعمیم‌ها و خواص

علاوه بر تعریف استاندارد α -LDP (معادله ۸-۲)، دو مفهوم دیگر نیز در تحلیل‌های نظری و طراحی مکانیزم‌ها اهمیت دارند: محترمانگی تقریبی و خاصیت ترکیب.

تعريف ۶-۲ (α, δ)-محرمانگی تفاضلی موضعی) یک مکانیزم تصادفی M دارای محرمانگی تفاضلی موضعی تقریبی یا $LDP(\alpha, \delta)$ است اگر برای هر دو ورودی $x, x' \in \mathcal{X}$ و هر زیرمجموعه خروجی $S \subseteq \mathcal{Z}$ داشته باشیم:

$$\Pr[M(x) \in S] \leq e^\alpha \cdot \Pr[M(x') \in S] + \delta \quad (10-2)$$

این تعریف (که در [۳] نیز بررسی شده است)، اجازه‌ی یک احتمال شکست کوچک δ را می‌دهد. اهمیت نظری این تعریف در آن است که ارتباط مستقیمی با واگرایی E_γ (که در فصل قبل معرفی شد) دارد.

قضیه ۱-۲ (ترکیب ترتیبی^{۱۹}) اگر یک کاربر در k مرحله‌ی مختلف در پروتکل‌های M_1, \dots, M_k شرکت کند که هر کدام به ترتیب دارای بودجه‌ی حریم خصوصی α_i باشند، آنگاه کل فرآیند دارای محرمانگی تفاضلی موضعی با بودجه‌ی $\sum_{i=1}^k \alpha_i$ خواهد بود. این خاصیت در تحلیل پروتکل‌های تعاملی (بخش بعد) که در آن خروجی‌های بعدی به خروجی‌های قبلی وابسته هستند، نقش بنیادین دارد.

پروتکل‌های تعاملی و غیرتعاملی

یکی از جنبه‌های مهم در تحلیل نرخ‌های مینیماکس (که در فصل بعد به آن می‌پردازیم)، نحوه‌ی تعامل کاربران با سرور است. دوچی و همکاران [۲] پروتکل‌های موضعی را به دو دسته تقسیم می‌کنند:

۱. **پروتکل‌های غیرتعاملی^{۲۰}**: در این حالت، خروجی هر کاربر Z_i تنها به ورودی خودش X_i وابسته است و مستقل از داده‌ها یا خروجی‌های سایر کاربران تولید می‌شود.

$$Z_i = M_i(X_i) \quad (11-2)$$

این مدل ساده‌ترین و رایج‌ترین شکل پیاده‌سازی α -LDP است.

۲. **پروتکل‌های تعاملی (ترتیبی)^{۲۱}**: در این حالت، مکانیزم کاربر i می‌تواند به خروجی‌های منتشر شده توسط کاربران قبلی (Z_1, \dots, Z_{i-1}) وابسته باشد. به عبارت دیگر، کanal ارتباطی Q_i می‌تواند به صورت پویا بر اساس تاریخچه تغییر کند:

$$Z_i \sim Q_i(\cdot | X_i, Z_1, \dots, Z_{i-1}) \quad (12-2)$$

این مدل به الگوریتم‌های تطبیقی اجازه می‌دهد تا دقیق تخمین را بهبود بخشدند. با این حال، همان‌طور که در فصل بعد خواهیم دید، حتی با وجود تعامل، محدودیت‌های بنیادی f -واگرایی همچنان مانع از کاهش چشمگیر نرخ خطأ می‌شوند.

²⁰Non-interactive

²¹Sequential/Interactive

۳-۲-۲ مکانیزم‌های پایه در α -LDP

در این بخش، مکانیزم‌های بنیادین را معرفی می‌کنیم که برای تحقق محترمانگی تفاضلی موضعی استفاده می‌شوند. این مکانیزم‌ها بلوک‌های سازنده‌ی پروتکل‌های پیچیده‌تر هستند و بسته به نوع داده (دودویی، دسته‌ای یا عددی) و اندازه دامنه انتخاب می‌شوند.

پاسخ تصادفی دودویی (RR)

پایه‌ای ترین و کلاسیک‌ترین مکانیزم در مدل موضعی، «پاسخ تصادفی»^{۲۲} است که دهه‌ها پیش از تعریف رسمی α -LDP توسط وارنر [۴] برای نظرسنجی‌های حساس معرفی شد. فرض کنید دامنه ورودی دودویی باشد ($\mathcal{X} = \{0, 1\}$).

مکانیزم M_{RR} با ورودی $\{1, x \in \{0, 1\}, z \in \{0, 1\}\}$ خروجی $\{0, 1\}$ را طبق احتمالات زیر تولید می‌کند:

$$\Pr[z = x] = p, \quad \Pr[z \neq x] = 1 - p \quad (13-2)$$

برای اینکه این مکانیزم شرط α -LDP را برآورده کند، طبق تعریف ۵-۲ باید نسبت احتمالات حداکثر e^α باشد:

$$\frac{\Pr[z = 1 | x = 1]}{\Pr[z = 1 | x = 0]} = \frac{p}{1 - p} \leq e^\alpha \quad (14-2)$$

بنابراین، برای دستیابی به کمترین خطأ، پارامتر احتمال p به صورت زیر تنظیم می‌شود:

$$p = \frac{e^\alpha}{1 + e^\alpha} \quad (15-2)$$

در این حالت، واریانس تخمین‌گر حاصل از این مکانیزم برابر است با:

$$\text{Var}[\hat{x}] = \frac{e^\alpha}{(e^\alpha - 1)^2} \quad (16-2)$$

این رابطه نشان می‌دهد که برای α ‌های کوچک، واریانس به سرعت (تقریباً با نرخ $1/\alpha^2$) افزایش می‌یابد که نشان‌دهنده‌ی هزینه بالای حریم خصوصی در دقت تخمین است.

پاسخ تصادفی تعمیم‌یافته (GRR)

زمانی که دامنه ورودی شامل $2 < k \in \{1, \dots, k\} \subset \mathcal{X}$ ، از نسخه تعمیم‌یافته پاسخ تصادفی استفاده می‌شود [۵]. این روش تعمیم مستقیم RR برای دامنه‌های گسته است.

²²Randomized Response (RR)

²³Generalized Randomized Response (GRR)

در این مکانیزم، برای ورودی x :

$$\Pr[\mathcal{M}(x) = z] = \begin{cases} p & \text{if } z = x \\ q & \text{if } z \neq x \end{cases} \quad (17-2)$$

از آنجا که مجموع احتمالات باید ۱ باشد، داریم $1 = p + (k - 1)q = p + \frac{p}{e^\alpha + k - 1}$. همچنین شرط α -LDP ایجاب می‌کند که $e^\alpha \leq \frac{p}{q}$. با حل این دستگاه معادلات، مقادیر بهینه p و q به صورت زیر به دست می‌آیند:

$$p = \frac{e^\alpha}{e^\alpha + k - 1}, \quad q = \frac{1}{e^\alpha + k - 1} \quad (18-2)$$

این مکانیزم برای دامنه‌های کوچک (k کوچک) بسیار کارآمد است و واریانس آن بهینه است. اما با افزایش k ، دقت آن به شدت کاهش می‌یابد زیرا احتمال گزارش پاسخ صحیح (p) با افزایش k کاهش می‌یابد و به سمت صفر میل می‌کند. بنابراین برای دامنه‌های بزرگ (مانند لغات یک دیکشنری)، GRR گرینه مناسبی نیست.

مکانیزم‌های مبتنی بر کدگذاری یگانی (UE)

برای غلبه بر مشکل کاهش دقت GRR در دامنه‌های بزرگ، خانواده‌ای از مکانیزم‌ها تحت عنوان «کدگذاری یگانی»²⁴ توسعه یافته‌اند. این رویکرد اساس پروتکل مشهور RAPPOR گوگل را تشکیل می‌دهد [۳].

در این روش، فرآیند خصوصی‌سازی طی دو مرحله انجام می‌شود:

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

۲. **اختلال (Perturbation):** هر بیت این بردار به صورت مستقل با استفاده از یک مکانیزم بازیزی معکوس می‌شود.

اگر v_i بیت i -ام بردار کدگذاری شده باشد، خروجی z_i به صورت زیر تولید می‌شود:

$$\Pr[z_i = 1] = \begin{cases} p & \text{if } v_i = 1 \\ q & \text{if } v_i = 0 \end{cases} \quad (19-2)$$

بر اساس انتخاب مقادیر p و q ، دو مکانیزم مهم در این خانواده تعریف می‌شوند:

²⁴Unary Encoding (UE)

- کدگذاری یگانی متقارن (SUE): که به آن Basic RAPPOR نیز گفته می‌شود. در این حالت، احتمالات تغییر بیت به گونه‌ای انتخاب می‌شوند که مکانیزم متقارن باشد ($1 = p + q$). مقادیر بهینه عبارتند از:

$$p = \frac{e^{\alpha/2}}{e^{\alpha/2} + 1}, \quad q = \frac{1}{e^{\alpha/2} + 1} \quad (20-2)$$

مزیت SUE این است که واریانس تخمین برای هر آیتم مستقل از تعداد کل آیتم‌ها (k) است، اما به دلیل استفاده از نیمی از بودجه حریم خصوصی ($\alpha/2$) برای هر بیت، خطای آن همچنان قابل توجه است.

- کدگذاری یگانی بهینه (OUE): وانگ و همکاران [۳] نشان دادند که برای تخمین فراوانی در دامنه‌های بزرگ، نیازی به متقارن بودن مکانیزم نیست. در روش OUE^{۲۵}، پارامترها به گونه‌ای تنظیم می‌شوند که اطلاعات بیت‌های ۱ (سیگنال اصلی) با بیشترین دقیقیت حفظ شود ($p = 1/2$) و نویز روی بیت‌های ۰ (که تعدادشان زیاد است) کنترل شود:

$$p = \frac{1}{2}, \quad q = \frac{1}{e^\alpha + 1} \quad (21-2)$$

تحلیل‌های نظری و تجربی نشان می‌دهند که OUE برای α ‌های متوسط و بزرگ، واریانس کمتری نسبت به GRR و SUE دارد و استاندارد فعلی برای جمع‌آوری داده‌های دسته‌ای بزرگ مقیاس است.

مکانیزم لاپلاس موضعی

برای داده‌های عددی (مثل $x \in [-1, 1]$)، استفاده از مکانیزم لاپلاس که در مدل متمرکز محبوب است، در مدل موضعی نیز ممکن است اما با چالش‌هایی همراه است.

حساسیت سراسری (Δ) در مدل موضعی برابر با قطر دامنه است، زیرا هر دو ورودی $x, x' \in \mathcal{X}$ باید از نظر مکانیزم غیرقابل تمایز باشند. اگر دامنه ورودی $[-1, 1] = \mathcal{X}$ باشد، حساسیت برابر است با:

$$\Delta = \max_{x, x'} |x - x'| = |1 - (-1)| = 2 \quad (22-2)$$

بنابراین، مکانیزم لاپلاس موضعی خروجی را به صورت زیر تولید می‌کند:

$$\mathcal{M}_{Lap}(x) = x + \eta, \quad \eta \sim \text{Lap}\left(\frac{2}{\alpha}\right) \quad (23-2)$$

نکته مهمی که دوچی و همکاران [۴] به آن اشاره کردند این است که برخلاف مدل متمرکز، مکانیزم لاپلاس در مدل موضعی برای ابعاد بالا ($d > 1$) زیر-بهینه^{۲۶} است و نرخ خطای آن بدتر از مکانیزم‌های پیشرفته‌تر (مانند نمونه‌برداری هایپرکیوب) است که در فصل‌های آینده به آن‌ها اشاره خواهیم کرد.

²⁵Optimized Unary Encoding

²⁶Sub-optimal

۴-۲-۲ چالش سودمندی در مدل موضعی

بهای عدم اعتماد به سرور، کاهش شدید سودمندی^{۲۷} آماری است. از آنجایی که نویز به داده‌ی هر فرد به صورت مستقل اضافه می‌شود، خطای تجمعی در مدل α -LDP بسیار بیشتر از مدل مرکز CDP است. برای رسیدن به سطح دقت مشابه، مدل موضعی معمولاً^{۲۸} به تعداد کاربران n بسیار بیشتری نیاز دارد. به طور کلی، در حالی که خطای مکانیزم‌های CDP اغلب با $O(1/n)$ کاهش می‌یابد، خطای مکانیزم‌های α -LDP معمولاً^{۲۹} با $O(1/\sqrt{n})$ کاهش می‌یابد. این کاهش در «اندازه نمونه مؤثر» یکی از موضوعات اصلی است که در فصل آینده با استفاده از ابزارهای f -واگرایی آن را اثبات خواهیم کرد.

۳-۲ f -واگرایی‌ها

در بخش‌های قبلی، ما مکانیزم‌های محترمانگی تفاضلی را به عنوان روش‌هایی برای ایجاد «شباهت آماری» بین خروجی‌های دو پایگاه داده‌ی همسایه معرفی کردیم. در این بخش، ما ابزار ریاضیاتی اصلی برای سنجش این «شباهت» یا «فاصله» بین توزیع‌های احتمالی را معرفی می‌کنیم. این ابزار، خانواده f -واگرایی‌ها^{۲۸} است که بسیاری از معیارهای رایج فاصله‌ی آماری را به عنوان حالت‌های خاص خود در بر می‌گیرد.

۱-۳-۲ تعریف f -واگرایی

مفهوم f -واگرایی اولین بار توسط سیسر^[۶] و به طور همزمان توسط علی و سیلوی^[۷] معرفی شد. این معیار، یک روش عمومی برای اندازه‌گیری تفاوت بین دو توزیع احتمال P و Q (تعریف شده بر روی یک فضای یکسان) ارائه می‌دهد.

تعریف ۱-۲ (f -واگرایی) فرض کنید P و Q دو توزیع احتمال باشند به طوری که P نسبت به Q مطلقاً^{۲۹} پیوسته^{۲۹} باشد. فرض کنید p و q توابع چگالی احتمال (یا توابع جرم احتمال) آن‌ها باشند. برای هر تابع محدب $\mathbb{R} \rightarrow \mathbb{R}$ که $f(0) = 0$ باشد، f -واگرایی P از Q به صورت زیر تعریف می‌شود:

$$D_f(P||Q) = \int q(x)f\left(\frac{p(x)}{q(x)}\right) dx \quad (۲۴-۲)$$

²⁷Utility

²⁸ f -divergences

²⁹Absolutely Continuous

در حالت گسسته، این تعریف به صورت حاصل جمع زیر در می‌آید:

$$D_f(P||Q) = \sum_{x \in \mathcal{X}} q(x) f\left(\frac{p(x)}{q(x)}\right) \quad (25-2)$$

تابع f «ژنراتور» (تولیدکننده) و اگرایی نامیده می‌شود و با انتخاب f ‌های متفاوت، می‌توان معیارهای فاصله یا اگرایی متفاوتی را به دست آورد. شرط $\bullet = (1)$ تضمین می‌کند که اگر دو توزیع یکسان باشند $(P = Q)$ ، و اگرایی آن‌ها صفر خواهد بود.

۲-۳-۲ نمونه‌های مهم f -واگرایی

بسیاری از معیارهای معروف در آمار و نظریه اطلاعات، حالتهای خاصی از f -واگرایی هستند:

- **واگرایی کولبک-لایبلر^{۳۰}**: این معیار که به آن آنتروپی نسبی^{۳۱} نیز گفته می‌شود، با انتخاب تابع $f(t) = t \log t$ به دست می‌آید:

$$D_{KL}(P||Q) = \sum_x p(x) \log \left(\frac{p(x)}{q(x)} \right) \quad (26-2)$$

- **فاصله‌ی واریانس کل^{۳۲}**: فاصله‌ی TV (که اغلب با $\Delta(P, Q)$ یا d_{TV} نشان داده می‌شود) ارتباط نزدیکی با f -واگرایی دارد و با انتخاب $f(t) = \frac{1}{2}|t - 1|$ حاصل می‌شود:

$$d_{TV}(P, Q) = \frac{1}{2} \sum_x |p(x) - q(x)| \quad (27-2)$$

- **واگرایی کای-دو^{۳۳}**: این معیار آماری با انتخاب $f(t) = (t - 1)^2$ به دست می‌آید:

$$\chi^2(P||Q) = \sum_x \frac{(p(x) - q(x))^2}{q(x)} \quad (28-2)$$

- **فاصله‌ی هلینجر (مربع)^{۳۴}**: این فاصله با انتخاب $f(t) = (\sqrt{t} - 1)^2$ (یا معادل آن $= f(t) = (\sqrt{t} - 1)^2$) حاصل می‌شود:

$$H^2(P, Q) = \sum_x (\sqrt{p(x)} - \sqrt{q(x)})^2 \quad (29-2)$$

³⁰Kullback-Leibler (KL) Divergence

³¹Relative Entropy

³²Total Variation (TV) Distance

³³Chi-Squared (χ^2) Divergence

³⁴Squared-Hellinger Distance

۳-۳-۲ ارتباط f -واگرایی‌ها با یکدیگر

این واگرایی‌ها مستقل از هم نیستند و روابط ریاضی مهمی بین آن‌ها برقرار است. یکی از مشهورترین این روابط، نامساوی پینسکر^{۳۵} است که ارتباط بین واگرایی KL و فاصله‌ی واریانس کل را نشان می‌دهد:

$$d_{TV}(P, Q) \leq \frac{1}{\sqrt{2}} D_{KL}(P||Q) \quad (30-2)$$

این نامساوی‌ها در تحلیل‌های حریم خصوصی بسیار کاربردی هستند، زیرا به ما اجازه می‌دهند که با داشتن یک کران (حد) بر روی یک معیار واگرایی، بتوانیم کرانی برای سایر معیارها نیز به دست آوریم.

در فصل بعدی، ما به تفصیل بررسی خواهیم کرد که چگونه تضمین $D_{\alpha-LDP}$ (که در معادله ۸-۲ تعریف شد) مستقیماً منجر به ایجاد یک کران بالا بر روی f -واگرایی‌های مختلف بین توزیع‌های خروجی می‌شود.

۴-۲ مبانی آماری و نظریه اطلاعات

در بخش‌های پیشین، ابزارهای سنجش فاصله بین توزیع‌ها (f -واگرایی‌ها) را معرفی کردیم. در این بخش، به معرفی چارچوب آماری می‌پردازیم که در آن از این ابزارها برای تحلیل حدود پایین خطأ در حضور محدودیت‌های محروم‌گری استفاده می‌شود. این تعاریف و قضایا عمده‌ای^{۳۶} بر اساس چارچوب ارائه شده در [?] تدوین شده‌اند.

۱-۴-۲ معیارهای فاصله اطلاعاتی

برای دو توزیع احتمال P و Q که روی فضای \mathcal{X} تعریف شده‌اند و نسبت به یک اندازه‌ی پایه μ مطلقاً پیوسته هستند (با توابع چگالی p و q ، معیارهای زیر را تعریف می‌کنیم:

تعریف ۸-۲ (واگرایی کولبک-لایبلر) واگرایی کولبک-لایبلر (KL) بین دو توزیع P و Q به صورت زیر تعریف می‌شود:

$$D_{KL}(P||Q) = \int_{\mathcal{X}} p(x) \log \frac{p(x)}{q(x)} d\mu(x) \quad (31-2)$$

³⁵Pinsker's Inequality

تعريف ۹-۲ (فاصله‌ی واریانس کل) فاصله‌ی واریانس کل^{۳۶} بین دو توزیع P و Q به صورت زیر تعریف می‌شود:

$$\|P - Q\|_{TV} = \sup_{S \in \sigma(\mathcal{X})} |P(S) - Q(S)| = \frac{1}{2} \int_{\mathcal{X}} |p(x) - q(x)| d\mu(x) \quad (32-2)$$

تعريف ۱۰-۲ (اطلاعات متقابل) اگر X و V دو متغیر تصادفی باشند، اطلاعات متقابل^{۳۷} بین آن‌ها به صورت امید ریاضی و اگرایی KL بین توزیع شرطی و توزیع حاشیه‌ای تعریف می‌شود:

$$I(X; V) = D_{KL}(P_{X,V} || P_X \otimes P_V) = \mathbb{E}_V [D_{KL}(P_{X|V} || P_X)] \quad (33-2)$$

این معیار نقش کلیدی در نامساوی فانو (که در ادامه می‌آید) ایفا می‌کند.

۲-۴-۲ ریسک مینیماکس

در نظریه تصمیم‌آماری، هدف تخمین یک پارامتر $(P)\theta$ از یک توزیع ناشناخته $P \in \mathcal{P}$ است. اگر $\hat{\theta}$ یک تخمین‌گر باشد که تابعی از داده‌های مشاهده شده (مانند Z_1, \dots, Z_n) است، کیفیت آن با استفاده از یک تابع زیان صعودی $\Phi \circ \rho$ سنجیده می‌شود (که ρ یک شبهمتر روی فضای پارامتر است).

نخ مینیماکس^{۳۸}، کمترین خطای ممکنی است که یک تخمین‌گر در بدترین سناریو (بدترین توزیع P در کلاس \mathcal{P}) متحمل می‌شود.

تعريف ۱۱-۲ (نخ مینیماکس) برای یک کلاس از توزیع‌ها \mathcal{P} و پارامتر θ ، نخ مینیماکس \mathfrak{M}_n به صورت زیر تعریف می‌شود:

$$\mathfrak{M}_n(\theta(\mathcal{P}), \Phi \circ \rho) = \inf_{\hat{\theta}} \sup_{P \in \mathcal{P}} \mathbb{E}_P [\Phi(\rho(\hat{\theta}(Z^n), \theta(P)))] \quad (34-2)$$

که در آن اینفیم روی تمام تخمین‌گرهای ممکن $\hat{\theta}$ گرفته می‌شود.

در حالتی که محدودیت محرومگی تفاضلی موضعی با پارامتر α وجود داشته باشد، نخ مینیماکس خصوصی (Minimax - Private α) با در نظر گرفتن اینفیم روی تمام مکانیزم‌های کانال Q که شرط α -LDP را برآورده می‌کنند، تعریف می‌شود [?].

³⁶Total Variation Distance

³⁷Mutual Information

³⁸Minimax Rate

۵-۲ آزمون فرض آماری و روش تقلیل

برای اثبات حدود پایین نرخ‌های مینیماکس، روش استاندارد این است که مسئله‌ی تخمین پارامتر را به یک مسئله‌ی آزمون فرض^{۳۹} تقلیل دهیم. ایده اصلی این است: اگر نتوانیم بین چند مقدار گسته از پارامتر با دقت بالا تمایز قائل شویم، قطعاً نمی‌توانیم پارامتر را در فضای پیوسته با خطای کم تخمین بزنیم.

۱-۵-۲ آزمون فرض دودویی

ساده‌ترین حالت آزمون فرض، تصمیم‌گیری بین دو توزیع احتمال P_0 و P_1 است. فرض کنید داده‌ی مشاهده شده Z از یکی از این دو توزیع تولید شده است. ما دو فرض داریم:

$$\bullet \text{ فرض صفر } (H_0) : Z \sim P_0$$

$$\bullet \text{ فرض مقابل } (H_1) : Z \sim P_1$$

یک آزمون (یا تابع تست) $\psi : \mathcal{Z} \rightarrow \{0, 1\}$ تابعی است که بر اساس داده‌ی مشاهده شده، حدس می‌زند کدام فرض صحیح است. خطای این آزمون به صورت مجموع احتمال خطای نوع اول و دوم تعریف می‌شود:

$$P_{err}(\psi) = \Pr_{H_0}(\psi(Z) = 1) + \Pr_{H_1}(\psi(Z) = 0) \quad (35-2)$$

لم نیمن-پیرسون^{۴۰} نشان می‌دهد که کمترین خطای ممکن برای هر آزمون دودویی، مستقیماً با فاصله‌ی واریانس کل (d_{TV}) بین دو توزیع ارتباط دارد:

$$\inf_{\psi} P_{err}(\psi) = 1 - \|P_0 - P_1\|_{TV} \quad (36-2)$$

این رابطه نشان می‌دهد که هرچه دو توزیع P_0 و P_1 به هم شبیه‌تر باشند (فاصله‌ی TV کمتر)، احتمال خطای بیشتر شده و به ۱ (حدس تصادفی) نزدیک‌تر می‌شود. در فضای α -LDP، نویز اضافه شده باعث کاهش شدید فاصله‌ی TV و در نتیجه افزایش خطای آزمون می‌شود.

۲-۵-۲ تقلیل تخمین به آزمون (روش بسته‌بندی)

برای استفاده از ابزارهای آزمون فرض در مسئله‌ی تخمین نرخ مینیماکس (معادله ۳۴-۲)، از تکنیک گسته‌سازی فضای پارامتر Θ استفاده می‌کنیم. این روش شامل مراحل زیر است:

³⁹Hypothesis Testing

⁴⁰Neyman-Pearson Lemma

۱. ساخت مجموعه‌ای بسته‌بندی^{۴۱}: مجموعه‌ای متناهی از پارامترها $\Theta \subset \{\theta_1, \dots, \theta_M\}$ را انتخاب می‌کنیم به طوری که از یکدیگر فاصله‌ی معناداری داشته باشند. به طور دقیق‌تر، اگر ρ متريک خطای باشد، برای هر $i \neq j$ باید داشته باشیم $\rho(\theta_i, \theta_j) \geq 2\delta$.

۲. تعریف مسئله‌ی آزمون: فرض می‌کنیم طبیعت^{۴۲} یک اندیس V را به صورت تصادفی و یکنواخت از مجموعه $\{M, \dots, 1\}$ انتخاب می‌کند و داده‌ها بر اساس توزیع P_{θ_V} تولید می‌شوند. هدف، یافتن V بر اساس داده‌های مشاهده شده است.

۳. ارتباط خطاهای خطا: اگر یک تخمین‌گر $\hat{\theta}$ وجود داشته باشد که خطای تخمین آن با احتمال بالا کمتر از δ باشد، می‌توانیم از آن برای حل مسئله‌ی آزمون فرض استفاده کنیم (با انتخاب نزدیک‌ترین θ_i به $\hat{\theta}$). بنابراین، کران پایین روی خطای آزمون فرض، یک کران پایین برای خطای تخمین ایجاد می‌کند:

$$\mathfrak{M}_n(\theta(\mathcal{P})) \geq \Phi(\delta) \cdot \inf_{\psi} \Pr(\psi(Z^n) \neq V) \quad (37-2)$$

۳-۵-۲ نامساوی‌های کران پایین

برای اثبات کران‌های پایین، سه روش اصلی که بر پایه f -واگرایی‌ها بنا شده‌اند را معرفی می‌کنیم:

قضیه‌ی ۲-۲ (نامساوی لو کم^{۴۳}) این روش برای آزمون بین دو توزیع P_1 و P_2 استفاده می‌شود. کمینه احتمال خطای استفاده از فاصله‌ی واریانس کل (رابطه^{۴۴}-۲) کران دار می‌شود:

$$\inf_{\psi} \Pr(\psi(Z^n) \neq V) \geq \frac{1}{2} (1 - \|P_1^n - P_2^n\|_{TV}) \quad (38-2)$$

این روش زمانی مفید است که مسئله را به تشخیص بین دو حالت ساده تقلیل دهیم.

قضیه‌ی ۳-۲ (نامساوی فانو^{۴۵}) زمانی که پارامتر مورد نظر متعلق به مجموعه‌ای بزرگ‌تر \mathcal{V} باشد (تعداد فرضیه‌ها $|\mathcal{V}| > 2$)، نامساوی فانو کران پایین قوی‌تری ارائه می‌دهد که مبتنی بر اطلاعات متقابل است:

$$\inf_{\psi} \Pr(\psi(Z^n) \neq V) \geq 1 - \frac{I(Z^n; V) + \log 2}{\log |\mathcal{V}|} \quad (39-2)$$

که در آن V متغیر تصادفی یکنواخت روی مجموعه اندیس‌ها \mathcal{V} است.

⁴¹Packing Set

⁴²Nature

لم ۴-۲ (لم اسود^{۴۵}) این لم مسئله تخمین را به چندین آزمون فرض دودویی مستقل روی مختصات یک ابرمکعب^d $\{1, -1\}$ - تبدیل می‌کند. نسخه دقیق تر آن که در [؟] استفاده شده است، کران پایین را بر اساس فاصله‌ی واریانس کل توزیع‌های مخلوط حاشیه‌ای بیان می‌کند:

$$\mathfrak{M}_n(\theta(\mathcal{P})) \geq \delta \sum_{j=1}^d \left[1 - \|M_{+j}^n - M_{-j}^n\|_{TV} \right] \quad (40-2)$$

که در آن M_{+j}^n و M_{-j}^n توزیع‌های حاشیه‌ای مخلوط روی مقادیر $+1$ و -1 در بعد j -ام هستند.

فصل ۳

تحلیل‌های مبتنی بر انقباض و نرخ‌های مینیماکس

۱-۳ 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 [۲] توسعه داده شده است. ایده مرکزی این چارچوب، نگاه به مکانیزم‌های محرمانگی به عنوان «عملگرهای انقباضی»^۱ است. به بیان شهودی، اعمال شرط α -LDP باعث می‌شود که توزیع‌های خروجی $(M|x)$ و $(M'|x')$ 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-لایبلر) مدل‌سازی کرد و از آن برای اثبات نرخ‌های مینیماکس در مسائل تخمین آماری استفاده نمود [۲].

۲-۳ 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 [۸].

فرض کنید M یک مکانیزم α -LDP باشد. 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 ۱-۳ (انقباض KL در مکانیزم‌های موضعی) فرض کنید M یک مکانیزم α -LDP 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:

$$D_{KL}(M(\cdot|x) \| M(\cdot|x')) \leq 4(e^\alpha - 1)^2 \quad (1-3)$$

به طور دقیق‌تر، اگر $1 \leq \alpha$ باشد، این کران به صورت $O(\alpha^2)$ رفتار می‌کند [۲].

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 α -LDP می‌دانیم که برای هر $z \in \mathcal{Z}$:

$$e^{-\alpha} \leq \frac{q(z|x)}{q(z|x')} \leq e^\alpha \quad (2-3)$$

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:

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

$$\leq \int p(z) \left(\frac{p(z)}{q(z)} - 1 + \frac{1}{2} \left(\frac{p(z)}{q(z)} - 1 \right)^2 \right) dz \quad (4-3)$$

با اعمال کران‌های α -LDP 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 [۲] 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 α -LDP 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 [۹] یا واگرایی E_γ نیز بیان کرد که در فصل بعد به آن می‌پردازیم. [۱۰]

³Strong Data Processing Inequality (SDPI)

۱-۲-۳ 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 [۲]:

قضیه‌ی ۲-۳ (انقباض TV) تحت شرایط مشابه، برای هر مکانیزم α -LDP :

$$\|\mathcal{M}(\cdot|x) - \mathcal{M}(\cdot|x')\|_{TV} \leq \min\{1, e^\alpha - 1\} \cdot \|x - x'\|. \quad (5-3)$$

(در اینجا $\|x - x'\|$ نشان‌دهنده فاصله همینگ یا متریک مجزا روی ورودی است). برای α کوچک، این رابطه بیان می‌کند که فاصله آماری خروجی‌ها نمی‌تواند بیشتر از $O(\alpha)$ باشد.

۳-۳ تحلیل نرخ‌های مینیماکس 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 [۲] و بعدها با جزئیات بیشتر در [۱۱] 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 [۱۲].

۳. محاسبه ریسک نهایی: ترکیب نتایج برای رسیدن به کران پایین خطای تخمین.

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

$$I(V; Z^n) \leq \sum_{i=1}^n I(V; Z_i) \leq n \cdot \alpha^2 \cdot C \quad (6-3)$$

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 دلیلی است که «اندازه نمونه موثر» در مدل موضعی برابر با $n\alpha^2$ در نظر گرفته می‌شود.

⁴Le Cam

⁵Lower Bounds

۴-۳ 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 میانگین» (MSE) در نظر می‌گیریم.

قضیه ۴-۳ (کران پایین تخمین میانگین) برای هر مکانیزم α -LDP و هر تخمین‌گر $\hat{\mu}$ ، ماکسیمم خطای مورد انتظار با رابطه زیر محدود می‌شود [۲]:

$$\inf_{\hat{\mu}, \mathcal{M}} \sup_P \mathbb{E}_{\|\hat{\mu} - \mu\|^2} \geq \Omega \left(\frac{d}{n \min\{\alpha, \alpha^2\}} \right) \quad (4-3)$$

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 ۱-۳ و نامساوی پینسکر، می‌دانیم که:

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

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.

۵-۳ محدودیت‌های تحلیل کلاسیک

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

همان‌طور که در رابطه (۱-۳) 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 و اگرایی 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_7) است [۸، ۱۰] که در فصل آینده به تفصیل به آن خواهیم پرداخت.

فصل ۴

همارزی α -LDP و انقباض E_γ -واگرایی

۱-۴ مقدمه و انگیزه

در فصل پیشین، دیدیم که چگونه دوچی و همکاران [۲] 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 نیست. تعريف- α -LDP (معادله ۸-۲) 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 ديگر به نام E_γ -واگرایی وجود دارد که دقیقاً ساختار هندسى α -LDP را تسخیر می‌کند. ما ثابت خواهيم کرد که شرط α -LDP دقیقاً معادل صفر شدن $-E_\gamma$ -واگرایی (برای $e^\alpha = \gamma$) است. سپس از اين همارزی برای استخراج کرانهای انقباض دقیق^۱ برای سایر واگرایی‌ها استفاده خواهیم کرد که نتایج دوچی را بهبود می‌بخشند [۱۰].

¹Tight

۲-۴ 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 ۱-۴ (-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:

$$E_\gamma(P||Q) = \sup_{\mathcal{S} \in \sigma(\mathcal{X})} (P(\mathcal{S}) - \gamma Q(\mathcal{S})) \quad (1-4)$$

این تعریف را می‌توان به صورت بسطهی زیر نیز نوشت:

$$E_\gamma(P||Q) = \int_{\mathcal{X}} \max\{\cdot, p(x) - \gamma q(x)\} d\mu(x) \quad (2-4)$$

که در آن p و q توابع چگالی احتمال هستند.

۱-۲-۴ 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:

$$E_1(P||Q) = \sup_{\mathcal{S}} (P(\mathcal{S}) - Q(\mathcal{S})) = \|P - Q\|_{TV} \quad (3-4)$$

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 مرتبط می‌کند.

۳-۴ قضیه همارزی اصلی

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

قضیه‌ی ۱-۴ (همارزی α -LDP) یک مکانیزم \mathcal{M} در شرط $E_\gamma \cdot e^\alpha \Pr[\mathcal{M}(x) \in \mathcal{S}] \leq \Pr[\mathcal{M}(x') \in \mathcal{S}]$ می‌کند اگر و تنها اگر برای تمام جفت ورودی‌های $x, x' \in \mathcal{X}$

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

اثبات. اثبات را در دو جهت انجام می‌دهیم.

جهت اول (\Rightarrow): فرض کنید \mathcal{M} خاصیت α -LDP دارد. طبق تعریف ۵-۲، برای هر زیرمجموعه خروجی $\mathcal{S} \subseteq \mathcal{Z}$ و هر $x, x' \in \mathcal{X}$:

$$\Pr[\mathcal{M}(x) \in \mathcal{S}] \leq e^\alpha \Pr[\mathcal{M}(x') \in \mathcal{S}] \quad (5-4)$$

این نامساوی را می‌توان به صورت زیر بازنویسی کرد:

$$\Pr[\mathcal{M}(x) \in \mathcal{S}] - e^\alpha \Pr[\mathcal{M}(x') \in \mathcal{S}] \leq 0 \quad (6-4)$$

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 ۱-۴، این سوپریمم دقیقاً همان E_{e^α} است. چون E_γ نمی‌تواند منفی باشد (با انتخاب $\mathcal{S} = \emptyset$ 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} :

$$\Pr[\mathcal{M}(x) \in \mathcal{S}] - e^\alpha \Pr[\mathcal{M}(x') \in \mathcal{S}] \leq 0 \quad (7-4)$$

که بلافارسله نتیجه می‌دهد:

$$\frac{\Pr[\mathcal{M}(x) \in \mathcal{S}]}{\Pr[\mathcal{M}(x') \in \mathcal{S}]} \leq e^\alpha \quad (8-4)$$

□ این دقیقاً همان تعریف α -LDP است.

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

۴-۴ بهبود کران‌های انقباض

در فصل ۳ دیدیم که دوچی [۲] کران زیر را برای انقباض KL ارائه کرد:

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

حال با استفاده از چارچوب E_γ ، می‌توانیم کران‌های بسیار دقیق‌تری استخراج کنیم. آسوده و همکاران [۱۰] 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 ۴-۲ (کران دقیق انقباض KL) اگر \mathcal{M} یک مکانیزم α -LDP باشد، آنگاه:

$$D_{KL}(\mathcal{M}(\cdot|x) \parallel \mathcal{M}(\cdot|x')) \leq \frac{e^\alpha - 1}{e^\alpha + 1} \cdot (e^\alpha - 1) \quad (10-4)$$

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:

$$\bullet \text{ کران دوچی: } 4(e^\alpha - 1)^2 \approx 4\alpha^2$$

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

این بهبود ضریب ثابت (از 4 به 0.5) در تحلیل‌های مینیماکس بسیار حیاتی است و نشان می‌دهد که «اندازه نمونه موثر» واقعی می‌تواند تا 8 برابر بهتر از چیزی باشد که آنالیزهای قبلی نشان می‌دادند.

۵-۴ 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:

$$\Pr[\mathcal{M}(x) \in \mathcal{S}] \leq e^\alpha \Pr[\mathcal{M}(x') \in \mathcal{S}] + \delta \quad (11-4)$$

با بازنویسی این رابطه داریم:

$$\sup_{\mathcal{S}} (\Pr[\mathcal{M}(x) \in \mathcal{S}] - e^\alpha \Pr[\mathcal{M}(x') \in \mathcal{S}]) \leq \delta \quad (12-4)$$

که دقیقاً معادل است با:

$$E_{e^\alpha}(\mathcal{M}(\cdot|x)||\mathcal{M}(\cdot|x')) \leq \delta \quad (13-4)$$

نتیجه‌ی ۳-۴ محرمانگی تقریبی $\text{-LDP}_{\alpha, \delta}$ دقیقاً معادل محدود کردن مقدار 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.

۶-۴ 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 مینیماکس برای این مسئله تحت شرط α -LDP برابر است با:

$$\mathfrak{M}_n \asymp \frac{k}{n(e^\alpha - 1)^2} \quad (14-4)$$

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.

۷-۴ 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 [A]، نشان داده شده است که مکانیزم‌های موضعی خاصیت «انقباض قوی» را برای طیف وسیعی از واگرایی‌ها به ارمغان می‌آورند.

۱-۷-۴ 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 مینیماکس بسیار ساده‌تر از KL است.

قضیه‌ی ۴-۴ (انقباض χ) 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:

$$\chi^*(MP||MQ) \leq \eta_\alpha \cdot \chi^*(P||Q) \quad (15-4)$$

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

$$\eta_\alpha = \left(\frac{e^\alpha - 1}{e^\alpha + 1} \right)^2 \quad (16-4)$$

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

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

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 «تاít» (Tight) است.

۲-۷-۴ تعمیم به سایر واگرایی‌ها

نویسنده‌گان در [A] 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 مجدور H^2 و واگرایی KL) نیز صادق است.

نتیجه‌ی ۵-۴ برای هر مکانیزم α -LDP، کران‌های زیر برقرار هستند:

$$D_{KL}(MP||MQ) \leq \eta_\alpha \cdot D_{KL}(P||Q) \quad (18-4)$$

$$H^*(MP, MQ) \leq \eta_\alpha \cdot H^*(P, Q) \quad (19-4)$$

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

۸-۴ نامساوی ونتریز خصوصی (Inequality Private van Trees)

اکثر تحلیل‌های موجود در ادبیات α -LDP (مانند کارهای دوچی)، بر روی «ریسک مینیماکس» (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 [۸] نسخه‌ی خصوصی شده‌ی این نامساوی را ارائه کردند که ابزاری نوین در جعبه‌ابزار تحلیل محروم‌گی محسوب می‌شود.

قضیه‌ی ۶-۴ (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^۹ دارای کران پایین زیر است:

$$\mathbb{E}_{(\hat{\theta}-\theta)^2} \geq \frac{1}{\mathbb{E}_{\mathcal{I}(\theta)} + \mathcal{I}_{prior}(\pi)} \quad (20-4)$$

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

$$\mathcal{I}_{priv}(\theta) \leq \eta_\alpha \cdot \mathcal{I}_{orig}(\theta) \quad (21-4)$$

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 اندازه $\alpha^2/4$ $\approx \eta_\alpha$ تضعیف می‌شود.» این نتیجه، اثبات حدود پایین برای مسائل تخمین پارامتر را بسیار ساده می‌کند. به جای درگیر شدن بالمهای پیچیده اسود یا فانو، کافیست اطلاعات فیشر مسئله‌ی اصلی را محاسبه کنیم و در ضریب η_α ضرب کنیم.

۹-۴ کاربردهای نوین و بهبود نرخ‌ها

استفاده از کران‌های انقباض قوی (بخش ۴-۴) و نامساوی ونتریز خصوصی (بخش ۴-۸) 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:

$$R_{opt} \asymp \left(\frac{1}{n\alpha^2} \right)^{\frac{1-\beta}{1+\beta}} \quad (22-4)$$

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 ۵

نتیجه‌گیری

Bibliography

- [1] C. Dwork. Differential privacy. In *International colloquium on automata, languages, and programming*, pages 1–12. Springer, 2006.
- [2] J. C. Duchi, M. I. Jordan, and M. J. Wainwright. Local privacy and statistical minimax rates. In *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*, pages 429–438, 2013.
- [3] T. Wang, X. Zhang, J. Feng, and X. Yang. A comprehensive survey on local differential privacy toward data statistics and analysis, 2020.
- [4] S. L. Warner. Randomized response: A survey technique for eliminating evasive answer bias. *Journal of the American statistical association*, 60(309):63–69, 1965.
- [5] P. Kairouz, S. Oh, and P. Viswanath. Extremal mechanisms for local differential privacy. *J. Mach. Learn. Res.*, 17(1):492–542, Jan. 2016.
- [6] I. 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] 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.
- [8] S. Asoodeh and H. Zhang. Contraction of locally differentially private mechanisms. *IEEE Journal on Selected Areas in Information Theory*, 5:385–395, 2024.
- [9] P. Cuff and L. Yu. Differential privacy as a mutual information constraint. In *Proceedings of the ACM Conference on Computer and Communications Security*, pages 43–54, 2016.

- [10] S. Asoodeh, M. Aliakbarpour, and F. 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.
- [11] J. C. Duchi, M. I. Jordan, and M. J. Wainwright. Minimax optimal procedures for locally private estimation. *Journal of the American Statistical Association*, 113(521):182–201, 2018.
- [12] L. P. Barnes, W. N. Chen, and A. Özgür. Fisher information under local differential privacy. *IEEE Journal on Selected Areas in Information Theory*, 1:645–659, 2020.

واژه‌نامه

الف	
س	ب
ش	پ
ص	ت
غ	ج
ف	ح
ق	خ
ک	د
گ	داده دودوبی
م	ر
مجموعه	ز
ن	

۵

۶

پیوست آ

مطالب تكميلی

Abstract

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

Keywords: Thesis, Typesetting, Template, X_EPersian



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

February 2026