הרחב יותר של רגרסיה. בכך, אנו מקבלים את התוצאה הראשונה הממירה בעיות הרגרסיה גנריות לבעיות דחיסה באופן המבטיח שהמידע שאבד בתליך הינו קטן באופן שרירותי.

תחום הפרטיות הדיפרנציאלית חווה פריחה בשנים האחרונות, אך יחד עם זאת, ישנן משימות יסוד שהבנתן אינה מלאה. בחלק השני של עבודת דוקטורט זו, אנו בוחנים את קו המחקר העוסק בשאלה:

כמה נתונים נדרשים כדי ללמוד מנתונים, תוך הבטחה שהפרטיות אינה מופרת?

כימות זה של גודל הנתונים הדרוש מכונה מורכבות המדגם של הבעיה. אנו בוחנים משימה אחת כזו - לימוד מלבנים מיושרים לצירים. ידוע שהתלות של כמות המידע הנדרשת במימד הבעיה חייבת להיות ליניארית לפחות, אך עבודות קודמות שהשיגו תלות אופטימלית כזו דרשו ממורכבות המדגם לגדול באופן לוגריתמי בגודל המרחב. אנו מציגים אלגוריתם חדשני שמשיג את שניהם גם יחד, מכיוון שכמות הנתונים שהוא דורש גדלה באופן ליניארי במימד וקטן באופן אסימפטוטי מהלוג של גודל המרחב. הטכניקה המשמשת על מנת להשיג שיפור זה כרוכה במחיקה של נתונים "שנחשפו" תוך כדי ריצת האלגוריתם, כך שההשפעה של כל פרט על התוצאה הסופית מוגבלת באופן המובנה בתכנון האלגוריתם.

בחלק השלישי של הדוקטורט, אנו חוקרים את עצם ההגדרה של למידה פרטית. ההגדרה הסטנדרטית של למידה מכוונת לספק ערבויות דיוק, בהנחה שההתפלגות הבסיסית של הנתונים היא הגרועה ביותר בכל פעם. ישנו קול הולך וגובר במחקר הדוגל בכך שההגדרה הזו פסימית מדי, כלומר אינה משקפת את המאפיינים האמיתיים של נתונים אמיתיים. פרדיגמת המקרה הגרוע ביותר מואשמת בהיותה חלק מהפער הידוע בין תיאוריה לפרקטיקה בלמידת מכונה. יתרה מכך, השפעה של פסימיות זו מתגברת תחת דרישת הפרטיות. כך למשל, ישנן בעיות יסוד שפשוט בלתי אפשרי ללמוד תחת מגבלת הפרטיות, זאת בניגוד לכך שקיים להם פתרון פשוט כאשר מגבלה זו לא נדרשת. אנו מצטרפים לקו העבודה הזה, ומציגים טיעונים בעד שימוש במודל גמיש יותר בשם "למידה אוניברסלית", וחוקרים את יתרונותיו על פני המודל הקלאסי.

לבסוף, בחלק האחרון של תזה זו, אנו עוברים לעסוק בניתוח נתונים אדפטיבי. המחקר בתחום זה סובב סביב הניסיון לייצר כלי ניתוח במודל פורמלי ללמידה שמטרתו להתקרב יותר לתהליך המתרחש במעבדות ובפרקטיקות שונות של ניתוח נתונים. במקום מודל סטטי של ניתוח שבו נשאלת שאלה אחת ומתקבלת תשובה אחת, במודל האדפטיבי נשאלות שאילתות מחקר ובחינות סטטיסטיות רבות באופן שכל שאילתה נובעת מהמידע שנצבר במהלך התהליך האנליטי הקודם. במודל כזה, שקרוב מאוד לתהליך ריאליסטי, הבנות סטטיסטיות מהמודל הסטטי הרגיל אינן תקפות. מחקר בתחום זה משלב רעיונות מספרות הפרטיות והדחיסה, מכיוון שניתן להשתמש בשניהם לתכנון אלגוריתמים אמינים תחת מודלים אדפטיביים. במסגרת המסגרת המורכבת אך החשובה הזו, אנו חוקרים את הבעיה של הרחבת הכלים והתוצאות מספרות ניתוח נתונים אדפטיבית למצב בו קיימת תלות בין הנקודות שנדגמו. אנו מספקים תוצאות הן עבור כלים מבוססי פרטיות והן עבור כלים מבוססי דחיסה.

לסיכום, עבודה זו שמה לה למטרה להעמיק את ההבנה בכל הנוגע לנקודות ההשקה בין פרטיות דיפרנציאלית, למידת מכונה וסכימות דחיסה, על ידי התייחסות לשאלות המחקר הללו. על ידי כך, אנו מקווים לתרום לפיתוח אלגוריתמי למידה יעילים יותר ומשמרי הפרטיות.

תקציר

למידת מכונה היא תחום הצומח במהירות בתוך מחקר מדעי המחשב, ויש לו פוטנציאל לחולל מהפכה בתעשיות שונות. עם היכולת לעבד כמויות עצומות של נתונים ולשפר את הביצועים לאורך זמן, הפך התחום לכלי רב עוצמה לפתרון בעיות מורכבות והנעת חדשנות, והוא נמצא בשימוש במגוון רחב של יישומים בתעשייה.

בתזה זו אנו בוחנים שני נושאים הקשורים זה בזה בתחום למידת המכונה - פרטיות ודחיסה. הגידול הדרמטי בייצור ושימוש בנתונים בשנים האחרונות הביא להזדמנויות חסרות תקדים ללמידת מכונה ויישומים מבוססי בינה מלאכותית. עם זאת, ככל שהנתונים הופכים ליותר ויותר אישיים ורגישים, הצורך בהגנה על פרטיות הפרט הפך משמעותי. פרטיות דיפרנציאלית, מסגרת מתמטית לכימות פרטיות התהליך החישובי של אלגוריתם ביחס לקלט שלו, התגלתה כטכניקה מובילה להתמודדות עם אתגר זה. אם ברצוננו לאפשר את המשך החדשנות וההתקדמות בתחום, ואולי אף להרחיב אותה, יש להבטיח למשתמשים שהשימוש במאגרי המידע לא יאפשר פגיעה בפרטיות של אף משתמש. היבט נוסף שחשיבותו הולכת ומתבררת, ככל שמאגרי מידע גדלים, הוא נושא הדחיסה. בשנים האחרונות אנו עדים לעלייה של מודלים המבוססים על כמויות אדירות של מידע. בין אם מדובר במודלים גדולים של שפה טבעית עם מיליארדי פרמטרים, אלגוריתמים של ניתוח חזותי או מחוללי תמונות שהוכשרו באמצעות טרה-בייטים רבים של תמונות מכל רחבי הרשת, גודל המערכות ומסדי הנתונים מתחיל להוות בעיה. ראשית, גידול זה יוצר אתגרים עצומים בהיבטים החישוביים וההנדסיים הכרוכים באימון מודלים כאלה. כיום ניכר כי ישנן משימות רבות שבהן לא תיתכן התקדמות מצד אף אחד מלבד חברות הטכנולוגיה הענקיות, שכן רק הן יכולות לבצע חישובים בסדר גודל כזה. רעיון אחד שיכול להציע אפשרות לשינוי בפרדיגמה זו הוא דחיסה. הבסיס לרעיון ישן זה הוא שדפוסים במידע, כמו אלה שזוהו על ידי כלי למידת מכונה, יכולים לאפשר לדחוס את הנתונים למספר קטן יחסית של רשומות המכילות את כל הידע הדרוש לדפוס התיוג. אותו היגיון חל גם בכיוון השני. אם ניתן לזהות מספר קטן של רשומות כאלה, אז ניתן למנף תהליך זיהוי זה כדי לייצר תהליכי למידה. רעיון זה עלה באופן טבעי במהלך השנים במסגרת פיתוח אלגוריתמים פופולריים כגון Support Vector Machine ו-Condensed Nearest Neighbor. למרות שרעיון הדחיסה הוא כלי משמעותי בארגז הכלים של המחקר והפיתוח בתחום למידת המכונה, הקשר המדויק בין מושג הדחיסה ללמידה כולל מספר שאלות יסוד בלתי פתורות. עבודת גמר זו חוקרת את נקודת ההשקה של שלושת התחומים הללו על ידי התייחסות לארבע שאלות מחקר שמטרתן להעמיק את ההבנה שלנו לגבי הקשרים בין פרטיות, דחיסה ולמידת מכונה.

הנושא הראשון, שיהווה את הבסיס לתזה זו, נובע מהשאלה הבאה:

באיזו מידה למידת מכונה ודחיסה קשורים זה בזה, הן מבחינה איכותית והן מבחינה כמותית?

שני המושגים ידועים כקשורים מאוד, ולפי כמה הגדרות אפילו שווה ערך. ראשית, אנו חוקרים האם ניתן להרחיב את השקילות הזו למקרים בסיסיים נוספים, ובמיוחד, לפונקציות בעלות ערך ממשי הידועות גם כבעיות רגרסיה. כדי להתמודד עם האתגר, ,תחילה נתחיל בתיאור שיטה חדשה ויעילה להמרת כל אלגוריתם למידה לסכימת דחיסה. לאחר מכן נרחיב את הטכניקה הזו מהמקרה הבסיסי של סיווג, כלומר לימוד פונקציות בינאריות, למקרה