

# דוח מעבדה

טים בוכבינדר 313419814

מבוא:

המטרה של פרויקט זה היא לבנות מודל שמזהה תמונות של חתולים משאיות ורכבים בדיוק כמה שיותר גבוהה בהינתן דאטא סט ורשת ניורונים קבועים שניתנו לנו.

בדוח אחקור את הבעיה ואציע פתרונות אפשריים שיעזרו למקסם את הדיוק של המודל.

בכל שלב:

(1) אציג את הביצועים הנוכחיים של המודל בעזרת וויזואליזציה של התוצאות

(2) אעלה בעיה שלדעתי כדאי להתמקד בה

(3) אציע פתרון אפשרי.

(4) אציג את התוצאות לאחר הפתרון.

לפני שנתמקד בשיפור המודל עלינו להכיר את הדאטא איתה אנחנו עובדים,

ממבט קצר ניתן לראות כי 88% מהתמונות הן של רכבים, כלומר הדאטא מאוד לא מאוזן.

כמו כן לאחר הצגת התמונות והלייבלים (במחברת JUPYTER) ניתן לראות כי קיימות לא מעט תמונות של חתולים שמתוייגות כרכבים.

המחשה קצרה להתפלגות הדאטא (DEV+TRAIN)

DEV	TRAIN
88.16% of the labels are cars	87.98222222222222% of the labels are cars
8.16% of the labels are trucks	7.982222222222222% of the labels are trucks
3.68% of the labels are cats	4.035555555555556% of the labels are cats

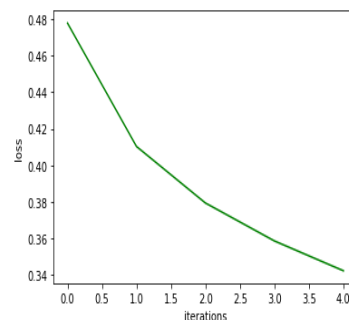
כעת לאחר שלמדנו את הדאטא נתחיל מלבנות מודל מאוד פשוט, בעזרתו נוכל "להרגיש" את הבעיה, את התוצאות שלו נוכל לנתח ולגלות איפה כדאי להשתפר.

המודל מתאמן על הדאטא הגולמית ( כמו שקיבלנו אותה) במשך 5 אפוקים עם OPTIMIZER ADAM

ההיפר פרמטרים של המודל דיפולטים ברובם, אלו התוצאות עבור המודל:

הגרף מראה את ה LOSS בTRAIN במשך האפוקים, הנתונים מראים את אחוז הדיוק על DEV

Accuracy of car : 100 %  
Accuracy of truck : 0 %  
Accuracy of cat : 0 %



Accuracy of the network test images: 88 %

## מסקנות:

אפשר לראות שהמודל מסווג את כל התמונות כרכבים, אמנם הוא משיג אחוז דיוק לא רע על DEV ברור לנו שצריך לשפר את המודל.

ראינו קודם ש88% מהתמונות שלנו הם רכבים, זאת אחת הסיבות שהמודל לא מצליח ללמוד איך לסווג חתולים ומשאיות.

כדי שהמודל יצליח ללמוד ולהכליל עבור האובייקטים השונים נרצה לאזן את הדאטא.

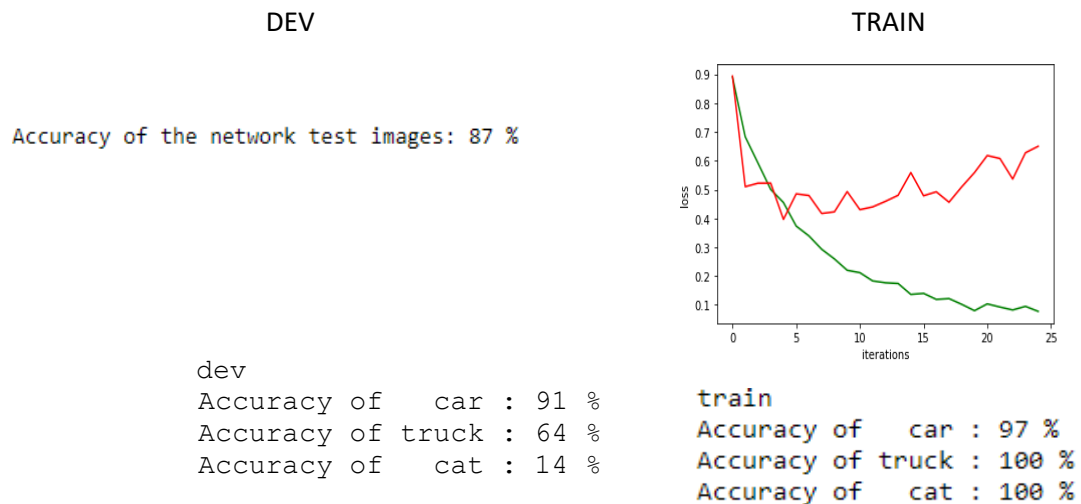
**השלב הבא אם כך הוא לאזן את הדאטא:**

איזנתי את BATCHES בעזרת WEIGHTED SAMPLER

כל לייבל קיבל משקל 1 פחות אחוז ההופעות שלו בדאטא

הרצתי 25 אפוקים וקיבלתי :

( הגרף הקו הירוק מסמל את הLOSS ב TRAIN ובאדום הLOSS ב DEV ) בהמשך הוספתי LEGEND



## מסקנות:

ניתן לראות כי אחוז הדיוק של המודלמלא השתנה אך כעת הוא מצליח לסווג גם משאיות וחתולים.

אמנם הוא עדיין מזהה חתולים בצורה רעה מאוד.

כמו כן ניתן לראות בבירור את ה OVERFITTING של המודל.

אחוז תמונות החתולים בדאטא עדיין נמוך יחסית ואולי זאת אחת הסיבות שהמודל לא מזהה חתולים טוב.

השיפור הבא שאציע יהיה :

**להגדיל את כמות החתולים בכל BATCH ( כלומר לתת משקל יותר גבוהה לחתולים ב SAMPLER )**

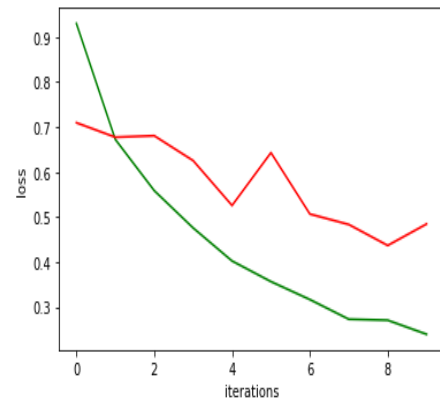
**ולהוריד את מס האפוקים.**

תוצאות:

DEV

TRAIN

Accuracy of the network test images: 83 %



Accuracy of car : 85 %  
Accuracy of truck : 78 %  
Accuracy of cat : 28 %

train  
Accuracy of car : 91 %  
Accuracy of truck : 100 %  
Accuracy of cat : 100 %

### מסקנות:

ניתן לראות כי אחוז דיוק המודל ירד קצת ( $83 \leftarrow 88$ ) אך הדיוק בסיווג משאיות וחתולים עלה, כלומר המודל קצת יותר מאוזן. אך עדיין מאוד חלש בסיווג חתולים.

סיווג החתולים החלש של המודל יכול לנבוע מכך שמספר החתולים בדאטא הוא הקטן ביותר (3%), ולכן כאשר אני מאזן את התמונות בדאטא אני יוצר הרבה שכפולים בתמונות של החתולים, והמודל OVERFITTING לתמונות האלה, ואכן ניתן לראות כי באימון המודל יודע לזהות 100% מהחתולים.

### מחשבה לשיפור:

אוגמנטציה:

עשיתי לכל תמונה בהסתברות מסויימת אוגמנטציה, כאשר אם התמונה היא של חתול ההסתברות לאוגמנטציה היא הגבוהה ביותר ואילו אם התמונה היא של מכונית ההסתברות לאוגמנטציה נמוכה יותר.

כל אוגמנטציה יכולה להיות אחת מ 7 אפשרויות

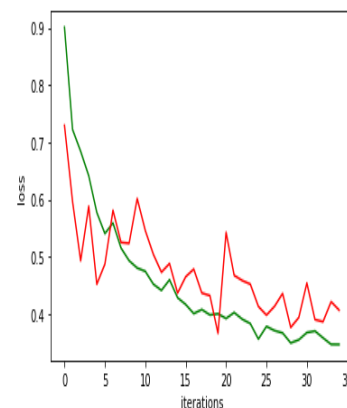
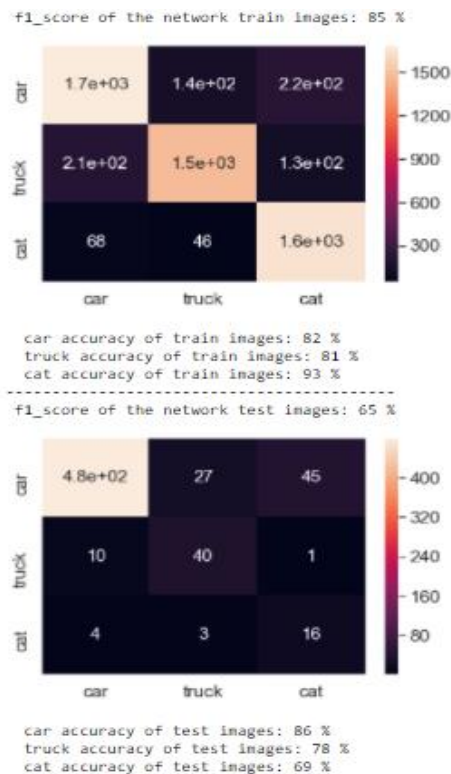
סיבוב מאוזן, מאונך, רוטציה של התמונה, חיתוך והגדלה לגודל המקורי, GRAYSCALE, BLUR, ובהירות.

כעת לכל תמונה של חתול הסתברות גבוהה לעבור שינוי ולכן המודל יראה מספר יותר גדול של תמונות חתולים שונות, ובכך יקטן האוברפיטינג שהמודל יעשה לתמונות מסויימות.

שינתי את האבלואציה ל PERCISION-RECALL ו CONFUSION MATRIX כדי לקבל הבנה יותר טובה על התוצאות.

הסבר על המטריקות <https://www.dataschool.io/simple-guide-to-confusion-matrix-terminology>

## תוצאות:



## מסקנות:

אפשר לראות שהרשת למדה לזהות חתולים בדיוק לא רע.

אך כעת הבעיה היא בזיהוי הלא נכון של המכוניות. ניתן לראות שמספר המשאיות שהרשת מזהה כמכוניות ומספר המכוניות שהרשת מזהה כמשאיות הוא די גבוהה ( 27,10 בהתאמה) אך המצב הזה סביר שכן יש הרבה פיצרים משותפים למכוניות ומשאיות.

הנתון החריג הוא מספר המכוניות שמתויגות על ידי המודל כחתולים. הזכרנו בניית הדאטא שהרבה תמונות של חתולים מתויגות לא נכון ( מתויגות כרכבים) דבר שיכול לגרום למודל לטעות בין חתול לרכב.

## פתרון אפשרי הוא לתקן את הדאטא:

הרצתי את המודל המאומן על ה TRAINSET ובדקתי את התמונות שהמודל מתייג כחתול אבל הן מתויגות כרכב או משאית.

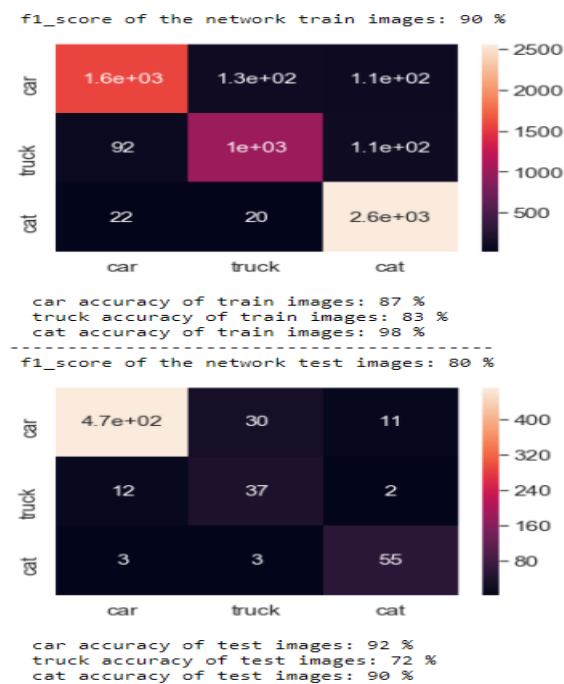
הרבה מהתמונות שהמודל זיהה כחתול אכן היו מתויגות בדאטא לא נכון.

כמובן שהתיקון הזה לא מבטיח שתיקנתי את כל התמונות שמתויגות לא נכון אבל זו דרך מהירה למצוא חלק מהן.

התהליך בוצע גם ל־TRAIN וגם ל־DEV

הדאטא המתוקן נמצא בקבצים: fixed\_dev\_set.pickle, fixed\_train\_set.pickle

## תוצאות:

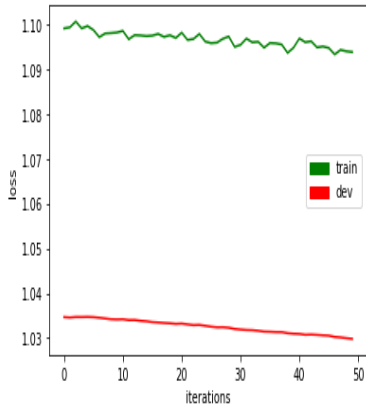
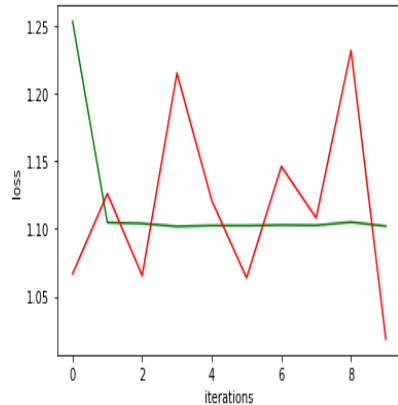


## מסקנות:

ניתן לראות את השיפור המשמעותי בכמות המכוניות שהמודל מתייג כחתולים ומכאן גם שיפור גדול ב f1\_score ובאחוזי דיוק ב זיהוי חתולים ורכבים. התוצאות שקיבלנו לא רעות ביחס לרשת הפשוטה והדאטא הלא מאוזן שקיבלנו.

כעת נשאר "לשחק" עם ההיפר פרמטרים הנותרים. בתור OPTIMIZER נראה היה ש ADAM עבד הכי טוב ( ההיפר הפרמטרים הקשורים אליו מפורטים במחברת ה JUPYTER ).

## LR

(3e-7) (LOW)		0.05 (HIGH)	LR
			GRAPH
<p>גם כאן אפשר לראות שהמודל כמעט לא לומד, העדכונים של הפרמטרים מאוד קטנים ועל כן הוא לומד מאוד לאט (כמעט ולא היה שינוי ב 50 אפוקים) אפשר לראות שה DEV כאן נמוך בהרבה מה TRAIN זה קורה בגלל ההתפלגות השונה של ה DEV מה TRAIN מכיוון שרוב התמונות ב DEV הן מכוניות אם המודל מתייג מכוניות בצורה קצת יותר טובה ה DEV יהיה יותר נמוך, אבל ניתן לראות שגם ה DEV לא משתפר במשך הזמן</p>		<p>אפשר לראות שהמודל לא לומד כאשר LR גבוהה מדי העדכונים של הפרמטרים גדולים מדי, והקפיצות של המודל גדולות מדי לכן המודל לא מצליח להתכנס ( מפספס את נקודת המינימום בקפיצות גדולות מדי ).</p>	CONCLUSIONS

שתי הדוגמאות שהראיתי הן כמובן קיצוניות, השלב הבא הוא לחפש את ה LR המתאים. אם להסתכל על התוצאות אכן עבור חלק מערכי ה LR המודל לא לומד בכלל ועבור חלקם הוא לומד מאוד לאט. לאחר נסיון על כמה ערכים בצורה רנדומית נראה שהערך הטוב ביותר הוא בערך  $10000/3$

## Adversarial

הסבר:

טענתי את המודל שלי ובחרתי תמונה מהדאטא סט, בחרתי תמונה של משאית מכיוון שהקטגוריה הכי קטנה היא של תמונות של משאית שהמודל תייג כחתול, כלומר מבחינת המודל חתול ומשאית מאוד רחוקים אחד מהשני.

נתתי למודל להריץ את התמונה שבחרתי, התוצאה של המודל היא שבהסתברות של 96% התמונה היא אכן של משאית. ( הגיוני , התמונה נלקחה מה TRAINSET )

תייגתי את התמונה כחתול ונתתי למודל להריץ את התמונה 5 פעמים ( num\_steps ) כאשר בכל איטרציה

(1) המודל מחשב את ה LOSS ( ה LOSS מחושב לפי התיוג השגוי )

(2) המודל מחשב את הנגזרת של LOSS ביחס לתמונה עצמה

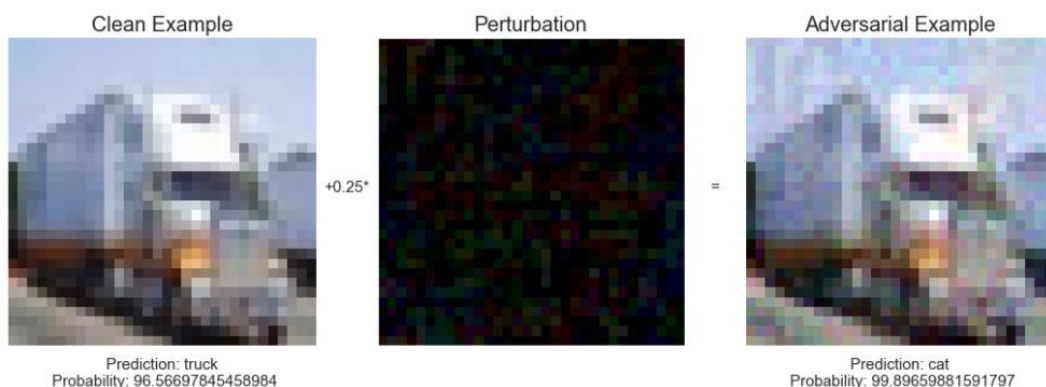
(3) מעדכן את התמונה

כלומר במהלך האיטרציות אף פרמטר מהמודל לא מתעדכן פרט לתמונה עצמה

לבסוף נתתי למודל את התמונה המעודכנת ( ADVERSIAL )

ובדקתי מה הוא חושב עליה עכשיו

אלו התוצאות :



**התמונה השמאלית** היא התמונה של התמונה המקורית שהמודל חושב שהיא משאית בהסתברות 96%

**התמונה הימנית** היא התמונה לאחר שעדכנו את התמונה אך כעת המודל חושב שהתמונה היא חתול בהסתברות של 99%

**התמונה האמצעית** היא הרעש שהוספנו לתמונה המקורית כדי "לעבוד" על המודל

ניתן לראות שהתמונה המקורית והמעודכנת מאוד דומות אך לא בשביל המודל