תרגיל 1 – למידת מכונה

1.1

נתון לנו שיש מסווג (נסמן אותו ב- M) שהוא מסווג באופן וודאי את הנקודות. כלומר, בהינתן נקודה מחזיר האם היא חיובית או שלא. באופן פורמלי נתונים מספרים $a_1 \leq b_1, a_2 \leq b_2$, ובהינתן השאלה האם הנקודה נמצאת בין טווח המספרים אזי אם התשובה חיובית מחזיר 1 (נקודה חיובית), ואחרת 0.

התשובה מתייחסת לנתון בשאלה כי המלבן מיושר לצירים.

טענה: האלגוריתם A מחזיר את המלבן הקטן ביותר שמכיל את כל הנקודות החיוביות בסט האימון, ואינו מכיל אף נקודה שלילית.

ולמה?

נניח כי המלבן ש- A מחזיר מוגדר כך: בין c_1 ל- d_1 ובין c_2 ל- d_2. ונניח בשלילה שהוא מכיל נקודה שלילית. כלומר קיימת נקודה שלילית (y_1, y_2) כך שמתקיים:

$$c_1 \leq y_1 \leq d_1 \quad , \quad c_2 \leq y_2 \leq d_2$$

אם המלבן ש- A החזיר הוא הקטן ביותר המכיל את כל הנקודות החיוביות אזי לא קיימת נקודה חיובית בטווח שבין חוץ המלבן הקטן ביותר לבין הגבול של המלבן של המסווג M. באופן פורמלי:

לא קיימת נקודה חיובית (x_1, x_2) כך ש-

$$a_1 \leq x_1 < c_1, \qquad d_1 \leq x_1 < b_1, \qquad a_2 \leq x_2 < c_2, \qquad d_2 \leq x_2 < b_2$$

ולכן המלבן הקטן ביותר מוכל במלבן של המסווג שאנו מניחים שמסווג נכון.

ולכן אם במלבן הקטן ביותר המוחזר מ- A יש נקודה שלילית, אזי גם היא תהיה בתוך המלבן של המסווג הנכון. **זוהי סתירה להנחה** שבמסווג הנכון אין נקודות שליליות בטווח: $a_1 \leq b_1, a_2 \leq b_2$

ולכן A הוא $Empirical\ Risk\ Minumization$. כלומר, אלגוריתם A מביא למינימום את הטעות (ה- $Loss$) על סט האימון.

1.2

נרצה להוכיח כי:

$$\mathbb{E}_{S\sim D^m}[L_S(h)] = L_D(h)$$

לפי הנתון מתקיים כי:

$$\mathbb{E}_{S\sim D^m}[L_S(h)] = \mathbb{E}_{S\sim D^m}\left[\frac{1}{m}\sum_{i=1}^{m}\mathbb{1}_{[h(x)\neq f(x)]}\right]$$

כעת נכניס את התוחלת לתוך הביטוי בסיגמא (מלינאריות התוחלת):

$$\frac{1}{m}\sum_{i=1}^{m}\mathbb{E}_{S\sim D^m}\left[\mathbb{1}_{[h(x)\neq f(x)]}\right]$$

נשים לב שכעת התוחלת $\mathbb{E}_{S\sim D^m}\left[\mathbb{1}_{[h(x)\neq f(x)]}\right]$ זוהי למעשה התוחלת של x כלשהו מתוך ההתפלגות D. ומזה נקבל כי:

$$\mathbb{E}_{S\sim D^m}\left[\mathbb{1}_{[h(x)\neq f(x)]}\right] = \mathbb{E}_{x\sim D}\left[\mathbb{1}_{[h(x)\neq f(x)]}\right]$$

בנוסף, אנו יודעים מ"הסתברות" שהתוחלת של $Indicator$ היא ההסתברות עצמה, כלומר נקבל כי:

$$\mathbb{E}_{x\sim D}\left[\mathbb{1}_{[h(x)\neq f(x)]}\right] = \mathbb{P}_{x\sim D}\left[[h(x) \neq f(x)]\right]$$

ולכן נקבל כי:

$$\frac{1}{m}\sum_{i=1}^{m} \mathbb{E}_{S\sim D^m}\left[\mathbb{1}_{[h(x)\neq f(x)]}\right] = \frac{1}{m}\sum_{i=1}^{m} \mathbb{P}_{x\sim D}\left[[h(x) \neq f(x)]\right] = \frac{1}{m}\sum_{i=1}^{m} L_D(h)$$

נשים לב שהביטוי $\frac{1}{m}\sum_{i=1}^{m} L_D(h)$ הוא סכימה של אותה הסתברות m פעמים ואז לחלק ב- m,
ולכן נקבל כי:

$$\frac{1}{m}\sum_{i=1}^{m} L_D(h) = L_D(h)$$

ולסיום נקבל כי:

$$\mathbb{E}_{S\sim D^m}[L_S(h)] = \mathbb{E}_{S\sim D^m}\left[\frac{1}{m}\sum_{i=1}^{m} \mathbb{1}_{[h(x)\neq f(x)]}\right] = L_D(h)$$

כנדרש.

ההיגיון בהוכחה הוא: הביטוי $\mathbb{E}_{S\sim D^m}[L_S(h)]$ זוהי תוחלת - על קבוצות אימון S בגודל m מתוך התפלגות D - של ה- $empirical\ risk$. בוחרים שוב ושוב קבוצות אימון S מתוך התפלגות D באופן אין סופי. מה שיקרה לבסוף הוא שהתוחלת על ה- $empirical\ risk$ תהיה שווה ל- $true\ risk$.