

Review 1: Curriculum by Smoothing

תחום מאמר: ארכיטקטורות CNN, למידת curriculum

מושגים ו כלים מתמטיים במאמר: קרנלים גאוסיאניים

מאמר הציג בכנס: NeurIPS

תמצית מאמר: המאמר מציע להוסיף קרנלים (מסוגנים) גאוסיאניים מחלקיים עם עצמת החלקה יורדת אחרי כל שכבת קונבולוציה (לפni אקטיבציה) של CNN. קרנלים אלו נועדים להתמודד עם הארטיפקטים בעלי תדרים גבוהים הנוצרים בפייצרים של שכבות CNN (לטענת מחבריו המאמר) בשלבם המוקדם של אימון הרשת. בעצם הגישה שלהם (הנקראת CBS) מזכירה את העיקרון של למידת curriculum: אימון רשותות נוירונים על משימות בעליות רמת קושי הולכת וגדלה. במקרה זה הפיצרים בעלי תדרים נמכים הינם "משימות קלות" ואלו בעלי תדרים גבוהים מיוחסים ל"משימות קשות יותר". בעצם CBS מנסה להוסיף (לשלוט) בכמות האינפורמציה בעלת תדרים גבוהים המגיע לשכבות שונות של CNN.

רעיון בסיסי: אז מה בעצם קורה כאן? בשכבות המוקדמות מוסיפים קרנלים המעבירים רק תדרים נמכים (ערך גובה של פרמטר סיגמא של גאוסיאן). זה אומר בתכלס CBS "מכריחה" את השכבות המוקדמות ללמידה רק מידע בעל תדרים נמכים ("דרגת קושי נמוכה" בשפה של למידת curriculum). ככל שמתקדמיים לשכבות עמוקות יותר אנחנו לאט לאט משחררים ו"מרושים" לרשות ללמידה אינפורמציה בעלת תדרים הולכים וגדלים ("רמת קושי גבוהה"). בנוסף בכך זו הם חוסמים העברת מידע רועש מהשכבה המוקדמת לשכבות יותר עמוקות בתחילת תהליכי אימון של רשת.

תקציר מאמר: כמו שכבר נאמר לעלוה המאמר מציע להוסיף קרנלים גאוסיאניים דו-ממדיים מחלקיים לייצאה של קונבולוציה ולפni האקטיבציה בכל שכבה. אז קודם כל בואו נזכיר מהם בעצם הקרנלים האלה.

קרナル גאוסיאני: קרナル גאוסיאני דו-ממדי זה בעצם טרנספורמציה המוגדרת ע"י פונקציית צפיפות גאוסיאת דו-ממדית בעלת מטריצה קווריאנס covariance^{*} כאשר וקטור התוחלת שלה נמצא (y, x) שבה קרナル זה מופעל. לקרナル זה יש תכונות של מסנן מעביר נמכים וככל שסיגמא הולכת וקטנה הוא מעביר תדרים יותר ויותר גבוהים (קרי יכולת החלקה יורדת).

בחירה סיגמאות של קרנלים: הם מצינים שבבחירה של עצמות החלקה (פרמטרים סיגמא) תלוי רק בגודל המודול ובמשך זמן אימון של רשת (שיש ביניהם קורלציה חיובית). ההסבר שלהם (לא הוכח) הוא זה: ככל שמשך זמן אימון של רשת יותר ארוך, המשקלים של הרשת רוחקים ממרכז האופטימליים ואז צריך "להחלק אותם יותר" כדי למנוע יצירת ארטיפקטים. מעניין שקצב הדעיכה של סיגמאות נשאר קבוע לכל הארכיטקטורות שהם בדקו (שווה ל 0.9).

הישגיה ממאמר:

שיטות השוואה עם SOTA: הרעיון של המאמר הינו מאד פשוט ומובן אך נדרשת הוכחה שגישה זה משפרת ביצועים למגוון ארכיטקטורות ומשימות. אז הם הראו CBS טוביה מ SOTA עבור 3 סוגים של משימות:

1. אימון רשת לטאsek ספציפי (סיווג תמנונות)

הם השוו אימון רשת בצורה רגילה מול CBS לשימוש סיווג הוכחו את עליונותה של CBS למגוון ארכיטקטורות רשת: VGG-18, ResNet18, Wide ResNet-50, ResNext-50

DATA SETS: SVHN, CIFAR10, CIFAR100, ImageNet

1. **הפקת פיצ'רים חזקים** לאותו סוג של **משימה בדומין** אחרת: הם עשו פריטריין של רשות VGG16 על Imagenet רגיל ועם CBS והקפיאו את משקל הרשת. אחר כך הם הוסיפו 3 שכבות FC ואימנו אותם על דאטה סטימ אחרים (SVHN, CIFAR10, CIFAR100). התוצאה - ניצחון לCBS בכללם.

2. **הפקת פיצ'רים חזקים לסוג אחר של משימה:** דומה לשיעף הקודם רק המשימה Downstream היא הינה סגמננטציה סמנטית (Faster-RCNN, Pascal-Voc, VAE). התוצאה: ניצחון לCBS זהה כי מעוניין לדעת: הם השתמשו ב-SBS בשכלי לאמן שני סוגי סוגים של VAE וnicetho את הארכיטקטורה הרגילה מבחינת NLL (שערון של לווי) וגם מבחינת המידע ההדדי בין הייצוג הלטנטי ובין התמונה המוגנרטת עבור דאטה סטימ: CelebA MNIST ו-MNIST.

לינק למאמר: <https://arxiv.org/pdf/2003.01367.pdf>

לינק לקוד: <https://github.com/j3soon/arxiv-utils>

נ.ב. מאוד אהבתי את הרעיון של המאמר, הוא פשוט, קל למימוש ולא דורש יכול הייפר פרמטרים. הם גם הצליחו לשכנע אותי ש CBS מושפרת את ביצועי הרשת למשימות מגוונות. מה שטיפה חסר לי במאמר זו הצדקה תיאורטית כלשהי של "גפנופי ידיים" רבים בו - התקווה שהזה יבוא בהמשך.

Review 2: Contrastive Representation Distillation

תחומי מאמר: המאמר משתמש בשיטה הנקרואות (NCE) המבוססת על מידע הדדי (mutual information) השיכת לתהום למידת הייצוג (representation learning) בשכלי הפקת ידע (knowledge distillation - KD).

הסבר קצר על תחומי השינוי:

קודם כל הלמידת הייצוג זה תחום העוסק בשיטות להפקה ייצוגי מימד נמוך יעילים לדאטה בעלי מימד גבוה. ההנחה המהותית ב NCE הינה שייצוג חזק בהכרח יודע להפריד בין הדוגמא חיובית בהינתן הקונטקסט (הדוגמאות הקשורות או או אינה דוגמא עם אוגמנטציה) לבין דוגמא רנדומלית. בין השימושים של טכניקה זו אפשר להזכיר negative sampling שהשתמשו בו למשל ב-word2vec. במאמר שהציגו infoNCE הוכח כי אם ככל הלווא של NCE קטן המידע הדדי בין הדוגמא במרחב המקורי לבין הייצוג של מרחב מימד נמוך עולה שהזאה מבצע על אובדן פחות אינפורמציה בין הדאטה לבין הייצוג קרי לייצוג פחות לווי ויתר מכך. חשוב לציין שאימון מתבצע במרחב הייצוג לא במרחב המקורי כמו הלווא מחושב על הייצוגים במרחב מימד נמוך. לווי NCE זה בעצם עונה הוא לוחץ זוג דוגמאות קרובות והרבבה דוגמאות רנדומליות ומנסה לקנסם את המנה בין דמיון של זוג הקרוב לסיכון הדמיונות בין לבין דוגמאות רנדומליות.

KD זה תחום שהומצא ע"י Hinton J. הענק בשלהי 2015. התחום עוסק בצמצום (dimensionality reduction) מודלים גדולים וכבדים חישובית למודלים יותר קלים ונוחים יותר לאינפרנס. רוב השיטות של KD מתחולקות לשתי קבוצות:

1. אימון רשת סטודנט כר שהוא יחקה כמה שיותר טוב את הפלט הערך (לפני הסיגמוואיד) של רשת (או רשתות המורה). בדרך כלל משתמשים בקרוס-אנטראופי בין ההסתברויות של רשת המורה ורשת הסטודנט (ההסתברויות מחושבות "תחת טשטוש מסוים הנקרא טפרטוריה", פשוט מחלקים באיזה קבוע את הכניסה לsigmoidoid לאיזה קבוע)

2. שיטות המנסות לגרום לרשת הסטודנט לחקות לא רק את היציאה של השכבה האחורונה של המורה אלא גם יציאות של שכבות ביניהם. יש שם מגוון מאוד רחב של שיטות (יש רפרנסים רבים במאמר)

תקציר המאמר:

از מה שהמאמר הנסקר מציע הוא לאמן רשת הסטודנט כך שהמידע הגרפי בין לבין הייצוג של רשת המורה תהיה מksamלית. כמו שאותם יודעים החישוב של המידע הגרפי בין הרשותות הוא מאוד קשה, והמחברים מציעים להשתמש ב- NCE (יותר נכון ב- infoNCE) בשבייל למקסם את המידע הגרפי. הרי כמו שהזכיר כל ש NCE לוס קטן המידע הגרפי עולה (הם מוכחים את החסם הזה בצורה רגורוזית).

از מה עושים בתכליס, אתם שואלים? לוקחים דוגמא (חיובי) ומעבירים אותו דרך שני הרשותות (מורה וסטודנט). אחר כך לוקחים N זוגות של דוגמאות רנדומליות ומעבירים אותן דרך שני הרשותות גם כן ואז מנסים "להתאים" את NCE לוס לבנייה הבאטץ' שלהם (דוגמא אחת חיובית והשאר שליליות - נוסחה 11 במאמר) כלומר אמן מודל פשוט המשערק אותן. החישוב מתבצע בצורה מאוד דומה ל- infoNCE. ובשלב האחרון מאנים את המשקלים הרשות הסטודנט בשבייל למקסם את מה שיצא בשלב האחרון. כמו הערך המתkeletal בסוף מהוות חסם תחתון למידע הגרפי בין ייצוג הסטודנט לייצוג המורה כך שככל התהילה זהה מיותר להעלאתו.

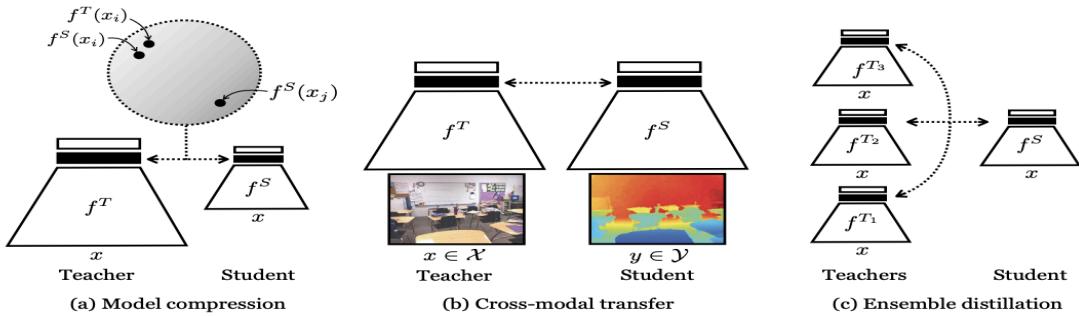


Figure 1: The three distillation settings we consider: (a) compressing a model, (b) transferring knowledge from one modality (e.g., RGB) to another (e.g., depth), (c) distilling an ensemble of nets into a single network. The contrastive objective encourages the teacher and student to map the same input to close representations (in some metric space), and different inputs to distant representations, as indicated in the shaded circle.

הלוס הסופי שלהם מרכיב מהלוס המקורי של `shorten` המבוסס על קירוב אנטרופי בין הייצוגים של הסטודנט ושל המורה והlös המשערק את המידע הגרפי בהתאם בפסקה הקודמת

הישגיה המאמרים: הם מראים את היתרונות של השיטה שלהם על מגוון שיטות SOTA עבור שלוש משימות הבאות:

1. דחיסת המודול (נבדקת כאן ירידה ביצועים של הסטודנט יחסית למורה)
2. Cross-modal transfer (לא יודע איך לתרגם את זה לעברית).

המטרה כאן לנסות לבנות רשת למשימה שיש לסטודנט הרבה דatasets מדויק מאשר למורה

3. למידה מכמה מורים (לי זה נראה ממשימה מאוד לא טרייניאלית)

הערה לגבי הביצועים:

משמעותה השניתה מבחן הביצועים הינה KD קלואס של הינטוון ולא כל שיטות שהומצאו ב 4 שנים האחרונות. זה קצת חמוד מוזר.

данаха Стіпів: V2 CIFAR-100, ImageNet, STL-10, TinyImageNet NYU-Depth

[لينك لمقالة: מאמר](#)

[لينك لكود: code](#)

Review 3: Are Deep Neural Architectures Losing Information? Invertibility Is Indispensable?

המאמר משלב עיני כי שמו בתרגום לעברית "האם רשתות נירונים מאבדים מידע? האם הפיכות נחוצה!"

תחום המאמר: זרימת המידע ברשתות נירונים

הדקמה: קודם כל אנו יודעים היטב שהתשובה על השאלה הראשונה הינה חיובית מהעבודות של פרופ' תשבי שהראה בצורה גורזית שיש אובדן מידע בכלל שכבה (הרי בסופו של דבר במרבית המקרים אנו דוחסים את התמונה לקטור קצר פי 1000 מכמota הפיקסלים בתמונה).

תקציר המאמר על קצה המצלג: המאמר שואל את השאלה המתבקשת האם ניתן לבנות רשת הממחזרת את אובדן המידע הזה. למשל רשת המסוג זהה עשויה להיות טובה למשימות עיבוד תמונה low-level כמו שחזור התמונה או *colorization*.

תקציר: קודם כל אנו מגדירים את אובדן המידע הדדי בין התמונה והציג הlatent שלה. אחר כך הם מוכחים (למרות שהוא די ברור) כי ככל שהסתברות לקבל תמונה X בהינתן הייצוג הלטנטי Z קרוב ל 1 אז המידע הדדי הולך עולה. זה הוביל אותם למסקנה כי לצורך שימוש את המטריה \tilde{Z} הם צריכים לחת את השיטה ליגנרט שנקראת "זרימות מנורמלות" (NF - normalizing flows). העיקרון של NF הינו די פשוט. בוחרים התפלגות לטנטית כלשהי בדרך כלל גאוס או יוניפורמי. ואז מנסים לבנות פונקציה הפיכה (חד-חד ערכית) מרחב התמונות למרחב הלטנטי. אז גינרט התמונות י יצא די פשוט - דוגמים את Z ומפעלים עליה את ההופכית של הפונקציה \tilde{Z} . נשמע לא מסובך אך הבניה של פונקציות כאלה זו ממש מהאוד לא טריומיאלית. אחת הסיבות לכך זה ההופכית של היעקוביאן של הטרנספורמציה (פונקציה) המופיעה בביטוי של הפונקציה ההופכית וכאשר גודל המטריצה הוא עצום החישוב של מטריצה הההפוכה הינו מאד כבד חישובי. אז בונים אותה בצורה autoregressive היעקוביאן יצא מטריצה משולשת עליונה הקלה להיפוך.

בקיצור המאמר לוקח את הארכיטקטורה של NF עם יכולת גינרט היכי גבואה הנקראית GLOW (מבית היוצר של הממצא של VAE דרך אגב) משנים טיפה את הארכיטקטורה (לדעתי זה לא צזה קרייטי למראות שבמאמר נתען אחרת). השינוי המהותי היחיד שהם עושים יחסית ל GLOW זה הוספה של Decoder במקומ להשתמש בהופכית של ה encoder. פונקציית לוט: L1

הם מוכחים שעם הארכיטקטורה הזו הם מצליחים לשפר את הביצועים של שורה של משימות עיבוד תמונה low-level כמו שחזור תמונה, *colorization*, שחזור תמונות דחוסות

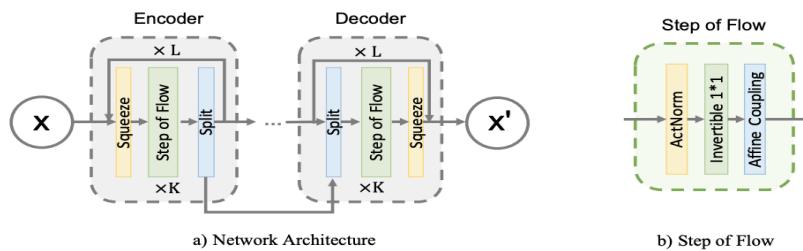


Fig. 1: Architecture of our Invertible Restoring Autoencoder (IRAE) network.
“ActNorm” means “activation normalization”.

הישגי מאמר: שחזור תמונה, *colorization*, שחזור תמונות דחוסות.

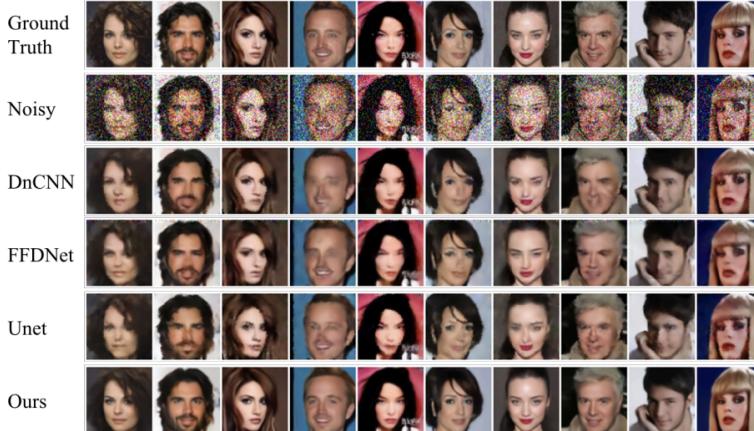


Fig. 2: Qualitative visualization of image denoising of our model compared with other methods. The noise level $\sigma = 50$.

הערות על ניסויים: אני סבור שהניסויים שלהם מאוד מוטים לטובתם ובכלל ההשוואות שהם עשו לא הגיוניות. בגדול הם השוו את הרשות שלהם לרשומות ניקוי רעש בעיבוד תמונה אבל יש שתי נקודות בעייתיות בהשוואה זהו. 1. הרשותות שלהם הם השוו הן לא עדכניות. אחת מהן מ- 2016 והשנייה מ- 2018 ומאז הי' המן שיפורים בתחום.

2. נראה שהם אימנו את הרשות שלהם לדטה 55 ספציפי, למשל סלב, אז בדקנו עלי'ו בעוד שההרשאות האחרות מאומנות על דטה כללי של תמונות טבעיות. ברור הרי שכאשר רשות שאומנה על פרצופים בלבד מחלצת פיצרים הרבה יותר רלוונטיים מרשות שאומנה על תמונות טבעיות כלליות. זה החלק הבועייתי באמת

[לינק למאמר:](#) [paper](#)

[לינק לקוד:](#) [code](#). אפשר להריץ אותו דרך `train.sh`.

ג.ב. לא השתכנעתי מחלוקת הזה בעובדה, בעיקר כאשר יש תחום של היפוך של models generativemodels שאוליך ותווסף תואצה וניתן לעשות השוואות יותר רלוונטיות.

Review 4: Deep Double Descent: Where Bigger Models and More Data Hurts

בין המחברים של המאמר נמנה Ilya Sutskever שהוציא מאמרם בעלי השפעה רבה בתחום.

תחום המאמר: הייתה מגדרו אותו כחקיר תוכנות אימון של רשותות הנוירונים.

תקציר המאמר בשני משפטים: המאמר מצא שיש מצבים שבהם הוספה של טריין דטה כמו כן הגדלה של כמה מושגים ברשות גורמת לעלייה בשגיאת טסט. הקטע הוא שההתופעה הזה אינה זמנית, כלומר אם אנחנו ממשיכים להגדיל את גודל הטריין דטה/להגדיל כמה מושגים ברשות שגיאת טסט מתחלת לרדת

תקציר המאמר:

הטענה העיקרית של המאמר אפשר לסכם באופן הבא: יש בעצם 3 רג'ימיים (מקטיעים) בציר סיבוכיות המודל מבחינת השפעתו על שגיאת הטסט. תופעה זו התגלתה ע"י מ.בלקין ושותפיו ב [Belkin_DD1](#), (2018)

הראשון המודל שנמצא במצב של under parameterized ו כל הגדלה של סיבוכיות המודל כגון (הגדלה של מספר פרמטרים של המודל, אורך האימון, כמות הרעש בלייבור וcdcma) גורמת לירידה של שגיאת הטסט. יש את רגליים הבנויים הנקרה במאמר אינטראול קרייטי כל הגדלה של סיבוכיות המודל גורמת לעלייה בשגיאת הטסט. במקטע השלישי על ציר הסיבוכיות שגיאת הטסט שוב מתחילה לרדת ככל שסיבוכיות המודל עולה(המודל double-descent phenomenon זהו נקראת overparameterized במאמר התופעה זהו נקראת Chzhen).

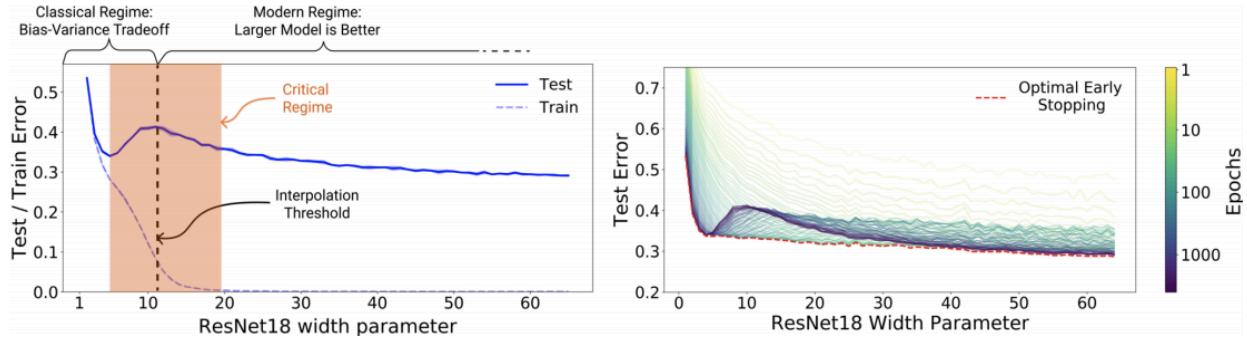


Figure 1: **Left:** Train and test error as a function of model size, for ResNet18s of varying width on CIFAR-10 with 15% label noise. **Right:** Test error, shown for varying train epochs. All models trained using Adam for 4K epochs. The largest model (width 64) corresponds to standard ResNet18.

המאמר מגדר שלושה מצבים בהם תופעה זו יכולה להתרחש וראהם את זה על מגוון רחב של ארכיטקטורות, דатаה סטים, שיטת אימון ושיטות אוגמנטציה:

Model-wise double-descent .1

מודל יותר גדול מזיך לשגיאת טסט. הם מראים שיש כאשר מספר הפרמטרים במודל נמצא בתחום מסוים (אינטראול קרייטי) הגדלת מספר הפרמטרים גורם לעלייה בשגיאת הטסט, שמתחלפת בירידה כאשר מספר הפרמטרים משיג רף מסוים (יצא האינטראול הקרייטי). כמו כן כאשר בודקים את זהה שאר הפרמטרים של המודל נוטרים קבועים

2. אי מונוטוניות של השפעת גודל טרין סט.

יש אינטראול של גגלי טרין סט שבו הגדלתו גורמת לעלייה בשגיאת הטסט וכאשר עוברים אותו לשגיאת הטסט חוזרת לרדת שוב. במאמר מגדרים את מה שנראה סיבוכיות מודל אפקטיבית כמספר דוגמאות מקסימלי כאשר המודל מצליח להשיג שגיאת אימון קרובה לאפס (המאמר מגדר את הקרבה הזה בצורה מתמטית ריגורוזית). אצין ש- EMC כמובן תלוי במודל. אך האינטראול הקרייטי במקרה זה נמצא סיביב EMC

Epoch Number Double Descent .3

המשמעות כאן שקיים אינטראול בציר האפוקס שקיים בו תופעה דומה ואחר כך שגיאת טסט מתחילה לרדת שוב. דרך אגב אחת המשמעות של התופעה זהו כאן היא שאימון ממש ארוך עשוי עשו למונע אווורפייניג.

בנוסף הם מראים תופעה דומה גם לרמת הרעש הליבלים אולם הם מצינים שיש במקרים מסוימים ההתנגדות של שגיאת הטסט באינטראול קרייטי יכולה להיות שונה.

דатаה סטים: CIFAR-10, CIFAR-100, IWSLT'14 de-en

[lienק לקוד: code](#)[lienק למאמר: paper](#)

נ.ב. מאוד אהבתني את המאמר הזה, המסקנות שלו נראות מאוד מעניינות. עם זאת אני חשב שיש צורך לבדוק את המסקנות האלה על ארQUITקטורות רשת מורכבות יותר כמו כן על מגוון יותר רחב של דatasets. מומלץ!!

Review 5: Single Headed Attention RNN: Stop Thinking With Your Head

תחום מאמר: טרנספורמרים, multi-head attention

תקציר בשתי שורות: המאמר מצהיר שהוא מציע ארQUITקטורה פשוטה בהרבה ותופסת משמעותית פחות זיכרון מהטרנספורמר בעל ראשים רבים המהווה חלק מהותי (כמעט כל מה שיש שם) בBERT וצאצאיו.

תקציר מאמר: מכיוון שרובכם יודעים היטב מה זה טרנספורמר ו- Attention מודול בעל ראשים רבים, לא ארכחיב על זה כאן. מחבר המאמר מתרעם הרבה על כך שהטרנספורמר בעל ראשים רבים זה ארQUITקטורה מאוד כבדה, קשה לאימון ודורשת הרבה משאבי GPU. הוא מצין כדי לא ברור למה צריך מראשים רבים וטוען שאפשר להשיג תוצאות דומות גם עם ראש אחד בלבד עם כל מיני תוספות ארQUITקטוניות נחמדות. דרך אגב קיימות עבודות המציאות שיטות לניצול היטב יותר של הפלט של הראשים הרבים של הטרנספורמר. אז מה הוא בעצם מציע זה להחליף את הראשים הרבים של הטרנספורמר ע"י "שילוב של attention מודול מנון עם ראש אחד בלבד עם מה שנקרא AWD-LSTM", שהוא בעצם LSTM עם תוספת של כמה טרייקים נחמדים כמו DropConnect, Average SGD וכו' מושתנה של סדרת backprop בזמן ועוד כמה. הוא קורא לארQUITקטורה זו SHA-RNN

از מה שעושה מחבר המאמר הוא פשוט מוסיף לארQUITקטורה זו את מודול ה- attention מנון (תיכף אסביר מה מנון שם) עם ראש אחד ומודול שנקרא Boom. מודול ה- attention הינו מנון כי רק האינפוט q מוכפל במטריצה משקלים נלמדים כאשר האינפוטים key ו $value$ נכנסים כמו שהם ללא הכפלה במטריצה. עבור הארQUITקטורה זו q הינו הייצאה של LSTM אחריו שכבה נירמול (layer norm), כאשר k ו v הם היזכרון של התא mem (למייבז זכרוני הוא מסומן ב c בדרך כלל) ואוטו זכרון מועבר דרך LN (לא ברור לי מה הטעם להעיבר למודול זהה שני אינפוטים שהם שונים רק במשמעות ובסיקיל'). את הפלט מעבירים דרך הנקרא boom שזה

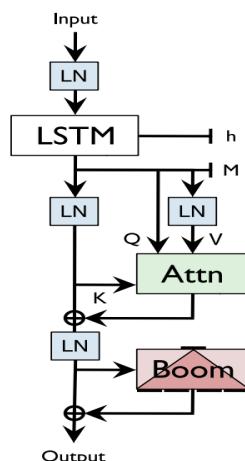


Figure 1. The SHA-RNN is composed of an RNN, pointer based attention, and a "Boom" feed-forward with a sprinkling of layer normalization. The persistent state is the RNN's hidden state h as well as the memory M concatenated from previous memories. Bake at 200°F for 16 to 20 hours in a desktop sized oven.

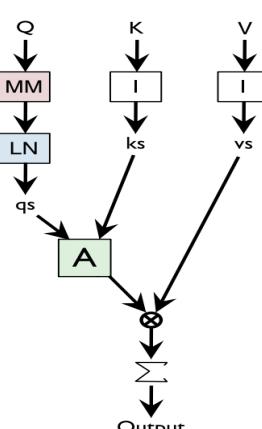


Figure 2. The attention mechanism within the SHA-RNN is highly computationally efficient. The only matrix multiplication acts on the query. The A block represents scaled dot product attention a vector-vector operation. The operators $\{qs, ks, vs\}$ are vector-vector multiplications and thus have minimal overhead. We use sigmoid to produce $\{qs, ks\}$. For vs see Section 6.4.

בעצם רשות זו שכבתית. בשכבה הראשונה מגדילים את המילד (מטריצה עם הרבה שורות), מעבירים דרך GELU, אז מצמצמים מילד עי' חלוקה של וקטור לכמה וקטורים קטנים וסכימתם (סוג של average pooling).
הישג מאמר: המחבר בחר להשוו את softmax זהה word per word מול מודלים שונים של הטרנספורמרים. הוא הצליח להראות שהוא מצליח להפיק את אותו softmax עם ארכיטקטורה פשוטה יותר. צריך לציין שכמות המשקלים בארכיטקטורה שלו עליה על זה המתחרים (בReLU אוטם ביצועים). דרך אגב אחד הוריאנטים של LSTM זה ארכיטקטורה עם 4 שכבות של LSTM כל אחד עם הראש שלו זהה רחוק מלהיות פשוט. בקיצור לא השתכנע.

данה Стим: enwik8, wikiText, wikiText103

נ.ב. המאמר לא הצליח להוכיח לי שהארכיטקטורה שהוא מציע עדיפה על הטרנספורמר בעל ראשים רבים. לא הוכיחו תוצאות על בנאים ידועים (סוגי משימות שונות). השילוב של LSTM עם ראש אחד של attention נחמדה אך התועלת לא ברורה. בקיצור המלצת קרייה - רק אם יש לכם הרבה זמן פנו.

לינק למאמר: [paper](#)

לינק לקוד: [code](#)

Review 6: A Metric Learning Reality Check

תחום: המאמר שיר לתחום של למידת מטריקה (Metric Learning) ובוחן התקדמות האחורנות בתחום זהה ב-5-4 השנים האחרונות.

מטרת המאמר: בchnerה של מגוון שיטות שהוצעו במאמרים שונים בתחום למידת מטריקה (או למידת הייצוג) על פרויויקט אחד (אותם ארכיטקטורות, אותם הייפר פרמטרים, אותו דאטא סט וכדומה).

סיכון מאמר בשורה: בעיות מהותיות עם שיטות ההשוואה הנוכחית בתחום למידת המטריקה

סיכום עיקרי המאמר: הטענה העיקרית במאמר שרוב התוצאות שהוצעו במאמרים שונים בתחום הושגו בצורה לא הוגנת. דוגמא בולטת לכך שהוא מביא זה השוואת של שיטות למידת מטריקה על ארכיטקטורות רשות שונות. הוא נותן דוגמא למאמר מפורסם ומוצטט רבות (לא נוקב בשמו כמובן) שימושה ב-ResNet50 בזמן שכל מתחמי משתמשים ב- Inception-BN . הטענה של המחבר במקורה זהה שהשיפור הזה הושג ברובו אם לא בכלל בغالל של ResNet50 יש ארכיטקטורה יותר מתקדמת שמסוגלת להוציא פיצרים יותר חזקים.

בסוף הוא טוען שהמטריקות שאיתן נמדדים הביצועים של שיטות שונות כמו $\text{Recall}@k$, מדע הדדי מנורמל (NMI) ו- Fscore אינם מטריקות מספק טובות לשערוך עד כמה יציג מפheid בין קטגוריות שונות ועד כמה הייצוגים של אותן קטגוריות קרובות (ראו תמונה 1 במאמר שמחישה את הדבר זהה)

איך המאמר מציע? בעצם 2 דברים:

1. לעורק השוואות של שיטות על אותה ארכיטקטורה של הרשת (Inception-BN) שאותן לפני על ImageNet , אותן אוגננטציות אותן שיטות אימון (RMSProp) לכל שיטת למידת המטריקה הנבחנת. התוצאה של כל שיטה מוצגת כממוצע של 10 ריצות עם ציון של רוח סמך (לא כל מאמר טורח לעשות זאת לא רציני לדעת).

2. להשתמש במטריקה הנקרה ($\text{MAP@R}(\text{mean average precision})$). מה זה בעצם? לכל יציג לוחים R יציגים הקורבים אליו ביותר. אז מחשבים את Precision@k $\text{Precision}@k$ לכל דוגמא השיכת לאוינו קלואס. בסוף MAP@R זה הסכום של התוצאות המוחלט ב-R. הם מראים ש MAP@R הינה מטריקה טובה יותר לאיפין מדויק של איות הקלאסטרים במרחב יציג (ראה טבלה 3 במאמר)

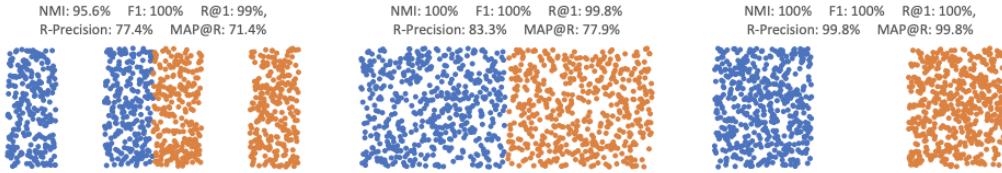


Fig. 1. How different accuracy metrics score on three toy examples.

מסקנות המאמר: המאמר משווה את השיטות שהוצעו ב 10 מאמרים שונים ל 3 דatasets סטימס טיפוסים של התחום ועובד כל אחד מהם מראה שאמם משווים לתופחים ומשתמשים בשיטת השוואה "טובה" כמו MAP@R אך ההתקדמות שהושגה הינה מזערית או לרוב בכלל לא קיימת. בעצם בכל 10 המאמרים לא השיגו כמעט שום שיפור יחסית ל contrastive loss **קלואסי** שהוצע לפני שנים.

dataset סטימס : CUB200 , Cars196 and Stanford Online Products

[lienck למאמר](#): [paper](#)

[lienck לקוד](#): [code](#)

נ.ב. מאמר מצין, כתוב מאד ברור, מסביר היטב את כל הטענות שלו. הרעיון נראה פשוט ונקי. רק קצת חבל שהרבה מהתקדמות בתחום למידת המטריקה בשנים האחרונות עלול להיות פיקציה. אולם אם יש לכם מאמרים דומים בתחום אחרים.

Review 7: PeerNets: Exploiting Peer Wisdom Against Adversarial Attacks

תחום מאמר: adversary training, graph attention network

תקציר מאמר בשתי שורות: המאמר מציע שיטה להטמודד עם תקיפות אדוורסריות באמצעות הוספת שכבות מנצלות את הדמיון בין הדוגמא הננתונה לבין התמונות האחרות בdataset סט. יצא בערך לפני שנתיים.

אינטרואיציה: קודם נזכיר מה זה התקפה אדוורסרית על רשת נירוניים מאומנת. המשמעות של התקיפה אדוורסרית היא יצירה של דוגמאות אדוורסריות. דוגמא אדוורסרית מתחילה מדוגמא רגילה x עם לייבל y . המטריה היא להוסיף פרטurbציה (רעש קטן) לתמונה וליצור תמונה \hat{x} אשר הרשת מזהה אותה עם לייבל שונה מ y בזמן שהעין האנושית בקהלות מסווגת את הדוגמא הזו עם הליבל המקורי. כמו שאמרתי המאמר מציע לנצל את הדמיון בין הדוגמא המסוגגת לתמונות אחרות בdataset סט שזה בעצם מקשה על יצירה דוגמא אדוורסרית כי עכשו המסוג ידע שאפיילה עם הרעש הקטן המוסף התמונה עדין "דומה" לתמונות אחרות בעליות אותו לייבל.

הרעיון: במאמר התמונה מוגדרת כמטריצה $d \times d$, כאשר d מספר הפיקסלים בתמונה ו d כמות הpixelsים פר פיקסל. אז לכל פיקסל בתמונה מחפשים את K (המבחרו $= 10$) פיקסלים הקרובים ביותר במנוחה מרחק קוסיני (cosine distance). החיפוש מתבצע בין כל (!!!) הפיקסלים של כל התמונות (הנקראות $peers$ תמונות peers במאמר). הבנייה הזו היא בעצם יצירתה של הגרף K -שכנים ברמת הפיקסל עבור הדטה סט. לאחר מכן מעבירים את הגרף הזו דרך graph attention network(GAT) כדי לקבל את ייצוג ארגטיבי התמונה ע"י כל ה $peers$.

בעצם לכל פיקסל בתמונה ולכל פיקסל בתמונה peer בgraf K-שכנים מחשבים attention score בין 0 ל 1. בדומה למה שעושים בשכבות attention קלאסיות המשמשים למשל למשימות סגמנטציה וגם לתרגומים אוטומטי. בשלב האחרון לכל פיקסל בתמונה סוכמים את כל scores עבור כל השכנים שלו. הם קוראים לשכבה הזו PR layer.

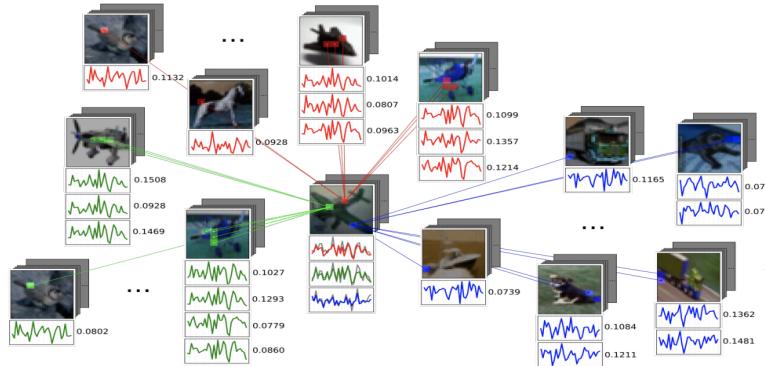


Figure 1: Our Peer Regularization illustrated on three pixels (red, green, blue) of a CIFAR image (center). For each pixel, K nearest neighbors are found in peer images. Plots represent the feature maps in the respective pixels; numbers represent the attention scores.

אימון: מכיוון שבנית גראף צזה לדאטה סט גדול זו משימה מאד כבדה מבחינה כמות החישובים באימון ה peers נבחרים מהתמונות במיניבאטץ'

אינפרנס: peers נבחרים קבוע של תמונות ולכל דוגמת טסט הגרף נבנה רק בן הדוגמא זו לסת זהה.

תוצאות: המאמר מוכיח כי עברו סוג תקיפות מגוונים:

Universal adversarial perturbations , Gradient descent attack, Fast Gradient Sign attack.
הוספה שכבת PR לרשת מגבירה את הרובוטיות של הרשת (fooling rate) לעוצמת פרטורה נטוונה מול שיטות הגנה אחרות.

דאטה סטם שנבחנו: MNIST, CIFAR10

מסקנה: השיטה נראה די מבטיחה אך לא ברור עד כמה היא מאריכה את זמן האימון. גם בחירה של גודל הבאטץ' לא נראה טרייזיאלי. אבל שווה לעקוב אחרי התפתחויות (

lien: [paper](#)
lien廉政: לא פורסם במאמר

Review 8: Adversarial Concurrent Training: Optimizing Robustness and Accuracy Trade-off of Deep Neural Networks

תחום: adversary training (אימון עם יריב או אימון לעומתי בעברית)

תקציר מאמר בשתי שורות : המאמר מציע שיטה הנקראת (ACT) adversary concurrent training (ACT) שבליבה אימון בו זמני של הרשת לדוגמאות הרגילות והשניה לדוגמאות האדרסריות (שזה הרשת הרובוטית נגד התקפות)

הסבר על תחום: המטרה האולטימטיבית של אימון עם יריב הינה להעניק לרשותות נוירונים רובוטיות נגד דוגמאות אדוורסריות (לא מצאתי תרגום יותר טוב - אשמה להצעות). הדוגמא אדוורסרית נוצרת (בהינתן רשות מאומנת) עי"ה הוספת רעש קטן לתמונה רגילה כדי לעוזת את הסיווגה עי"ה הרשת. אתם זוכרים את התמונה של הפנדת החמודה שמוסיפים לה קצת רעש (הען האנושית עדין מזהה של פנדה בקהלות) אבל הרשת מסוגת אותה כפרפר בהסתברות 0.95 בערך. אז בגישה של האימון עם היריב מנסים לחסל את הרשת נגד הדוגמאות האלה.

גישות קלואסית: הגישה הקלואסית לאימון עם יריב הינה לאמן רשות שתיתן פרדייקציות קרובות לדוגמאות אדוורסריות ולדוגמאות הרגילות שמננה הדוגמא אדוורסרית נוצרה בדרך כלל). הגישה הזאת פוגעת ביכולת הכללה של המודל כי פונקציית לוס לא ממצעת את הלוס על הדוגמאות הנקיות באופן ישיר. הגישה היותר מתקדמת זה לשלב את הלוס על הדוגמאות הנקיות עם loss adversarial שזה שני לוסים ניגודיים ולחוב זה עבד לא כל כך טוב.

תקציר המאמר: אז בשביל לנסות לשפר את ההיבטים הנ"ל המאמר מציע לאמן שתי רשותות : אחד לדוגמאות הרגילות והשנייה G רובוטית על הדוגמאות האדוורסריות. כל אחד מהlösions מורכב משני מחוברים: הראשון זה הלוס על דוגמא אדוורסרית (או נקייה בהתאם) והשני הוא "מרחב" KL בין הסיווגים של שתי הרשותות (KL הפור (inverse KL-

$$\mathcal{L}_G(\theta, \phi, \delta) = (1 - \alpha)\mathcal{L}_{CE}(G(x + \delta; \theta), y) + \alpha D_{KL}(F(x; \phi) || G(x + \delta; \theta))$$

$$\mathcal{L}_F(\theta, \phi, \delta) = (1 - \alpha)\mathcal{L}_{CE}(F(x; \phi), y) + \alpha D_{KL}(G(x + \delta; \theta) || F(x; \phi))$$

בנוסף בלוס של הרשת עם יריב מבוצע מיקסום על פני התוספת לדוגמא רגילה כדי ליצור דוגמא אדוורסרית "טובה" שהופך את הבעה ללוס הראשון לבעיית maximization.

$$\begin{cases} \min_{\theta} E_{(x,y) \in D} \max_{\delta \in S} \mathcal{L}_G(\theta, \phi, \delta) \\ \min_{\phi} E_{(x,y) \in D} \mathcal{L}_F(\theta, \phi, \delta) \end{cases}$$

בעצם הטענה במאמר שהרעיון הזה מאפשר אימון של רשות רובוטית נגד דוגמאות אדוורסריות עם פגיעה יותר קטנה ביכולת הכללה שלה.

шиפורים שהושגו: הם בודקים את הביצועים של הרשת המאמנת נגד דוגמאות אדוורסריות:

- הם משווים את הסטייה המינימלית הנדרשת בשביל לגרום לרשות לא לסואג נכון את הדוגמא
- ביצועים בהתקפות ידועות.

[lienק למאמר: Paper](#)

[lienק לקוד: לא מצאתי](#)

Review 9: Benchmarking Neural Network Training Algorithms

המאמר מציע שיטה למדידת ביצועים של אלגוריתמים לאימון רשותות נוירונים..

המאמר מזהה שלושה אתגרים עיקריים העומדים בפני השוואות של אלגוריתמי אימון

1. כיצד להחליט מתי האימון הושלם ולמדוד במדויק את זמן האימון
2. כיצד מתמודדים עם רגישות מדידות הביצועים לסוגים שונים וכמות שונה של DATA

3. כיצד להשוות באופן הוגן אלגוריתמים הדורשים אופטימיזציה של היפר-פרמטרים

כדי להתגבר על אתגרים אלו המאמר מציג במצמרך חדש הנקרא **AlgoPerf: Training Algorithms for the Comparison of Algorithmic Methods** להשוואת ביצועי אלגוריתמי אימון על חומרה קבועה עבור סוג דатаה שונים

Arxiv: <https://arxiv.org/abs/2305.20030>
<https://huggingface.co/papers/2306.07179>

Review 10: Meta-Learning with Implicit Gradients

תחום: meta deep learning

תקציר מאמר: המאמר המכיל את MAML - model-agnostic meta learning. השיטה המוצעת במאמר הנסקר נקראת באופן לא מפתיע MAML, כאשר האות הראשונה היא ממילה implicit. בגודל מאוד הרעיון ב-MAML המקורי זה לאמן רשות (חיצונית) לחישוב משקלים לרשות הפנימיות למגוון רחב של טאנסים, דומיניבים ארוכיטקטורות הרשות. הרשות מאומנת בשביל למצויר את הלס המוצע לרשות הפנימיות. הבעה העיקרית בגישה זו היא לבצע אופטימיזציה (גרדיינט דסצנט) על הרשות החיצונית כי בעצם בשביל לחישוב את הלס לכל טאנס בכל רשות חיצונית צריך לבצע כמה איטרציות של באקפروف. כמובן קשה מאוד לגלגלו את האיטרציות הללו לבאקפروف של הרשות החיצונית. אפשר לעשות קירוב מסדר ראשון אבל זה לא עובד כל כך טוב.

רעיון של מאמר: מה ש- *maml* מציעים זה בעצם שני דברים:

1. לאמן את הרשות החיצונית כך שהמשקלים שהוא מוציא יהו כמו שיוצר קרובים (מרחב ריבוע) ל"משקלים אופטימליים" של כל הרשותות הפנימיות. פשוט מוסיפים איבר רגולרייזציה שמודד את המרחק הזה.

2. המשקלים האופטימליים של כל רשות פנימית הן אלו המבאים למינימום את הלס (ראו תמונה המצורפת) עכשו זה נראה מההבט הראשון בלתי אפשרי לאמן דבר זהה כי לך תדע כמה איטרציות צריך לבצע בכל רשות פנימית וחישוב הגרדיינט מסתבר עוד יותר. וכך בא הטריק המתמטי האלגנטי שמכח שם מוסיפים את איבר רגולרייזציה ריבועי שmbטל את הצורך לחשב אותו מפורשות (מכאן הimplicit).

יש ביטוי סגור לגרדיינט זהה.

2.2 Proximal Regularization in the Inner Level

To have sufficient learning in the inner level while also avoiding over-fitting, $\mathcal{A}lg$ needs to incorporate some form of regularization. Since MAML uses a small number of gradient steps, this corresponds to early stopping and can be interpreted as a form of regularization and Bayesian prior [20]. In cases like ill-conditioned optimization landscapes and medium-shot learning, we may want to take many gradient steps, which poses two challenges for MAML. First, we need to store and differentiate through the long optimization path of $\mathcal{A}lg$, which imposes a considerable computation and memory burden. Second, the dependence of the model-parameters $\{\phi_i\}$ on the meta-parameters (θ) shrinks and vanishes as the number of gradient steps in $\mathcal{A}lg$ grows, making meta-learning difficult. To overcome these limitations, we consider a more explicitly regularized algorithm:

$$\mathcal{A}lg^*(\theta, \mathcal{D}_i^{tr}) = \underset{\phi' \in \Phi}{\operatorname{argmin}} \mathcal{L}(\phi', \mathcal{D}_i^{tr}) + \frac{\lambda}{2} \|\phi' - \theta\|^2. \quad (3)$$

The proximal regularization term in Eq. 3 encourages ϕ_i to remain close to θ , thereby retaining a strong dependence throughout. The regularization strength (λ) plays a role similar to the learning rate (α) in MAML, controlling the strength of the prior (θ) relative to the data (\mathcal{D}_i^{tr}). Like α , the regularization strength λ may also be learned. Furthermore, both α and λ can be scalars, vectors, or full matrices. For simplicity, we treat λ as a scalar hyperparameter. In Eq. 3, we use $*$ to denote that the optimization problem is solved exactly. In practice, we use iterative algorithms (denoted by $\mathcal{A}lg$) for finite iterations, which return approximate minimizers. We explicitly consider the discrepancy between approximate and exact solutions in our analysis.

יש עוד לא מעט טריקים מתמטיים במאמר זהה שבעזרתו הם מציעים אלגוריתם בר מימוש אחד מהם זה חישוב היפוך של מטריצות מאד גדולות בעזרת conjugate gradient

הם מראים תוצאות לא רעות דרך אגב.

[לינק למאמר: paper](#)

[בלוג המסביר את המאמר: blog](#)

[הרצאה מצוינת של יענק: youtube explanation](#)

Review 11: A causal view of compositional zero-shot recognition

פינט הסוקר:

המלצת קריאה ממיק: מומלץ בחום לבורי ידע בתחוםים רלוונטיים.

בahirot כתיבה: גבוהה.

רמת היכרות עם מילים מתמטיים וטכניקות של DL/ML הנדרשים להבנת מאמר: נחוץ רקע טוב בהסתברות והבנה בסיסית של עקרונות הסיבתיות.

ישומים פרקטיים אפשריים: אפשר להשתמש בReLU זה בשביל לבנות מודל לייצרת דוגמאות (נגיד, תמונות) המכילות שילובים של אובייקטים שלא מופיעים בסט האימון.

פרטי מאמר:

[לינק למאמר: זמן להורדה.](#)

[לינק לקוד: זמן CAN](#)

פורסם בתאריך: 01.11.2020, בארכיב.

הציג בכנס: NeurIPS 2020

תחומי מאמר:

- **למידת ZS zero-shot.**
- **הכללה הרכבתית (compositional generalization).** – יכולה לזהות שילובים חדשים (שלא נראו יחד קודם) של מרכיבים (פייצ'רים) ידועים.

מילים מתמטיים, מושגים וסימונים:

- **הסקה סיבטיבית:** גרפ סיבתיות, פיצ'רים מעורבים (confounding), התערבות (intervention) לפיצ'רים.
- **למידת יציגי דатаה מופרדים (disentangled representations).**

- קרייטריון מידע של הילברט-شمידט (HSIC): כל שערוך של מידת אי תלות בין שני מדגמים של משתנים אקראיים.
- שערוך פריקות של ייצוגי DATA לא מתואג (PIDA).

תמצית מאמר:

אחד האתגרים המשמעותיים בלמידה-zero-shot זו הקניית יכולת הכללה הרכבתית למודל ZS. במילים אחרות אנו רוצים "ללמד" את המודל לזהות קומבינציות חדשות (!!) של מרכיבי DATA בסיסיים שהוא הצליח לזהות בסע אימון (בעיקרון הכללה הרכבתית הינה מקרה פרטי של למידת ZS). בואו נתחילה מדוגמה של יכולת הכללה הרכבתית בדומין הייזאלי. נניח שאתם מעולם לא ראתם זאים לבנים אך ברגע שתראו אחד, אתם בקלוות תצליחו לזהות אותו כ "זאב לבן" בגלל שאתם יודעים איך נראה זאב וגם אתם יודעים לזהות צבע לבן. זאת אומרת בזיכרון של בני אדם האובייקט "זאב" והתמונה (אטריבוט) "לבן" נשמרים בצורה נפרדת וכל לנו לשלב אותם גם אם הם מעולם לא ראו את השילוב שלהם (!!). לעתנו המודלים שמאמנים בצורה דיסקרימינטיבית מתקשים להפgin יכולת זו ויש שתי סיבות עיקריות לכך:

1. **שינוי בתפלוגות** בין סט אימון לטסט סט: המודל "לא ראה" את השילובים מהטסט סט במשר האימון. זה גרם לכך המודל למד קשרים בין פיצרים שמספריים לו להרכיב אותם בצורה נכונה כאשר מרכיבים אותם על הטסט סט. למשל המודל שראה רק זאים אמורים למד שיש קשר בין התמונה "אפור" לאובייקט "זאב" ועקב לכך יתקשה לזהות זאים בצעדים אחרים.
2. **LIBELIM** מעורבים בסט אימון: המודל יתקשה "לפרק" אותם למרכיבים הבסיסיים שלהם בהתבסס רק על הליבלים. למשל אם הליבל של תמונה הוא "זאב אפור", המודל המאומן בצורה דיסקרימינטיבית נראה לא "שכיל להבין" אילו פיצרים ויזואליים חשובים לזיהוי אובייקט "זאב" ואילו מגדרים את התמונה "אפור"

המאמר מנסה להציג על קשה אלוי" הצעת מודל גנרטיבי W כאשר הקלט למודל הינו שילוב של אופיינים (LIBELIM) של תמונה. למשל, כדי לגנרט תמונה של זאב לבן אנו נבחר את סוג האובייקט (זאב) ואת האטריבוט (לבן) וניצר תמונה בהתבסס על אופיינים אלו. היתרון בכך זה הוא שההתפלוגות המותנית של תמונה, בשילובים של אופיינים אלו יהיה זהה בין סט האימון לטסט סט (!!).

פינת האינטואיציה: [scroll_highlight] שילוב של סוג אובייקט ואטריבוט של תמונה נתה ליצור תמונות דומות גם בסט אימון וגם בטסט סט [scroll_highlight] להבדיל מהתפלוגות התמונות מותנות רק בסוג אובייקט או באטריבוט בלבד. זה ההנחה המהותית שעליה מבוסס המאמר (!!).

אתם יכולים לשאול מה למודל הגנרטיבי זהה ולמשמעות למידת ZS שהמאמר מנסה לפתרו? התשובה הינה מאוד אינטואטיבית - "מאמנים" את המודל הגנרטיבי בתהליך הלמידה, כאשר בזמן ההסקה (אינפרנס) על תמונה X (המיוצגת ע"י) וקטור של פיצרים של X, אנו נבחר את שילוב האופיינים (o, a) המקסם את ההסתברות המותנית של (o, a) | X .P.

עד כאן הכל טוב ויפה אבל איך מבצעות הלמידה וההסקה (בסוגן ZS) המתבססות על הנחות אלו בפועל? למטרה זו המאמר בונה גרפ סיבתיות G המתאר את תהליך יצירת תמונות "אמיות". G ניתן לתיאור באופן הבא:

1. בוחרים זוג של סוג אובייקט o ואטריבוט a מרחב האובייקטים o_S ובמרחב האטריבוטים a_S בהתאם. שמו לב ש- o - a הינם **תלויים** (!!) זה זהה (confounding). תלות זו הינה המכשול המרכזי בהקניית יכולת של הכללה הרכבתית למודלים דיסקרימינטיביים בנסיבות למידה ZS. האובייקטים

והאטריובוטים ממודלים עי"י" משתנים קטגוריאליים (ניתן לחשב על S_f ו

- a_f

 בטור מיליון של סוג אובייקטים ושל אטריבוטים בהתאם).

2. אובייקט o ואטריבוט a יוצרים פיצ'רי הליבה o_f ו- a_f . כמו שכבר אמרנו הנחת היסוד של המאמר אומרת שהתפלגיות של o_f ו- a_f אין משתנות בין סט האימון לסט טט.
3. פיצ'רי הליבה o_f ו- a_f יוצרים וקטור פיצ'רים ושל תמונה (כלומר תמונה עצמה).

אבל איך גורף הסביבתיות המתואר קשור לבועית למידה Z_f , אתם שואלים? למעשה אנו צריכים למצאו דרך למDSL שלילבים בטסט סט שלא ראיינו בסט האימון עי"י" שינוי של G . המאמר מציע לבצע את מה שנ Kraa בטורות ה"התערבות" (intervention) ל- G . אנו נאלץ את a ואת o לקבל ערכים ספציפיים ובכך "נקרע" את התלות ביניהם". לאור זה הבועיה של Z_f שהמאמר פותר ניתנת לניסוח הבא: [scroll_highlight] מיציאת התערבות לסוג אובייקט [scroll_highlight] אטריבוט שיצרה תמונה נתונה בסביבות הגבואה ביותר. [/]

הסבר של רעיונות בסיסיים: אחרי שהבנו את העקרונות הבסיסיים של המאמר, הגיע הזמן לדבר על דרך מימוש של הגישה זו. המטרה שלנו עברו תמונה נתונה מטסט סט הינה למצוא את הזוג של אובייקט o ושל אטריבוט a , המקסם את ההסתברות המותנית של תמונה $\text{z} | \text{o}, \text{a}$.

הגדרות: כדי לפתור בעיה זו המאמר מגדר שני מרחבים לטנטים o_f ו- a_f המכילים ייצוגים לטנטים של אובייקטים ואטריבוטים בהתאם. אובייקט o יוצר התפלגות מותנית ($\text{o}|_f$) המודל עי"י" גאוסיאן עם המרכז (וקטור התוחלת) $(\text{o}|_f)_h$ ומטריצת קווריאנס אלכסונית. ניתן לפרש את $\text{o}|_f_h$ בתור יציג אבטיפוס (פרוטוטיפ) של אובייקט o . יציג לטנטי של אטריבוט a , המסומן a_f , מוגדרים באופן דומה. נציין שהמאמר מניח שהתפלגות $(\text{a}|_f)_k$ ו- $(\text{o}|_f)_k$ הינם זהות בין סט האימון לסט טט.

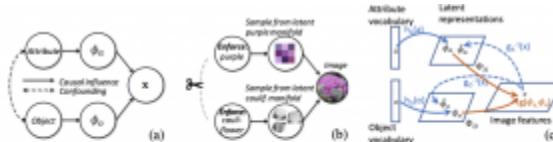


Figure 1: (a) The causal graph that generates an-image. The solid arrows represent the real-world processes by which the two categorical variables "Object" and "Attribute" each generate "core features" [21, 17] ϕ_o and ϕ_a . The core features then jointly generate an image feature vector x . The core features are assumed to be stable for unseen combinations of objects and attributes. The dotted double-edged arrows between the Object and Attribute nodes indicates that there is a process "confounding" the two: they are not independent of each other. (b) An intervention that generates a test image of a purple-cauliflower, by enforcing $\text{o} = \text{purple}$ and $\text{o} = \text{cauliflower}$. It cuts the confounding link between the two nodes [49] and changes the joint distribution of the nodes to the "interventional distribution". (c) Illustration of the learned mappings, detailed in Section 4

וקטור פיצ'רים של תמונה x מוגדר כגאוסי עם וקטור תוחלת $(\text{o}|_f)_g$ ומטריצת קווריאנס אלכסונית קבועה גם כן. כרגע בתחום האימון של מודלים גנרטיביים אנו צריכים גם למדל את התפלגות האפואוטרורית של וקטורי יציג לטנטים של o_f ו- a_f (בהינתן וקטור פיצ'רים של תמונה x). מודלים אלו יסומנים עי"י $\text{o}_i|_g$ ו- $\text{a}_i|_g$ בהתאם.

לאחר שסיימנו עם ההגדרות, נוכל לעבור לתיאור של תהליכי הלמידה. המטרה של תהליכי הלמידה הינה לאמן רשתות (כולן מסוג MLP) שהן $\text{o}_i|_g, \text{g}, \text{g}_i|_a, \text{h}_i|_a, \text{h}_i|_o, \text{g}_i|_o$. פונקציה הלווא L מורכבת מ- 3 חלקים:

1. לוא על נראית הדאטה like L: עבור תמונה בסט אימון מתייגת עם סוג אובייקט o ואטריבוט a בונים לווא המורכב מ 3 מחוברים:

. איבר שמודא שהשעורן של היציג הלטנטי של סוג אובייקט o הניתן עי"י הרשות $(\text{o}|_g)_g$ מקרוב בצוואה טובא את היציג פרוטוטיפ o_f של o . הקבוצה נمدדת כאן כהפרש ריבועי בין o_f לבין $\text{o}|_g$.

ii. איבר המשערק את המרחק הריבועי בין $(x)_{\text{ao}}^g$ לבין הפרוטוטיפ שלו a_h .
 iii. טריפלט לוע כאשר העוגן (anchor) הינו וקטור פיצ'רים של התמונה a , הדוגמא החיויבות זה הזוג (o, a) האמתי של התמונה (התיג), והדוגמא השילית זה זוג של אובייקט ואטריבוט אקראיים. פונקציית המרחק כאן הינה המרחק האוקלידי הריבועי בין x ל- $(o, a)^g$. מכך שהמטרה של טריפלט לוע הינה מינימיזציה של מרחק בין העוגן לדוגמא החיויבות ומקסום המרחק בין העוגן לדוגמא השילית. במקרה שלנו אנו רוצים ליצור תמונה בעלת פיצ'רים קרובים ל a בהינתן סוג האובייקט והאטריבוט שלו ולמקסם מרחק בין a לפיצ'רים של תמונה הנוצרת ע"ז זוג של אובייקט/אטריבוט אקראי.

2. חלק 2 של הלוס decompose : מנסה לieżור את התלות המותנית בין פיצ'רי ליבה a_f ו- o_f בהינתן סוג האובייקט/אטריבוט. למשל, הגרף הסיבתי בציור 1 מכתיב את אי התלות בין פיצ'ר ליבה o_f לאטריבוט a בהינתן האובייקט הנבחר o . ד"א המאמר מציין שאית תלות זו קשורה למטריקה המודדת את מידת הפריקות (disentanglement) של ייצוגו דאטה לא מתויגת ([PIDA](#)). בנוסף a_f צריך להיות בלתי תלוי ב o_f גם בהינתן האובייקט הנבחר o , ובנוסף אותה אי תלות צריכה להתקיים בהינתן אטריבוט o . מכיוון שאנו לא יכולים לדגום את המרכיבים הלטנטיים o_F ו- a_F , אנו מנסים לכפות את האית תלות המותנית אלו בין השעורכים אפואטריאוריים שלהם הניתנים ע"ז $(x)_{\text{ao}}^g$ ו- $(x)_{\text{oc}}^g$. אבל איך בונים לוע המציג את תלות סטטיסטית בין מדגמים של וקטורים אקראיים? כמובן, קורלציה פשוטה בין הוקטוריות המבוססות מספקת כאן כי היא מודדת רק את התלות הלינארית בין הוקטורים. קיימות שיטות פרמטריות המבוססות על המידע הדדי, ש שיטות המבוססות על אימון אדוורסרי, אבל המאמר בחר בשיטה לא פרמטרית הנקראית קרייטריון המודיע על הילברט-شمידט (HSIC). בלי' להיכנס יותר מדי לפרטים המתמטיים (HSIC זה ייצור די מורכב) ניתן לחשב על קרייטריון זה כהכללה מסוימת של קורלציה בין וקטורים כאשר הוקטורים עוברים איזושה טרנספורמציה לא לינארית (קרנל). אצ"י ש- decompose מורכב מ- 4 ביטויי HSIC (אנו רוצים לכפות אי תלות מותנית בין 4 זוגות של פיצ'רי ליבה, אובייקטיים ואטריבוטים (חלק מהם פורטו בתחילת הסעיף).

3. חלק 3 של הלוס invert : מנסה לאלץ את אמבידיגס o_h , a_h והווקטור פיצ'רים של תמונה $(o, a, h)^g$ להכיל כמה שיותר אינפורמציה על הליבלים האמתי של תמונה, a ו- o . אם זה לא יעשה a_h ו- o_h עלולים להתכנס לפתורנות טריוויאליים כי אין לנו גישה לערכים אמיתיים של הפיצ'רים הלטנטיים a_f ו- o_f (ראה את ההסבר על הלוס הראשון [like](#)). אך עושים את הדבר הבא:

- מוסףים שכבת לינארית a_h ו- o_h לשיווג של אטריבוט וסוג אובייקט בהתאם (כל אחד מקבל שכבה לינארית משלה ומאונן בנפרד) ומאמנים כל אחד מהם עם קרוס-אנטרכופי לוע (שני לואים).
- מוסףים שכבת לינארית לרשות הייצוג ו לשיווג של סוג אובייקט ושכבה לינארית לשיווג של אטריבוט ומאמנים אותם עם אותו קרוס אנטרכופי לוע (שני לואים).
- הלוס invert מורכב מסכם של 4 הלוסים המתוארים בסעיפים הקודמים.

הדבר האחרון שנזכיר לנו לדון כאן זה האופן שבו מתבצעת ההסקה (אינפרנס).

AIR UPSIM ANIPRNS: כמו שכבר אמרנו אנו מנסים למצוא זוג של (o, a) המ מקסם את את ההסתברות של תמונה נתונה a . המאמר מראה כי $(o, a)^g \log$ - ניתן לקרב על סכום של 3 האיברים הבאים:

i. מרחק רביעי בין $(x)_{\text{ao}}^g$ לפרוטוטיפ a_h של a (כל הרשותות כאן אומנו בשלב הלמידה). מרחק זה מבטא "עד כמה התמונה מכילה אטריבוט a המשוערך ע"ז" קרבתו של שעורך פיצ'ר ליבה a_f של x המשוערך ע"ז $(x)_{\text{ao}}^g$.
 ii. מרחק רביעי בין $(x)_{\text{oc}}^g$ לפרוטוטיפ o_h של o .

iii. המרחק הריבועי בין (o, h_o) לבין התמונה x המבטא עד כמה מדויק ניתן לשחזר תמונה x מהזאג של (o, a)

בסוף בוחרים זוג (o, a) הממקסם את $\log p(x|o, a)$.

הישג מאמץ: המאמר מראה שיפור בביצועים על משימות ZS על דאטה סטם MIT states ו-UTZappos50K - והדעתהס הסינטטי AO-CLEVR Mol כמה שיטות ZS כמו VisProd, ATTOP, TMN.

	UNSEEN	SEEN	HARMONIC	CLOSED	AUSUC
WITH PRIOR EMBEDDINGS					
LE	10.7 ± 0.8	52.9 ± 1.3	17.8 ± 1.1	55.1 ± 2.3	19.4 ± 0.3
ATTOP	22.4 ± 2.9	35.2 ± 2.7	26.5 ± 1.4	52.2 ± 1.8	20.3 ± 1.8
TMN	9.7 ± 0.6	51.9 ± 2.4	16.4 ± 1.0	68.9 ± 1.1	24.6 ± 0.8
NO PRIOR EMBEDDINGS					
LE*	15.6 ± 0.6	52.0 ± 1.0	24.0 ± 0.7	58.3 ± 1.2	22.6 ± 0.9
ATTOP*	16.5 ± 1.5	15.8 ± 1.9	15.8 ± 1.4	42.3 ± 1.5	16.7 ± 1.3
TMN*	6.3 ± 1.4	55.3 ± 1.6	11.1 ± 2.3	58.4 ± 1.5	24.5 ± 0.8
CAUSAL					
$\lambda_{\text{Adversarial}}$	22.5 ± 2.0	45.5 ± 3.7	29.4 ± 1.5	55.3 ± 1.1	22.2 ± 0.9
CAUSAL	26.6 ± 1.6	39.7 ± 2.2	31.8 ± 1.7	55.4 ± 0.8	23.3 ± 0.3

Table 1: Results for Zappos. ± denotes the Standard Error of the Mean (S.E.M.) over 5 random model initializations.

ג.ב. זהו מאמר מאד מעוניין המציע שיטה של למידת ZS הנוטנת מענה לקשיים שחווים מודלים דסקרייפטיביים בזיהוי שילובים חדשים (לא מופיעים בסט אימון) של אופיינים בטסט סט. המאמר מציע מסגרת סיביתית בשבי להתגבר על הקושי הזה ומצליח להציג שיפור ניכר בביצועים על משימות ZS על 3 דatasets. המאמר משתמש בכלים מתמטיים די כבדים אך כתוב בצורה מאוד הוננת ל羣ור להבין בקלות את הרעיון העיקרי. בקיצור המלצת קריאה ממנה!

Review 12: Alias-Free Generative Adversarial Networks

פינת הסוקר:

המלצת קריאה ממיק: חובה לעוסקים במודלים גנרטיביים של הראייה הממוחשבת, לכל האחרים מומלץ מאוד.

בהירות כתיבה: גבואה מינוס.

רמת היכרות עם כלים מתמטיים וטכניקות של DL/ML הנדרשים להבנת מאמרה: היכרות עם עקרונות של GAN-ים, הבנה של טכניקות דגימה (downsampling, upsampling) ושהזור אותן רציף מדגימות (משפט דגימה של ניוקויסט, נסחת שנון-ו-ויטק).

ישומים פרקטיים אפשריים: יצרה של תמונות invariant להזזה ולסיבוב ממוחב לטנטי של GAN.

פרטי מאמר:

[lienק למאמר: זמן להורדה.](#)

[lienק לקוד: הגיט](#) אומר שיצא בספטמבר.

פורסם בתאריך: 23.06.21, בארכיב.

הוגג בפנים: טרם ידוע.

תחומי מאמר:

- גאנים
- מניעת פיקסלים "קפואים" (דבוקים) למקום בתמונות מגונרטות.
- הקטנה של aliasing בתמונות המגונרטות באמצעות גאנים.

כליים מתמטיים, מושגים וסימונים:

- StyleGAN2
- Translation/rotation equivariance
- התמרת פורייה (Fourier transform)
- Aliasing
- נוסחת אינטרופולציה של Whittaker–Shannon
- מסננים לשחזר אות רציף מדגימות (hcjinc, sinc, מסנן קייזר)

מבוא:

בשנים האחרונות איכות ורזולוציה של תמונות, הנוצרות באמצעות N-GAN-ים השתפרו משמעותית. ארכיטקטורות גאנים שונות הצלימו ליצור תמונות באיכות מדיה גבוהה ובועלות רזולוציה גבוהה עבור מגוון שימושות של הראייה הממוחשבת בדומיננס רבים כגון:

- יצרה של תמונות פנים ותמונות פוטוריאליסטיות אחרות.
- יצרת דמויות מציאות (animation).
- "העתקה תמונה" לדומין אחר (כמו יצרת תמונה מסקיצה, שינוי סגנון תמונה, שינוי של דמויות בתמונה וכדומה).
- יצרה תמונה מתיאור מילולי.

בנוסף הוצעו ארכיטקטורות כמו StyleGAN2 המאפשרות ליצור פיסות דאטה ויזואלי בעלות פיצ'רים ויזואליים נתונים (disentangled) כגון גיל, צבע שיער, צורה של גבורה וכדומה. למרות כל ההצלחות המרשימות הללו נותרו מספר שאלות בנוגע למקור יצרת תמונות באמצעות רשתות נירונים.

המאמר מציין כי פיצ'רים בעלי סקלולים (scales) שונות בתמונות טבעיות הן בעלי מבנה היררכי מובהק. למשל הזזה של ראש בתמונה אמרה לגרום לשער לחוז בצורה דומה. לכורה נראה כי מנגנון של יצרת תמונות בגאנים אמר לבנות תמונות עם פיצ'רים בעלי מבנה היררכי דומה. למשל רשות הגונרטור של גאן (כגון StyleGAN) מתחילה מיצרת תמונה ברזולוציה נמוכה ואז מבצעת פעולה sampling כדי ליצור תמונות ברזולוציה גבוהה יותר.

תיאור הבעיה:

המאמר הנסקר טוען כי למראות הדמיון לעיל (בין תהליכי ייצור תמונות) הפיצרים הגסים בתמונות, הנוצרות באמצעותGANים, שולטים רק ב"נכחות" (נראות) של הפיצרים העדינים **ולא במיקום שלהם**. אי קוהרנטיות זו בא לידי ביטוי כאשר מזיזים או מסובבים פרט גדול בתמונה הנוצרת באמצעות גן (באמצעות שינוי של הייצוג הלטני). המחברים מראים כי במקרים רבים ניתן לראות פרטים עדינים (המהווים חלק של הפרט הגדל) של התמונה **ש קופאים באוטו מקום** בתמונה **במקום לוז/l הסתווב יחד עם הפרט הגדל**. המאמר מכיל מספר דוגמאות לתופעה המתוארת לעיל: כמו פרווה סביב העין של חתול נשארת במקום כאשר מזיזים את העין, השער לא זו כאשר משנה את תנוחת הראש **ודוגמאות רבות אחרות לבן**, נציין, כי קיומם פיקסלים קופאים/דבקים כאלו מעיד על הדר equivariance לפעולות הזזה וסיבוב של הגנרטור.



Figure 1: Examples of "texture sticking". **Left:** The average of images generated from a small neighborhood around a central latent (top row). The intended result is uniformly blurry because all details should move together. However, with StyleGAN2 many details (e.g., fur) stick to the same pixel coordinates, showing unwanted sharpness. **Right:** From a latent space interpolation (top row), we extract a short vertical segment of pixels from each generated image and stack them horizontally (bottom). The desired result is hairs moving in animation, creating a time-varying field. With StyleGAN2 the hairs mostly stick to the same coordinates, creating horizontal streaks instead.

תמצית מאמר:

המאמר מראה כי מניעת התקפלות תדרים (aliasing) מקלת את בעיית equivariance לשיבוב של תמונות הנוצרות ע"י הגנרטור. עבדות קודמות מצינוות כי התקפלות תדרים בתמונות, הנוצרות באמצעות רשתות נירונים ובפרט ע"יGANים, היא תופעה הנגרמת מפעולות לא-לינאריות ופעולות downsampling לא מדויקות כמו pooling או strided convolution. התקפלות תדרים מייצרות תדרים מעבר לתדר Nyquist (Nyquist) /מחצית תדר הדגימה של התמונה (הנגזר מהרצוליזציה שלה). אולם תדרים שאינם מפולטים מתקפלים לתדרים הנראים "מתחזים" לתדרים אמיתיים אף שאינם קיימים במקור. כתוצאה לכך השכבות הבאות של הרשת עלולות "למודד פיצרי" שווא"א המסתמכות על הארטיפקטים הנוצרים עקב התקפלות תדרים (ראה [An Effective Anti-Aliasing Approach for Residual Networks](#)).

המחברים מציעים להשתמש במסננים מעיבוד אוטומת למניעת התקפלות ומראים כי מסננים אלו מצליכים לגרום לתמונות המוגנרטות באמצעות הגנרטור להיות הזזה_equivariant לשיבוב. נציין כי כדי לגרום לתמונה להיות equivariant לשיבוב המאמר משתמש בסנן שהוא radial-symmetric (radial-symmetric) בעל תגובה תדר בצורת דיסק.

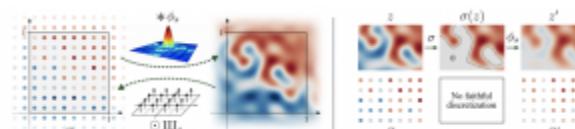


Figure 2: **Left:** Discrete representation Z and continuous representation z are related to each other via convolution with ideal interpolation filter ϕ_z and pointwise multiplication with Dirac comb III_z . **Right:** Nonlinearity σ , ReLU in this example, may produce arbitrarily high frequencies in the continuous-domain $\sigma(z)$. Low-pass filtering via ϕ_z is necessary to ensure that \hat{Z}' captures the result.

תקציר מאמר:

המאמר מציין שתי סיבות לתופעת התקפלות תדרים המתוארת בפסקה הקודמת:

1. שימוש במסננים (פילטרים) כגון בילינארי או strided convolution במהלך ייצור תמונה.
2. שימוש בפונקציות אקטיבציה לא לינאריות הפעלים על כל פיצ'ר בנפרד.

המאמר הנסקר מציע לנצל שיטות anti-aliasing קלאסיות מתחום עיבוד אותות להתקפלות תדרים בתמונות. למעשה המחברים מתייחסים לתמונה כאל דגימה של אות דו-מימדי רציף. אותן רציף זה הוא בעל רוחב פס סופי (bandlimited) לאחר והוא צריך להיות מוצג בצורה נאמנה באמצעות דגימה בגריד (grid) של פיקסלים. כתבי המאמר טוענים כי שימוש בטכניות anti-aliasing במהלך ייצור של תמונה ע"י הGENERATOR מצליח להקטין את חוסר equivariance בתמונה הנוצרת באופן משמעותי. המחברים טוענים כי טכניקות אלו מאפשרות למנוע מפיצרים ויזואליים עדינים של התמונה הנוצרת להיות "דבוקים" למיקומים קבועים בתמונה ובכך לנפטר בעית הפיקסלים השורפים.

כאמור המאמר מזהה שתי סיבות להתקפלות תדרים שמופיעות בתמונות שהGENERATOR יוצר: שימוש במסננים לא מדויקים ופונקציות אקטיבציה לא לינאריות המופעלות ברמה של פיצ'ר, שעולמים ליצור תדרים "גבויים מידי". המחברים מציעים לשנות את הארכיטקטורה של הGENERATOR (הDISCRIMINATOR נותר ללא שינוי) באופן הבא:

- החלפת קונבולוציות 3×3 ב-StyleGAN2 המקורי בקונבולוציות 1×1 סימטריות שבאופן די ברור-equivariant לשיבוב (ນציגן כי קונבולוציות 3×3 הן equivariant להזזה אך לא לשיבוב).
- הוספה של מסנן upsampling בפקטור m (הכנסת אפסים בין הדגימות) לפני כל אקטיבציה לא לינארית downsampling (ולאחריה מסנן downsampling באוטו פיקטור m בכל שכבה של GENERATOR). מכיוון שככל שכבה של GENERATOR מבצעת upsampling של תמונה (הגדלת רזולוציה פי שתיים) לפני הפעלת האקטיבציה, ניתן לאחד אותו עם ה-downsampling בפקטור m הנדרש עבור "טיפול בפונקציית אקטיבציה" ולבצע upsampling בפקטור $2m$. משנית המאמר משתמש ב- 2×2 מסנן downsampling וה- 2×2 מסנן downsampling הנבחר הוא מסנן קייר עם המותאם כי להיות רדייאלי-סימטרי.

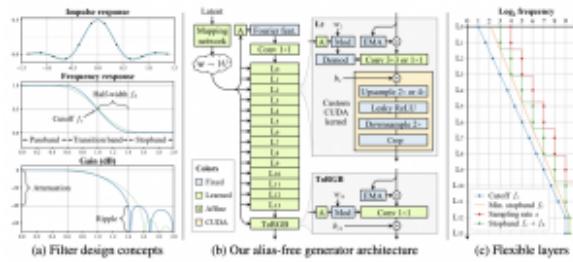


Figure 4: (a) 1D example of a $2 \times$ upsampling filter with $n = 6$, $s = 2$, $f_c = 1$, and $f_h = 0.4$ (blue). Setting $f_h = 0.6$ makes the transition band wider (green), which reduces the unwanted stopband ripple and thus leads to stronger attenuation. (b) Our alias-free generator, corresponding to configs T and R in Figure 3. The main datapath consists of Fourier features and normalization (Section 3.1), modulated convolutions [33], and filtered nonlinearities (Section 3.2). (c) Flexible layer specifications (config T) with $N = 14$ and $s_N = 1024$. Cutoff f_c (blue) and minimum acceptable stopband frequency f_t (orange) obey geometric progression over the layers; sampling rate s (red) and actual stopband $f_c + f_h$ (green) are computed according to our design constraints.

איך מודדים equivariance להזזה ולשיבוב:

כדי לשערק את מידת-equivariance של התמונה \mathbf{X} , הנוצרת באמצעות מוקטור לטוני \mathbf{w} , להזזה/шибוב, יש להבין איזו טרנספורמציה צריך לעשות ל- \mathbf{w} , כדי להזיז/לשובי את התמונה בהיסט/זווית נתונה \mathbf{t} . חיפוש אחריו טרנספורמציה כזו עבור ארכיטקטורה הסטנדרטית של StyleGAN2 הוא די מרכיב. כדי להתמודד עם סוגיה זו, המחברים מציעים להחלף את הקטלוק קבוע לרשת-h-synthesis [בפיצ'ר פוריה](#). נזכיר כי רשת-h-synthesis בונה את התמונה משני קלטיים:

- וקטור הסגן \mathbf{w} שנבנה מוקטור לטנסי \mathbf{z} מהתפלגות גאוסית באמצעות העברתו של \mathbf{z} דרך רשת מייפוי (mapping network). תת-וקטורים של \mathbf{w} "모자קיטים" לשכבות שונות של רשת ה-synthesis ליצירת פיצ'רים בסקלות שונות.
- וקטור דטרמיניסטי \mathbf{w} .

از כדי להקל על חיפוש טרנספורמציה של \mathbf{w} שתגרום היזה/סיבוב של תמונה בהיסט/זווית נתונה t , המחברים מציעים להחליף את \mathbf{w} בפיצ'רי פורה. התדרים של פיצ'רי פורה אלו נדגים (פעם אחת ונונרים קבועים בהמשך) מהתפלגות איחוד מהפס התדרים המתאים לתמונה ברזולוציה הנמוכה ביותר שיש ב-StyleGAN2 (כלומר 4×4). החלפה זו מאפשרת למצוא את הטרנספורמציה T ל- \mathbf{w} כדי שהגנרטור ייצור מ- $\mathbf{w}(T)$ את התמונה המוזצת/המסובבת, בזרה קלה.

לבסוף השערוך של התמונה X להיזה/סיבוב נמדד באמצעות (peak signal-to-noise ratio PCINR) בין X לתמונה המוזצת/המסובבת "המושלמת" בין זו, הנוצרת מהווקטור הלטני המוזץ/המסובב. לבסוף equivariance מחושב בתור ממוצע של PCINR-ים מעל סיבבים/היזאות של וקטורי \mathbf{w} האפשריים.

בנוספ' המאמר מציע כמה שיטות לארכיטקטורה של StyleGAN2 שביניהם ביטול רעש פר-פיקסל והקטנה של מספר השכבות בגנרטור.

הישgi מאמר:

המאמר הצילח ליצור תמונות שהם משמעותית יותר invariant寥寥 להיזה סיבוב ולהיזה מלאו הנוצרות באמצעות StyleGAN2 הסטנדרטי תוך שימוש עם אותו [FID](#).

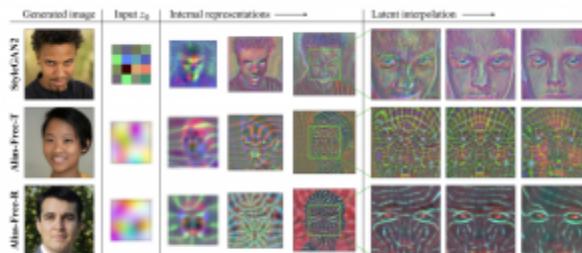


Figure 6: Example internal representations (3 feature maps as RGB) in StyleGAN2 and our generators.

ג.ב.

אחד המאמרים הראשונים שהציג שיטה מבוססת טכניקות anti-aliasing קלאסיות להטמודד עם תופעת הפיקסלים הדבקים, המתרכשת בתמונות הנוצרות באמצעות StyleGAN2. אני מניח שמדובר זה יהווה סמנית ראשונה למחקרים בנושא של התמודדות עם תופעת התקפלות תדרים במודלים גנרטיביים בתחום הראייה הממוחשבת.

ברצוני להודות עמוקות [לישי טוב](#), מנכ"ל טכנולוגיית [EntityMed.com](#) על עזרתו בפיענוח עיבוד האותות במאמר. ותודה ענקית [לירון יצחקי](#), ראש צוות מחקר [HourOne.ai](#) על סיועו המוחין בהבנת המאמר. ללא עזרתם של ישן של לירון סקירה זו לא היתה יצאת לאור!!

Review 13: AVAE: Adversarial Variational AutoEncoder

תאריך פרסום: 21.12.2020

הציג בכנס: טרם ידוע

תחומי מאמר:

- אוטו-אנקודר וריאציוני (VAE – Variational AutoEncoder) ().
- גאנים (GANs – Generative Adversarial Networks) ().

כליים מתמטיים, טכניקות, מושגים וסימונים:

- פונקציה לואס של VAE (המתקבלת מ- ELBO – Evidence Lower Bound).
- מרחק KL בין התפלגיות.
- מידע הדדי בין משתנים אקראיים/התפלגיות (Mutual Information).
- צואර בקבק אינפורמציוני (information bottleneck).
- פונקציית הלוס הסטנדרטית של גאן (מהמאמר המקורי) והפתרון האופטימלי שלה מבחינה הדיסקרימייטור.

בahirot ctiha: binonit minos

רמת היכרות עם כלים מתמטיים וטכניקות של ML/DL הנדרשים להבנת מאמר: נדרשת הבנה عمוקה ב- VAE, גאנים ותכונותיהם בשבייל להבין לעומק את הרעיון הבסיסי של המאמר. שליטה בכלים מתמטיים בתחום ההסתברות והסטטיסטיקה נחוצה להבנת המאמר.

ישומים פרקטיים אפשריים: גינרט תמונה באיכות גבוהה עם VAE (סוג של 😊).

המלצת קריית ממיך: מומלץ לבורי ידע עמוק ב- VAE, גאנים ובעל ידע מוצק בהסתברות בתור אתגר.

מבוא והסבר כללי על תחום המאמר:

יצירה של תמונות פוטוריאלייטיות ע"י רשותות נירונים הפכה לנושא חם בלמידה העמיקה מאז שיאן גודפלו (Chen Goodfellow) הגה את הרעיון של GANs ב- 2014. מאז הוצעו מספר מודלים גנרטיביים שונים לצירוף נתונים במספר דומיניים שהפופולריים ביניהם הגאנים -VAE-, כאשר לכל אחד מהם יתרונות וחסרונות משלו. למשל GAN מצטיין ביצירת תמונות שנראות ממש כמו אמיתיות (קרי פוטוריאלייטיות) אך הוא מאוד קשה לאימון. התופעות כמו Mode Collapse (יצירה של תמונות כמעט זהות ע"י הGENERATOR) וגם התכנסות של תהליכי האימון אינה מובטחת – אלו רק חלק מהבעיות שעלוות במהלך אימון של גאן. בנוסף המבנה של המרכיב הלטנטי

של גאן אינט נוח לניטוח ולא נתון בצורה מפורשת. מה עבר שני VAEs יותר קלים לאימון והמרחב הלטני שלהם נתון בצורה מפורשת יותר אך התמונות שנוצרות באמצעותם הן מוטשטשות ופחות פוטוריאלייטיות לרוב.

קודם כל נזכיר ממש בקצרה מה זה בעצם VAE.

הסבר קצר על VAE: ארכיטקטורה של VAE מורכבת משתי רשות עם פרמטרים בלבד.

- הרשות המקודדת (אנקודר) e_{vae} שmaps דוגמא מהמרחב המקורי למרחב הלטני Z (בעל מימד נמוך).
- הרשות המפענחת D_{vae} (דקודר) מנסה לשחזר את הדוגמא מה"יצוג הלטני" שלה.

האימון של VAE מתבצע בצורה הבאה:

- הרשות המקודדת e_{vae} ממפה דוגמא X לפרמטרים של ה"יצוג הלטני" שלה Z .
- מגירים וקטור אקריאי (בדרכו כל גאוסי) עם הפרמטרים מהשלב הקודם.
- מעבירים את הוקטור המוגדר דרך הרשות המפענחת D_{vae} לשחזר של הדוגמא המקורי X .

פונקציית הלווי של VAE, המסומנת ע"י e_{vae}^L , מקבלת ע"י שימוש בחסם העליון של ELBO – evidence:

- LOSE שחזר: עד כמה טוב D_{vae} הצליחה לשחזר את התמונה המקורי X . בדרך כלל LOSS השחזר מחושב למרחק הריבועי q_{KL} בין התמונה לבין התמונה המקורי המשוחזרת.
- מרחק KL בין התפלגות פריור על מרחב הלטני לבין התפלגות פואטריאיר או של (המשוערת על סמן פלטימן של הרשות המקודדת e_{vae}^E). סמן את המרחק הזה ב E_L .

בתהליך האימון של VAE הרשות המקודדת והרשות המפענחת מאומנות במטרה למזער את E_L .

כדי להבין את הסיבות העיקריות ליכולת החלהה של VAE ליצור תמונות פוטוריאלייטיות, המאמר מנתה את פונקציית הלווי שלה ומציין שתי סיבות עיקריות לכך:

סיבה 1: המאמר מנתה את האיבר השני שלו, כולם A_{KL} , ומוכיח שניתן לתאר את A_{KL} כסכום של המידע ההדדי בין הדוגמה X לייצוג הלטני האפואטריאיר שלה $|z|$, ומרחב KL בין התפלגות האפואטריאיר $|z|$ והתפלגות פריור של Z (בדרכו כל גאוסי בעל תוחלת אפס מטריצת קוריאנס I). מזער של איבר זה משמענו.

הגבלה על מידע הדדי בין דוגמא לייצוגה הלטני (!!) במטרה לקרב את התפלגות של $|z|$ לזו של פריור Z .

כלומר, איבר זה הינו למעשה צוואר בקבוק אינפורמציוני המגביל את זרימת המידע בין X לייצוג הלטני שלה. זה בפועל מקשה על הרשות המפענחת לשחזר את התמונה המקורי מהקוב הלטני Z (כי חלק מהמידע הולך לאיבוד בין הדוגמא לייצוגה הלטני עקב צוואר הבקבוק האינפורמציוני). בנוסף הלווי הריבועי המופיע באיבר הראשוני של e_{vae}^L , גורמת לו-VAE לייצור תמונות מוטשטשות. המאמר מצטט עבודה של [LeCun et al](#) המראה שלמעשה הערך האופטימלי של כל פיקסל בתמונה המשוחזרת הינו לו התוחלת שלו המותנית ב" מידע הנמצא בקוב הלטני שלה". כתוצאה לכך הרשות המפענחת לרוב פשוט לא מצליחה להפיק תמונה פוטוריאלייטית מה"יצוג החלקי" שמוצן אליה.

סיבה 2: הסיבה השנייה טמונה בהנחה המקובלת בראיה הממחשבת כבר שנים: לתמונות הטבעיות יתרות רבה (במיוחד היתרויות הлокליות) שמאפשרת לתאר אותן במרחב ממימד נמוך (low-dimensional manifold). אולם (לטענת המאמר) הטקסטורות כמו עץ, שער או גלים "חיים" במניפולד ממימד נמוך, עקב התכונות האינרגנטיות שלהם (למשל שיער של אדם מורכב מהרבה שערות שלכל אחד אופיינם משלו). לעומת זאת VAE, הגאים מצחיכים להתגבר חלקית על סוגיה זו ע"י יצרה של דוגמאות המהוות תת-קבוצה של המניפולד ממימד גבוה שבו "חיות" הטקסטורות, שמספיקות כדי "להוביל שלו" את הדיסקרימינטור. כתוצאה לכך התמונות של אן יוצאות יותר "טבעיות" ופחות מטושטות של VAEs.

רעיון המאמר בגודל: המאמר מציע לשלב את היתרונות של VAE וaganims ע"י שיבוצם בארכיטקטורה שלהם, הנקראת AVAE. אני רוצה לציין שהרעיון הזה לא חדש וכבר ב- 2015 ניסו לעשות זאת ב- VAE/GAN. במאמר הציעו להחליף את השגיאה הריבועית ברשות המפענחת בדיסקרימינטור כמו זה של אן. הבעיה בגישה הזאת שהדמיוון של התמונה המשוחזרת למקורית כבר לא בא לידי ביטוי. שיטה נוספת מפורסמת המשלבת את שתי גישות אלו (VAE חלקית וגאגן) הינה BiGAN שמורכב מהרשת המקודדת, הרשת המפענחת והדיסקרימינטור. הדיסקרימינטור מנסה לבדוק בין לאלו שנוצרים ע"י הרשת המקודדת. BiGAN מצליח ליצור תמונות פוטוריאלייסטיות אך (לטענת המאמר) יכולת השחזור שלו נמוכה (לומר תמונות נוצרות מוקטורים קרובים לייצוג לטנטי של תמונה נתונה א, לא תמיד יוצאות דומות ל-א), כלומר המרכיב הלטנטי פחות קוהרנטי.

המאמר הנזכר מציע לשלב את לוֹס השחזור עם הלוֹס האדוֹוְסֵרִי בצורה שתיצור גם תמונות באיכות דומה בלבד, לפחות ב"קוהרנטיות של המרכיב הלטנטי". הרעיון העיקרי של AVAE הינו הוספת רשת הגנרטור G ל- VAE הסטנדרטי, שלוקחת כיקלט את הוקטור הלטנטי המופיע ע"י הרשת המקודדת vae_E. המאמר גם מציע להוסיף(concatenate) לקלט של G וקטור נוסף a_z המפולג עם התפלגות גאומטרית סטנדרטית – לטענת המאמר a_z מיועד לייצוג מידע מתמונה שהרשota vae_E לא הצליחה להפיק ממנה.

הסבר מעמיק על רעיונות בסיסיים:

נתחיל מההסבר על פונקציית לוֹס avae_L של AVAE. פונקציית הלוֹס של AVAE הינה סכום (משוקלל) של הלוֹס הסטנדרטי של VAE, המסומן כ- vae_L והלוֹס של הגנרטור G, המסומן ב- G_L. עקרונית הגנרטור G צפוי לשרת כ"הפכית" של הרשת המקודדת E וזה הנקודה החשובה של המאמר:

התפלגות המותנית $z|x$ (G_k) של פלט הגנרטור G בהינתן וקטור לטנטי z והתפלגות $z|enc_k$ של פלט(!) הרשת המקודדת, בהינתן וקטור הלטנטי z, צריכה להיות כמה שיותר קרובות (כאשר הוקטור z מתפלג לפי התפלגות הפרIOR).

כלומר פונקציית המטרה G_L של הגנרטור G הינה הקروس-אנטרכפי בין $z|enc_k$ לבין $z|x$ (G_k) כלומר התוחלת של $-z|enc_k \log(z|enc_k)$ מעל התפלגות $z|x$ (G_k), כאשר z מתפלג לפי התפלגות הפרIOR (0, 1).

הערה צד לגבי האימון: במהלך האימון של AVAE, הקלט של G אינו נלקח מהפלט של הרשת המקודדת vae_E, אלא נציג ישרות מהתפלגות הפרIOR של z. אני מנחש שהה הופך את הגנרטור יותר דומה לזה של הגאגן המקורי במטרה "לחקות" את תכונות החזקות שלו ביצירה פוטוריאלייסטיות.

נתחייב מכך אינטואיציה מאחוריו הרעיון הד' לא טריויאלי זהה:

פינט אינטואיציה: שימו לב שהמטרה כאן היא לאמן את הגנרטור ליצור תמונות פוטוריאלי-סטיות מההתפלגות הפרIOR מחד (נראה בהמשך AIR_G_L מוביל ללוס דומה לזה של הגן הסטנדרטי) עבר וקטורים לטנטים המתפלגים לפי הpriOR הנთון. שנית זה "מאלי" את הרשות המקודדת להפיק פיצרים לטנטים הנחוצים ליצירת תמונה פוטוריאלי-סטית. שלישית vae_L מאלץ את הרשות המקודדת enc_E להפיק פיצרים הנחוצים לשחרר מדויק של התמונה (ע"י מזעור המרחק הריבועי בין התמונה המקורי למשוחזרת). המשחק המורכב זהה מאפשר G ליצור תמונות פוטוריאלי-סטיות מחד תוך שימוש קוגניטיבי של המרחב הלטני (וקטורים לטנטים קרובים יוצרם תמונות דומות כלומר "יחס' המרחק" במרחב המרקי נשרמים).

עכשו בואו נבין AIR_G_L מוביל ללוס דומה לזה של גאים "הגורם" לו ליצור תמונות פוטוריאלי-סטיות. המאמר מוכיח ש- vae_L ניתן לפרק לסכום של המרכיבים הבאים:

- **האיבר הראשון:** תוחלת של $(x|z(p)) \log(p)$ מעל התפלגות $(z|x)$ כאשר הווקטור z מתפלג לפי התפלגות priOR. איבר זה למעשה משערך עד כמה "סביר" להפיק וקטור לטנטי z מהתמונה דרך הרשות המקודדת enc_E , כאשר x שנוצר ע"י הגנרטור G בהינתן אותו וקטור לטנטי z . החלק הזה הוא קל יחסית לחישוב - ומשוערך כמרחק ריבועי בין z לבין התוחלת של הפלט ש- vae_E מפיק מ- G_x , מנורמל בשנות של הפלט שלו. נזכיר שהינתן תמונה x המקודד מוציא זוג של $(x|z(p)) \log(p)$ של התוחלת והשנות של הייצוג הלטני של x בהתאם (מהם מגירים את הקטלט לרשות המפענחת vae_D).
- **האיבר השני:** מרחק KL בין התפלגות האמיתית של הדטה $(x|data)$ לבין הקטוע של הלוס האדברסרי. כדי לשערך את הלוס הזה מאמנים רשות מבקרת (critic), המסומנת כ- C , שטרתה לבדוק אם התמונות האמיתיות מהדאטסהט לאלו שנוצרו ע"י הגנרטור (הפלט של הינו הסתרות של הקטלט להיות תמונה אמיתית). פונקציית המטרה של C הינה זהה לפונקציית המטרה סטנדרטית שלGAN. אבל איך כל זה למעשה קשור למרחק KL בין $(x|data)$ לבין $(x|z(p))$, אתם שואלים? אולי אתם זוכרים שהפתרון האופטימלי עבור GAN_L מבנית הרשות המבקרת C לרשות הגנרטור נתונה, הינו היחס בין $(x|G_z)$ לבין הסכום של $(x|data)$ ו- $(x|z(p))$. אם נציב את הפתרון הזה לפונקציית המטרה gan_L נקבל את הלוגריתם של היחס בין $(x|G_z)$ לבין $(x|data)$ המהווה משערך בלתי מוטה למרחק KL בין $(x|G_z)$ לבין $(x|data)$. כמובן אם נאמן את C מספיק טוב ונציב אותו ל gan_L עבור תמונה x נתונה הערך המתkeletal יכול לשמש כמשערך לאיבר השני של הלוס G_L .
- **האיבר השלישי:** אנטרופיה של $(x|data)$ (התפלגות התמונות הנוצרות ע"י הגנרטור). איבר זה אינו תלוי בדטה (מתאר את התפלגות הפלט הגנרטור). מינימיזציה של איבר זה מאלצת את $(x|data)$ להיות יותר מרכזית סביר המודים שלה (זה גורם לרידה באנטרופיה) והמאמר מציע לא לקחת אותו חשבן באמצעות רגולריזציה (מצין שהאיבר הזה הינו intractable)

לסיום, AAE מורכב מ 4 הרשותות הבאות:

- הרשות המקודדת הסטנדרטית vae_E
- הרשות המפענחת הסטנדרטית vae_D
- הגנרטור G המיועד לייצור תמונה מוקטור לטנטי (עם אופציה להוסיף וקטור לטנטי נוסף לכיסוי של תוכנות של תמונות ש- vae_E לא הצליחה להפיק)
- הרשות המבקרת (דיסקרימינטור) C שטרתה לבדוק אם התמונות מהדאטסהט לתמונות מגנרטות

המחלצת הזה מאומנת עם פונקציית מטרה שהיא סכום של vae_L ו- G_L שמושברים מעלה.

הישג מאמץ: המאמר משווה את ביצועיו של AVAE מול השיטות הבאות: BiGAN, VAE/GAN, BiGAN, VAE, BiGAN ו- LPIPS על הדאטאסטים הבאים:

- Bedroom
- CelebA
- CIFAR10
- CIFAR100
- SVHN

עבור כמה מהדאטאסטים האלו הם הצלחו להשתפר בחלוקת המטריקות (הלו סריבועי שופר עבור כל הדאטאסטים) אבל רוב השיפורים לא נראים לי ממש מרשים. הם גם טוענים שההתוצאות שלהם נראות יותר פוטוריאליסטיים מאשר VAEs אחרים ואני נוטה להסכים איתם אך זה די סובייקטיבי 😊



[לינק למאמר: זמין להורדה](#)

לינק לקוד: למורות שבמאמר מופיע שהקוד יהיה זמין בGITהאב לא הצלחתו לאתרו.

גב. מאמר עם רעיון מאד מעניין ומוגניב אך כתוב בצורה לא מספיק ברורה. תרשימי זרימה שיש במאמר לרוב לא עוזרים בהבנה. צריך להודות שהתוכנות לא הרשימו אותו יותר מדי וגם הקוד לא שותף שזה די מכובד. נאלץ לא להעניק לו המלצה קרייה ממיק. עם זאת הכלים/תובנות המתמטיים שפותחו במאמר נראים לי מבטחים ומעניינים ואני מקווה לראותם מיושמים בעתיד ומשיגים תוכאות משמעותיות יותר.

Review 14: BART: Denoising Sequence-to-Sequence Pre-training for Natural Language Generation, Translation, and Comprehension

פינט הסוקר:

המלצת קריאה ממילא: חובה לאנשי NLP, במיוחד לחוקרים העוסקים במודלי שפה, מbossו, טרנספורמרים.

בahirot כתיבה: גבוהה.

רמת היכרות עם כלים מתמטיים וטכניקות של DL/ML הנדרשים להבנת מאמר: נדרשת היכרות עם מודלי שפה, המבוססים על טרנספורמרים כמו BERT ו-GPT.

ישומים פרקטיים אפשריים: גנרט טקסטים ברמה גבוהה יותר ובדרך פשוטה יותר מאשר של BERT.

פרטי מאמר:

לינק למאמר: [זמן כאן](#)

לינק לקוד: [זמן כאן](#) (בתוך פיתורץ)

פורסם בתאריך: 29.10.19, בארכיון

הוצג בכנס: Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics

תחומי מאמר:

- טרנספורמרים
- denoising autoencoder
- מודלים גנרטיביים

תמצית מאמר:

המאמר הנסקר מציע ארכיטקטורת רשת חדשה מסוג denoising autoencoder לשחזור דата טקסטואלי מושרע. לאחר האימון ניתן להשתמש במודל לביצוע של מספר משימות NLP ו-NLU גנרטיביות ודיסקרימינטיביות כגון תרגום, מענה אוטומטי על שאלות, תמציות אבסטרקטיבי וכמה סוגים נוספים.

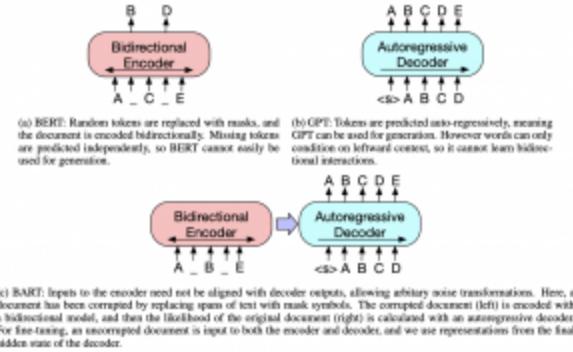


Figure 1: A schematic comparison of BART with BERT (Devlin et al., 2019) and GPT (Radford et al., 2018).

תקציר מאמר:

המאמר מנסה לשלב את התכונות החזקות של שני מודלי טרנספורמריםći פופולריים בתחום NLP היום:

- **GPT (וצאצאי):** יכולת לגנרט טקסטים ברמה "גבוהה" (יחסית למתרחרים ע"י למידה של מודל שפה באופן אוטורגרטיבי (המודל משתמש רק בטוקנים שקדמים ל토큰 הנחזה כדי לחזות את הטוקן הבא).
- **BERT:** למידת ייצוג לטנטי חזק (בעל מידת נמור) של טקסט באמצעות למידת מודל שפה דו-כיוונית.

נציר כי החולשה המשמעותית של BERT נמצאת באילו יכולתו לגנרט טקסטים בצורה פשוטה ושקופה (נכון שיש בעבודות שמציעות שיטות המצליחות "להכריח" את BERT לגנרט טקסטים אך בדרך כלל זה די מסובך ואיכות הטקסטים המוגנרטים תמיד יותר נחותה ממודל SOTA).

از מה בעצם החידוש ש-BART מציע לנו? קודם כל BART מורכב מהמקודד ומהמפענה (decoder-encoder) ומואמן כמו autoencoder denoising (הכוונה כאן ל-pretraining כי בעיקרון כל שימושה של הדרישה כיוול של הרשות). ככלمر הקטל למקודד הוא טקסט מורעש שהמקודד ממפה אותו למרחב הלטנטי כאשר המטריה של המפענה זה לשחרר את הטקסט המקורי.

ניתן להסתכל על BART כהכלאה של BERT ו-GPT כאשר הוא משלב את הארכיטקטורה הדו-כיוונית של BERT והגיישה אוטורגרטיבית של GPT (קרי בונה את הפלט משמאלי לימין - הכוונה כאן לשפות שכותבים בהן משמאלי לימין :)). גישה זו מאפשרת להריעש את הקטל במגוון דרכים שבහלט תורם חיובית לעוצמת הייצוגים הלטנטיים של טקסט השמודל בונה. אזכיר שלבדיל מ-BERT שמסווה חלק מהמלים ומנסה לשחרר אותם (האימון של BERT מכיל גם את הדיזמי של סדר בין מושגים - אתייחס לזה בהמשך), BART משתמש במספר שיטות מעניינות להריעש הטקסטים.

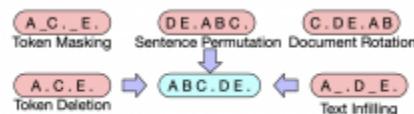


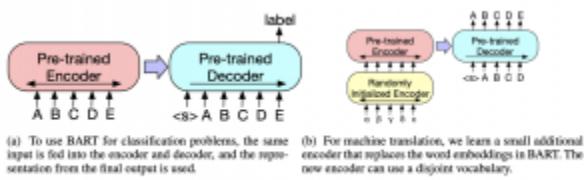
Figure 2: Transformations for noising the input that we experiment with. These transformations can be composed.

שיטות אימון:

כאמור בנוסף להסוואת הטוקנים, המחברים הציעו לאמן את BART עם שיטות הרעשה הבאות:

- מחיקת טוקנים:** והמודל צריך להחליט באילו מקומות יהיו הטוקנים החסרים.
- הסואאה של קבוצות של טוקנים רציפים (text infilling):** כאן מגרילים מספר טוקנים רציפים שיווין, באמצעות שימוש בתפלגות פואסן (לא מסבירים למה בחרו דזוקא בפואסן ולא כל התפלגות דיסקרטית אחרת) ומחליפים את כל הטוקנים האלו בטוקן MASK. צריך לציין שלכל הטוקנים המושווים יש טוקן MASK אחד בלבד שמחליף אותם. המודל מאמין לחזות כמה טוקנים הוועו. המאמר מציין כי מספר הטוקנים המושווים יכול להיות אף כלומר אף טוקן לא מסותר ו-MASK פשוט הוכנס אל תוך הטקסט.
- תמורה (פרמוטציה) של משפטיים:** סדר המשפטים שונה בהתאם לפרמוטציה אקראית. המודל צריך לחזות את הסדר הנכון של המשפטים.
- סיבוב המסתמך:** טוקן נבחר באקראי והtekst מסובב באופן זה שהטוקן הנבחר הופך להיות הטוקן הראשון. המטרה של המודל ליזהות את התחלת הטקסט.

המחברים בחנו את הגישות הנמל' והביצועים הכל' טובים מתקבלים כאשר משלבים את text infilling יחד עם פרמוטציה של משפטיים (2 ו- 3 בראשיהם). מעניין שימוש ב-2 ו-3 יחד לaimon מכליל את הגישה של BERT המשווה, כאמור, טוקנים בודדים ומנסה לחזות סדר של זוג נתון של משפטיים. במאמר נתען שהזיה גורם למודל להתחשב יותר באורך המשפט ולנקח בחשבון תלויות ארוכות טווח (כלומר להתחשב ביוטר טוקנים/משפטים לחיזוי הטוקן הבא).



ארQUITטורה:

היא די דומה לארכיטקטורה של BERT עם שני הבדלים משמעותיים: כל השכבות של המפענה מבצעות חישוב של cross-attention עם השכבה האחורונה של המקודד לעומת BERT שבמציע את זה רק בשכבה האחורונה של המפענה. ההבדל השני הוא העדר שכבות feed-forward לפני השכבה האחורונה. חוץ מזה יש הבדלים קלים נוספים כמו שימוש בפונקציית אקטיבציה מסוג GELU במקום RELU.

פונקציית LOSS:

לא מצאתי אזכור באיזו פונקציית LOSS השתמשו במאמר, נראה קרווס אנטרופי רגיל על הטוקנים המשוחזרים.

שיטות ציול (fine-tuning) של BART באמצעות משימות שונות:

- משימות סיווג של סדרת טוקנים:** אותו קלט מזון למקודד ולמפענה והשכבה האחורונה של המפענה משתמש במסוג מולטי-קלואס לינארי. זה קצת דומה לשימוש בטוקן CLS של BERT אבל כאן מוסיפים טוקן בסוף הטקסט ולא בהתחלה כדי (לטענתם) שהמפענה יוכל ליצל את הפלט של כל השכבות הקודמות שלו (hidden) עברו.
- משימות סיווג טוקן:** המספר המלא הוכנס למקודד ולמפענה והפלט של השכבה האחורונה של המפענה משמשת לסיווג של הטוקן.

- **משימות גנרטיבי טקסטואלי:** כמו שאתם בטח זכרים המפענה של BART הינו אוטורגרטיבי ונitin לכיל אותו בצויה פשוטה בשביל משימות גנרטיביות כמו גנרטיב תשובה על שאלה או יצירה של תמצות אבסטרקטיבי. המקודד פשוט מקבל את הקלט והמפענה מגנרט את הפלט בצויה אוטורגרטיבית.
- **משימת תרגום אוטומטי:** כאן המאמר עשה משהו מעניין. המחברים החליפו את שכבת אמביגג של טוקנים ב-BART במקודד נוסף שהקליט שלו הוא השפה שמתורגמים ממנו (הם ניסו להשתמש במודל זהה רק לתרגום לאנגלית). מקודד זה אומן מופיע למפות מילים מהשפה המתורגמת ל "אנגלית מוקולקת/מורעשת" ואז המפענה "מנקה" אותה והופך אותה לאנגלית תקנית. המודל אומן בשני שלבים שהלוון בשנייהם הוא קරוס אנטרופי על הפלט של BART. בשלב הראשון מאומנים את המקודד החדש, שכבת self-attention הראשונה של המקודד של BART ו-self-attention encoding. בשלב השני מאומנים את כל הפרמטרים של BART במשך מספר קטן של איטרציות.

Model	SQuAD 1.1 F1	MNLI Acc	ELI5 FPL	XSum FPL	ConvAI2 PPL	CNN/DM PPL
BERT Base (Devlin et al., 2019)	88.5	84.3	-	-	-	-
Masked Language Model	90.0	83.5	24.77	7.87	12.59	7.06
Masked Seq2seq	87.0	82.1	23.40	6.80	11.43	6.19
Language Model	76.7	80.1	21.40	7.00	11.51	6.56
PennTree Language Model	89.1	83.7	24.03	7.69	12.23	6.96
Multitask Masked Language Model	89.2	82.4	23.73	7.50	12.39	6.74
BART Base						
w/ Token Masking	90.4	84.1	25.05	7.08	11.73	6.10
w/ Token Deletion	90.4	84.1	24.61	6.90	11.46	5.87
w/ Text Infilling	90.8	84.0	24.26	6.61	11.05	5.83
w/ Document Rotation	77.2	75.3	53.69	17.14	19.87	10.59
w/ Sentence Shuffling	85.4	81.5	41.87	10.93	16.67	7.89
w/ Text Infilling + Sentence Shuffling	90.8	83.8	24.17	6.62	11.12	5.41

Table 1: Comparison of pre-training objectives. All models are of comparable size and are trained for 1M step on a combination of books and Wikipedia data. Entries in the bottom two blocks are trained on identical data using the same code-base, and fine-tuned with the same procedures. Entries in the second block are inspired by pre-training objectives proposed in previous work, but have been simplified to focus on evaluation objectives (see §4.1). Performance varies considerably across tasks, but the BART models with text infilling demonstrate the most consistently strong performance.

הישגי מאמר:

המחברים בחרו בדרך השואה מעניינת (לא סטנדרטיבית). קודם כל הם השווו את הביצועים של BART עם BERT ביחס למשימות רבות על מספר דatasets (זהה דווקא שగרתי למחרי). אז הם אימנו את BART באמצעות כמהGISות שהוצעו בעבר לאימון מודלי שפה מבוססי טרנספורמרים (BERT, XLNet, MASS) וכמה אחרת (והוכחו כי שיטת האימון המוצעת ל-BART מצליחה להשיג ביצועים יותר טובים מכל המשימות שנבדקו) פרט למשימה אחת (רשימת המשימות מפורטת בסעיף הבא). היהי רוצה לראות השוואת היא טובה של המודל המוצע מול ארכיטקטורות נוספות (למרות שדי השתקנות שיטת האימון המוצעת היא טובה אבל חסורה לי השוואת BART מול מודלים אחרים).

	SQuAD 1.1 EM/F1	SQuAD 2.0 EM/F1	MNLI m/mm	SST Acc	QQP Acc	QNLI Acc	STS-B Acc	RTE Acc	MRPC Acc	CoLA Acc
BERT	84.1/90.9	79.0/81.8	86.6/-	93.2	91.3	92.5	90.0	70.4	88.0	66.6
UniLM	-/-	80.5/83.4	87.0/85.9	94.5	-	92.7	-	70.9	-	61.1
XLNet	89.0/94.5	86.1/88.8	89.8/-	95.6	91.8	93.9	91.8	83.8	89.2	63.6
RoBERTa	88.9/94.6	86.5/89.4	98.2/90.2	96.4	92.2	94.7	92.4	86.6	96.9	68.0
BART	88.8/94.6	86.1/89.2	89.9/90.1	96.8	92.5	94.9	91.2	87.0	90.4	62.8

Table 2: Results for large models on SQuAD and GLUE tasks. BART performs comparably to RoBERTa and XLNet, suggesting that BART’s uni-directional decoder layers do not reduce performance on discriminative tasks.

משימות להשוואה:

המחברים ניסו את המודל שלהם על מגוון רחב של משימות כגון: SQuAD, MNLI, ELI5, XSum, ConvAI2, CNN/DM.

מאמר כתוב היטב עם רעיון פשוט שמצילח להוסיף יכולת גנרטיב יעילה ל-BERT. גם שיטת אימון המוצעת נראית לי מעניינת ויעילה. המאמר כתוב מעולה, קל מאוד לקרוא אותו. בקיצור מומלץ בחום.

Review 15: Bringing a GAN to a Knife-Fight: Adapting Malware Communication to Avoid Detection

פינט הסוקר:

המלצת קרייה מעדן ומיק: מומלץ לאנשים העוסקים בתחום ה-Cybersecurity או לאנשים שאוהבים GAN

בahirot כתיבה:

ידע מוקדם: GAN

"שומם פרקטיים אפשריים: זיהוי Malware

פרטי מאמר:

lienek למאמר: [זמן להורדה](#).

lienek לקוד:

פורסם בתאריך: 6.8.2018, בארכיב.

הוגג בכנס: IEEE Security and Privacy Workshops (SPW)

תחומי מאמר:

- זיהוי אנומליות
- GAN
- נזקנות

כליים מתמטיים, מושגים וסימונים:

מבוא:

כלי אבטחה שונים הנמצאים היום בשוק מצלחים להתמודד בהצלחה רבה עם נזקיות (Malwares) ידועים. כולם אלו כוללים חוקים סטטיים שנכתבו בצורה ידנית על ידי חוקר אבטחה, או לחילופין מערכות גלויי אונומליות שمبוססות על אלגוריתמים של למידת מכונה. אך, הצלחה זו בהווה אינה מבטיחה הצלחה בעתיד שכן אף שכלי הגנה שונים יודעים להשתמש בלמידה מכונה בשבל גלויי נזקיות, כך גם התוקפים יכולים להשתמש בלמידה מכונה כדי ליצור נזקיות מתוחכמתות יותר שיוכלו להתחמק מכלל כל הגנה הקיימים בשוק. הנזקה תוכל לשנות את התנהגותה בהתאם לסביבה ולתנאים אחרים היא רואה ובכך לחמק מכל הגנה השונים. נזקה שכזו יכולה להיות בעיה גדולה עבור תעשיית הסיבר.

כיום, נזקיות שמשנות את התנהגותן בצורה דינמית מסתמכות בעיקר על שיטות סטטיות (למשל אלגוריתם [DGA](#)). אך שיטות אלו אינן מספיקות כדי להתחמק מכל הגנה הטובים ביותר בשוק. כדי להתחמק מכל הגנה אלו הנזקקה צריכה להיות מסוגלת לפתח לוגיקה מורכבת וללמוד את הסביבה שלה. כאן, נכתבים כתבי המאמר שמצועים שימוש ב- [\(GAN\)](#) [Generative Adversarial Networks](#) שישמש את הנזקקה כיצד לפעול תחת תנאים שונים. הרעיון מאחורי השימוש ב-[GAN](#) הוא ש-[GAN](#) יוכל לעזור למדוד את תעבורת הרשות בה היא נמצאת ובכך לחכות אותה בצורה טובה יותר. בכך, היא תצליח להתחמק מכלל כל הגנה הפרושים בארגון ולא להתגלות.

הסבר על השיטה:

כתבי המאמר מציינים שתעבורת הרשות אותה [-GAN](#) ינסה לחקות הינה של פיסבוק ובפרט צ'ט של אפליקציית פיסבוק. זאת מכיוון שתעborות רשות מסווג זה היא נפוצה ורובה אפשררת על ידי כלים כמו חומת אש. לאחר ש-[GAN](#) ילמד כיצד תעborות פיסבוק נראות, הוא יוכל להנחות את הנזקקה כיצד לפעול כדי להתחמק מתחסימה. המטרה של הנזקקה היא לתקשר עם שרת התקוף. הסביבה (המגן) תוכל לחסום את ערז התקשרות של הנזקקה ועליה לדעת להתמודד עם מצב זה. [GAN](#) נועד לבדוק בשבל לענות על אותו מצב.

ה-[GAN](#) ביצע אימון מקדים([pretraining](#)) לפי הכנסתו לארגון, כאשר הפלט אותו ינסה ליצור הינה הקונפיגורציה בדמות שלושה פרמטרים, של הנזקקה שמכטיבה לו כיצד להתנהג. הפלט כולל שלושה פיצרים: כמות הביטים המקסימלית שתעbor ב-WGAN, הזמן של flow וכמה זמן לחכות בין ה-WGAN הנוכחי לבא אחריו (כאשר הכוונה ל-[network flow](#)).

ה-[GAN](#) עובד בשני חלקים:

Generator: מקבל רעש כלשהו ומנסה לבנות ממנו את הקונפיגורציה.

Discriminator: מקבל קונפיגורציה זו וקונפיגורציה אמיתי של פיסבוק וצריך להחליט האם הקונפיגורציה שנוצרה על ידי G הינה אמיתי או מזויפת.

לאחר החלטה של ה-D מחושב ה-[Loss](#) ותהליך של Backprop עדכן את המשקלים של D ו-G. כתבי המאמר מציינים שב-[GAN](#) קשה לקבוע מתי ה-[GAN](#) מתכנס שכן פונקציית ה-[Loss](#) לא בהכרח מוציבה על איקות הפלט

שה-GAN מייצר. כדי להתמודד עם בעיה זאת הכותבים השתמשו בכל הגנה חיצוני מסווג [Intrusion Protection System](#), או בקיצור IPS, כדי שיבחן את הפלט של ה-GAN.

לאחר שה-GAN עבר אימון מקדים, מחברים אותו לנזקה והוא מתחילה לייצר את הקונפיגורציה שנשלחת לנזקה. על ידי הקונפיגורציה החדשה, הנזקה תוכל לשנות את מאפייני ערוץ התקשרות עם שרת התוקף. אם הנזקה מגלה שערוץ התקשרות שלה נחסם היא מאותה ל-GAN שבתגובה מבצע אימון נוסף נוסך על הדטה שהנזקה שלחה לו שנחסם ומיצר לה קונפיגורציה חדשה.

הסביבה:

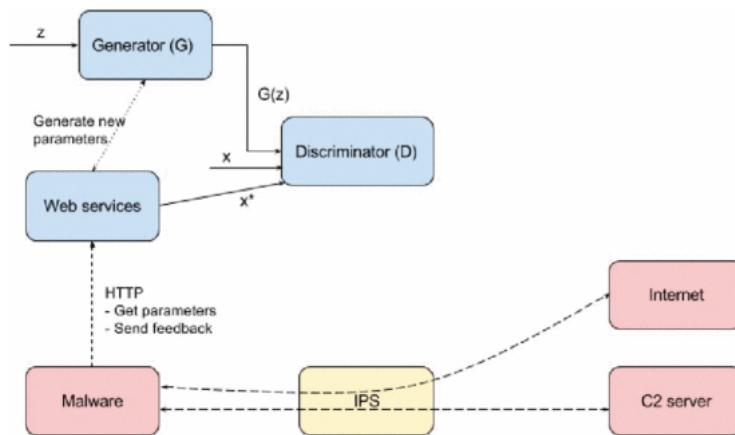
כדי להראות שהגישה אכן עובדת בסביבה אמיתיית, כותבי המאמר ציינו שתי מגבלות:

- הנזקה בה משתמשים הינה נזקה אמיתיית
- החסימה של תעבורת הרשות צריכה להיות אמיתית גם כן

הnezקה בה השתמשו הינה [FLU](#). הקוד שלא שונה בכך שאת הפרמטרים שקובעים כיצד לייצר את ערוץ התקשרות עם השרת היא מקבל מה-GAN. השרת של התוקף הוקם על גבי ענן AWS. מזכיר שוב שמטרת הניסוי היא לראות שהnezקה מצליחה לתקשר עם השרת עם כמה שפחות חסימות של המגן.

המגן במקרה זה הינו IPS מסווג [Stratosphere](#). ה-IPS הוקם בחיבור של הארגון עם האינטרנט ובכך ה-IPS יוכל לבדוק את כל התעבורה שייצאת מהארגון ולחסום תעבורה חשודה. במקרה זה עליו לנסוט לחסום את תעבורה הנזקה אל עבר השרת שלה.

הGAN בו השתמשו הינו רשת מסוג LSTM גם ל-Generator וגם ל-Discriminator. בנוסף מומש רכיב WEB שיהיה אחראי על התקשרות בין ה-GAN לבין הנזקה ובהעברת המידע של ה-GAN לנזקה.



איור 1: סביבת הניסוי. ה-GAN ממומש ומתאים באופן נפרד וمتקשך עם הנזקה דרך שירות WEB. הנזקה מקבלת את הקונפיגורציה מה-GAN ומנסה את ערוץ התקשרות שלה בהתאם בזמן אמיתי. על ערוץ התקשרות עם השירות להיות פעיל בכל זמן נתון. ה-IPS יחסום כל תעבורת רשות שלא נראה כמו צ'ט של פיסבוק.

הניסוי:

הданה שנאוסף בשבייל אימון ה-GAN הינו דата אמיטי של שני משתמשים המדברים ביניהם דרך אפליקציה הצעט של פיסבוק. השיחה כללה תמונות, טקסט ומסמכים כדי לדמות שיחה מגוונת ואמיתית. תובורת הרשות של השיחה הוקלטה ונשמרה בתוך הדנתה שהזון ל-GAN.

ה-IPS קונפג בחולנות זמן שונים, כאשר גודל החילון מציבע על כמות המידע אותו בוחן ה-IPS. על כל חילון שהוא רואה הוא מבצע פרדייקציה - כן או לא צעט של פיסבוק. שימוש בחולנות שונים נועד לראות כיצד ה-GAN מתמודד בזמן אמת עם שינויים בסביבה.

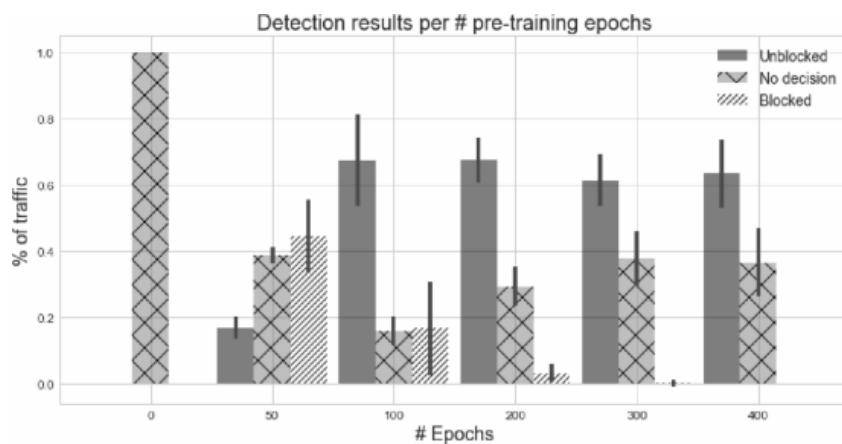
תוצאות:

בטבלה הבאה ניתן לראות את טיב האימון של ה-GAN:

# Epochs	Mean (%)	Std (%)
0	0.0	0.0
50	16.88	3.26
100	67.37	13.89
200	67.54	6.84
300	61.39	7.84
400	63.42	10.37

עמודת Mean ועמודת Std מייצגות את הממוצע וסטיית התקן של מספר הפליטים (קונפיגורציות) של ה-GAN שלא נחסמו על ידי ה-IPS. ניתן לראות שככל שה-GAN מתאמן יותר, כך מספר הקונפיגורציות שלא נחסמו בממוצע עולה. זה מצביע על כך שה-GAN מצליח ללמידה כיצד להתחמק מה-IPS.

בגרף הבא, כתובי המאמר מראים את כמות Flows שהנזקה יצרה בכל חילון זמן של חמיש דקות בהתאם לההואות שקיבלה מה-GAN:



ניתן לראות שככל שה-GAN מתאמן יותר אחוז המידע שנחסמת על ידי ה-IPS יורדת לאפס.

לבסוף כתבי המאמר מציינים שתוך כדי הניסוי, בזמן הריצפה, הדatta שה-IPS תיג, נשלח לאימון נוספת של ה-GAN כדי לנסות ולשפר אותו. הם מוסיפים ואומרים ששיטה זאת הראתה שיפור בBITSURIM אך לא במידה שהיא מובהקת מספיק. סה"כ השיטה הראתה תוצאות טובות. 63% מהתקשרות לא נחסמה, דבר שהופך את השיטה לפרקטיבית לדברי כתבי המאמר.

סיכום:

המאמר מציג את יכולת חבר GAN לפיתוח של נזקה אמיתית במטרה להפוך את הנזקה למתחכמת ומקלמת אף יותר. באמצעות ה-GAN הנזקה הצליחה להויריד ב-63% את סיכוי גילואה על ידי כל הגנה אמיתית מסווג IPS. ה-GAN אומן כדי לנסות ולחקות תעבורת רשת של צט פיסבוק והמשיך להתאים תוך כדי זמן הריצה לאחר שקיבל מידע מהנזקה אילו מפלטי התגלו על ידי ה-IPS. חשוב לציין שה-GAN התאים על כמות DATA קטנה בהתחלה ועדין האлич להביא תוצאות טובות מה שהופך את השיטה הזה לפרקטיבית במצבות.

שיטות פעולה: הסקירה נכתבה יחד עם עדן יבין.

Review 16: COCO-LM: Correcting and Contrasting Text Sequences for Language Model Pretraining

פינת הסוקר:

המלצת קריאה ממיק, משה: מומלץ לקרוא לאלו שעוסקים באימון מודלי שפה וגם אוהבים את הגישה הניגודית

ברירות כתיבה: גבורה מינוס

ידע מוקדם: ידע בשיטות אימון של מודלי שפה גדולים כמו BERT וגם ביסודות הלמידה הניגודית

פרטי מאמר:

لينק למאמר: [זמן להורדה](#).

لينك לקוד: [כאן](#)

פורסם בתאריך: 27.10.21, בארכיב.

הוזג בכנס: NeurIPS.

תחומי מאמר:

- עיבוד שפה טבנית (NLP)
- אימון של מודלי שפה

כליים מתמטיים, מושגים וסימונים:

- טרנספורמרים
- Pretraining של מודלי שפה גדולים
- לוס ניגודי ולמידה ניגודית
- BERT, ELECTRA

מבוא:

מודלי שפה ענקים, בעלי מיליארדי פרמטרים, המבוססים על רשתות ניורוניים, הפכו להיות ברירת מחדל למרבית משימות ה-NLP בשנים האחרונות. באופן יותר מדויק, משפחת הטרנספורמרים שליטה כמעט ללא עוררין בתחום זה. עקב ההגדלה והמורכבות של המודלים, קשה לאמן אותם מאפס, ומקובל לכיל מודל שאומן מוקדם יותר על דאטאsett גדול ומגוון (ובדרך כלל לא מותג), באמצעות הדעתה של המשימה החדשה. זאת, מתוך ההבנה שהשכבות המוקדמות של כל מודל נוטות להתכנס למשקלים דומים בכל המשימות באותו התחום, ולכן ניתן להסוך במידה רבה את האימון שלהם. תהליכי אימון מודל על דאטאsett גדול נקרא בספרות אימון מוקדם (pretraining), או שהוא נקרא פשוט אימון, ותהליך הכילו נקרא אימון חדש (retraining) או fine-tuning.

את השימוש בטרנספורמרים לשימוש מידות ניכרת הציג לראשונה BERT לפני כ-4 שנים. BERT הצעיר שוט שיטות ב"פיקוח עצמי" (self-supervised) לאימון:

1. מסור של כמה טוקנים בטקסט (בערך 15%) וחיזום באמצעות המודל (Masked Language Modeling - MLM).
2. עברו שני משפטים עוקבים נתוניים, המודל התבקש לחזות את סדר המשפטים.

אחד החסרונות של MLM הוא צורך בכמות גדולה מאוד של דата, בעיקר כי הוא מאמן על חיזוי של טוקנים ממוסכים. עבודה מאוחרת יותר הצעה שיטה בשם ELECTRA שמנסה להתגבר על קשיי זה. ב-ELECTRA, במקומ לחזות טוקן המודל מנסה להיות האם הטוקן הוא ground-truth או טוקן אחר הנדגם ממודל שפה. לצורך זה מאמנים שני מודלים:

1. מודל שפה אוטורגרסייבי קטן יחסית שבונה התפלגות של הטוקן הבא, בהינתן הטוקנים הקודמים. מסווג זה נקרא הטרנספורמר המשני (auxiliary transformer) ומהווה MLM. המודל שהוצע בעבודה המקורית של BERT, הוא בעל פונקציית loss softmax.
2. מסווג ביןארי שתפקידו להבדיל בין הטוקן האמתי לבין טוקן שונה הנדגם מהטרנספורמר המשני. השכבה الأخيرة כאן היא סיגmoid. מודל זה נקרא הטרנספורמר העיקרי (main transformer).

הערה: בשיטת ELECTRA, רק טוקנים מומסכים נדגים מההתפלגות של הטרנספורמר המשני.

שני מודלים אלו מאומנים יחד. כך ניתן לאמן מודל שפה על כל הטוקנים ולא רק על הממוסכים ומתקיים אימון עיל יותר הדורש פחות DATA. המחברים מראים (במהלך) ביצועים טובים על מספר משימות downstream. עם זאת ELECTRA יש מספר חסרונות:

1. היעדר יכולת מובנית לגנרטוט שפה. הרוי המשימה של הטרנספורמר העיקרי היא דיסקרימינטיבית (סיווג) ולא גנרטטיבית. זאת אומרת כדי להפוך את הטרנספורמר העיקרי למודל שפה צריך להוסיף לו מנגנון מיידול שפה נפרד ולאמן אותו. המאמר טוען שימושה זו אינה פשוטה כי האופי הדיסקרימינטיבי מגבל את יכולתו של הטרנספורמר העיקרי ללמידה פיצ'רים הנחוצים לגנרטוט שפה.
2. ייצוג המשפטים המתกาלים עם ELECTRA מרכזים באוצר צר של המרחב הלטנטי שלהם וייצוג משפטי שאינו קשורם סמנטי, בהרבה מקרים, קרובים יותר אחד לשני (במונע של cosine (similarity) מאשר ייצוגים של משפטים בעלי משמעות דומה).

הרעין הכללי מאחריו המאמר:

המאמר מציע גישה הנקראת LM-COCO, המשלבת יתרונות של

1. MLM
2. הגישה הדיסקרימינטיבית של ELECTRA
3. גישה ניגודית (contrastive) לשיפור ייצוג של טקסט

הארכיטקטורה של LM-COCO דומה לאחת הוריאציות של ELECTRA, שנקראה All-Token MLM. שיטה זו משלבת את MLM עם הגישה הדיסקרימינטיבית ע"י שימוש בשני ראשים: הראשון דיסקרימינטיבי D, מיועד לזהות האם הטוקן, שנגdam מההתפלגות של הטרנספורמר המשני, הוא אמיתי (עם סיגמוואיד כשכבה אחרונה), ואילו השני G הוא מודל שפה שמחשב הסתברות לכל טוקן בהינתן הטוקנים הקודמים (עם softmax על מרחב כל הטוקנים בשכבה الأخيرة). פונקציית הלוס של ELECTRA שנבנית באופן הבא:

1. עבור הטוקן האמתי x_i ההסתברות הוא סכום משוקל של הסתברויות של המחשבות על ידי שני ראשים: $G(x_i) + D(x_i)$ כאשר $D(x_i) = 1 - G(x_i)$ הוא הפלט של הראש הדיסקרימינטיבי (סיגמוואיד).
2. עבור כל טוקן אחר, ההסתברות מחושבת לפי $G(x_i) - D(x_i)$.

פונקציית הלוס במקרה זהה מוגדרת באופן הבא (לקח לי זמן להבין אותה ועקב כך הוספה את ההסביר בפסקה הקודמת):

$$p_{\text{LM}}(x_i | \mathbf{h}_i) = \mathbb{1}(x_i = x_i^{\text{MLM}}) p_{\text{copy}}(1 | \mathbf{h}_i) + p_{\text{copy}}(0 | \mathbf{h}_i) \frac{\exp(\mathbf{x}_i^\top \mathbf{h}_i)}{\sum_{x_t \in V} \exp(\mathbf{x}_t^\top \mathbf{h}_i)}$$

$$p_{\text{copy}}(y_i | \mathbf{h}_i) = \exp(y_i \cdot \mathbf{w}_{\text{copy}}^\top \mathbf{h}_i) / (\exp(\mathbf{w}_{\text{copy}}^\top \mathbf{h}_i) + 1),$$

כאן y היא היצוג של ההקשר (הטוקנים הקודמים) הנוצר על ידי הראש הגנרטיבי G ו- w הוא וקטור נלמד. x_i^{MLM} מסמן טוקן שנדגם מההתפלגות המתקבלת מהטראנספורמר המשני ו- $\{0, 1\} \in y$ היא "ההחלטה" של הדיסקרימינטור (1 - טוקן אמיתי ו- 0 אחרית).

תקציר המאמר:

הפרדה של מידת המשימות:

למעשה פונקציית הלוס של ELECTRA מערבבת בין שתי המטלות: הדיסקרימינטיבית (הבחנה בין טוקן אמיתי לנדגם) והגנרטיבית (בנייה מודל שפה). מחרבי COCO-LM טוענים שמבנה זה של לוס מנסה על מנתה בזמנית של משימות אלו ומצביע להפריד אותם כך שכל משימה תילמד בנפרד עד כמה שאפשר. כלומר הלוס יורכב סכום של שתי פונקציות לוס שכל אחת מהן מתאימה למשימה:

$$\begin{aligned}\mathcal{L}_{\text{copy}} &= -\mathbb{E} \left(\sum_{i=1}^n \mathbb{1} \left(x_i^{\text{MLM}} = x_i^{\text{orig}} \right) \log p_{\text{copy}}(1|\mathbf{h}_i) + \mathbb{1} \left(x_i^{\text{MLM}} \neq x_i^{\text{orig}} \right) \log p_{\text{copy}}(0|\mathbf{h}_i) \right), \\ \mathcal{L}_{\text{LM}} &= -\mathbb{E} \left(\sum_{i \in \mathcal{M}} \log p_{\text{LM}} \left(x_i^{\text{orig}} | \mathbf{h}_i \right) \right) \\ &= -\mathbb{E} \left(\sum_{i \in \mathcal{M}} \log \left(\mathbb{1} \left(x_i^{\text{MLM}} = x_i^{\text{orig}} \right) p_{\text{copy}}^{\text{sg}}(1|\mathbf{h}_i) + p_{\text{copy}}^{\text{sg}}(0|\mathbf{h}_i) \frac{\exp(\mathbf{x}_i^\top \mathbf{h}_i)}{\sum_{x_t \in V} \exp(\mathbf{x}_t^\top \mathbf{h}_i)} \right) \right) \\ \mathcal{L}_{\text{CLM}} &= \lambda_{\text{copy}} \mathcal{L}_{\text{copy}} + \mathcal{L}_{\text{LM}}.\end{aligned}$$

קל לראות ש- L_{copy} היא פונקציית הלוס הקלאסית של סיווג בינארי, כאשר L_{LM} מותאם למידה של מודל שפה בלבד. x_i^{orig} מסמן את הטוקן האמיתי במקומות. שימוש לב Ci \mathbf{h} מופיע בביטוי עבור L_{LM} עם stop-gradient רק מעצור הגרדיאנט אומר ש- L_{copy} לא משתתף בחישוב הגרדיאנט ולא זורם דרכו. כלומר, \mathbf{h} מתעדכן רק מ- L_{copy} וכן כל משימה תילמד בנפרד.

הערה: ניתן להתייחס למשימת מזעור פונקציית הלוס L_{LM} כסוג של "תיקון" של סדרת טוקנים הרוסה (corrupted). הרשות מקבלת סדרת טוקנים שיכולה להכיל שגיאות, ומנסה "لتיקון" אותן ע"י שיווק הסתברות גבואה לטוקן האמיתי. במאמר, זה נקרא CLM - Corrective Language Modeling. למעשה "CO" הראשון בשם השיטה המוצעת COCO-ML בא מהמילה corrective.

מידה ניגודית על משפטים:

הלמידה הניגודית הפכה להיות גישה מאוד פופולרית בלמידה מפוקחת עצמית (self-supervised learning). המטרה של SSL היא ללמידה יציג לטנטי חזק שישמש לאחד מכון עבור משימות למידה שונות. הרעיון העיקרי מאחוריה הלמידה הניגודית הוא לבנות זוגות של דוגמאות קרובות (שנקראים זוגות חיוביים) וזוגות של דוגמאות לא דומות, שבדרך כלל נבחרות באקראי מהדאטasset.

המאמר מציע להשתמש בגישה זו וללמוד ייצוגי משפטים באמצעות הgesה הניגודית. אבל איך נבנה את הזוגות החשובים והשליליים? הזוגות מורכבים ממשפטים דגומים מהטראנספורמר המשני L_{MLM}^i וחלקיים של משפטיים אמיתיים (cropped sentences) - פשוט לוחצים תח-סדרה רציפה של הtokens מהטקסט האמיתי. הסדרות שנדגמו והויצו מאותו משפט מהווים זוגות חיוביים ואלו שנלקחו ממשפטים שונים (שנבחרו באקראי) מהווים הזוגות השליליים. פונקציית הלס הניגודי מוגדרת באופן הבא:

$$\begin{aligned}\mathcal{L}_{SCL} &= -\mathbb{E} \left(\log \frac{\exp(\cos(\mathbf{s}, \mathbf{s}^+)/\tau)}{\exp(\cos(\mathbf{s}, \mathbf{s}^+)/\tau) + \sum_{X^- \in B^-} \exp(\cos(\mathbf{s}, \mathbf{s}^-)/\tau)} \right), \\ &= -\mathbb{E} \left(\cos(\mathbf{s}, \mathbf{s}^+)/\tau - \log \left(\exp(\cos(\mathbf{s}, \mathbf{s}^+)/\tau) + \sum_{X^- \in B^-} \exp(\cos(\mathbf{s}, \mathbf{s}^-)/\tau) \right) \right)\end{aligned}$$

כאשר \cos מסמן דמיון מכפלה פנימית (cosine similarity) והטמפרטורה $1 = \tau$.

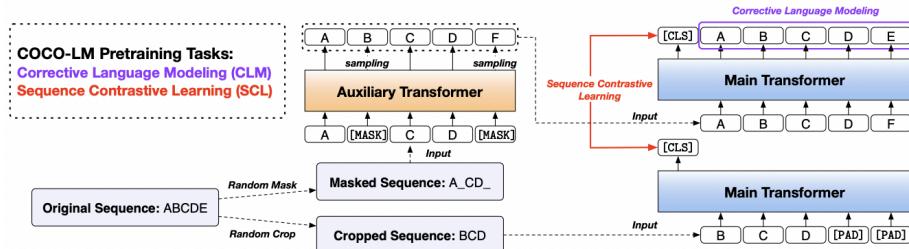


Figure 2: The overview of COCO-LM. The auxiliary Transformer is pretrained by MLM. Its corrupted text sequence is used as the main Transformer's pretraining input in Corrective Language Modeling and paired with the cropped original sequence for Sequence Contrastive Learning.

פונקציית הלס של LM-COCO היא למעשה סכום של 3 פונקציות לוס. הראשונה L_{MLM} היא הלס של מודל השפה המשני (auxiliary, שממומש ע"י טרנספורמר) ושני האחרים לוס על הטרנספורמר העיקרי של LM, והlös הניגודי L_{SCL} .

ביחד:

$$L = L_{MLM} + L_{CLM} + L_{SCL}$$

הישגי המאמר:

לצורך בוחנת ביצועי המודל מחברי המאמר פיתחו את מודל COCO-LM תחת שלוש וריאציות שונות של אימון מקדים, הנבדלות בינהן בכמות הנתונים הזמינים לאימון המקדים וארQUITקטורות שונות של הטרנספורמרם.

המחברים בוחנו כל אחד מהמודלים הנ"ל בעזרת מבחני GLUE (קבצת מבחנים שימושיים אמת מידת יכולות של מודלים ב-NLP), והם הושוו למודלים הותיקים RoBERTA, ELECTRA, BERT, שגם אומנו מחדש על ידי לצורך ההשוואה. בנוסף, המחברים השוו את ביצועי LM-COCO לתוצאות הסטנדרטיות שמקובלות ל מבחני GLUE.

השוואה ל מבחני GLUE

Model	Params	MNLI-(m/mm)	QQP	QNLI	SST-2	CoLA	RTE	MRPC	STS-B	Avg
Base/Base++ Setting: BERT Base Size										
BERT _{Base}	110M	84.6/83.4	89.2	90.5	93.5	52.1	66.4	84.8	85.8	80.8
ELECTRA _{Base++}	110M	88.5/88.0	89.5	93.1	96.0	64.6	75.2	88.1	90.2	85.6
COCO-LM _{Base++}	134M	89.8/89.3	89.8	94.2	95.6	68.6	82.3	88.5	90.3	87.4
Large/Large++ Setting: BERT Large Size										
BERT _{Large}	335M	86.7/85.9	89.3	92.7	94.9	60.5	70.1	85.4	86.5	83.2
ELECTRA _{Large++}	335M	90.7/90.2	90.4	95.5	96.7	68.1	86.1	89.2	91.7	88.5
COCO-LM _{Large++}	367M	91.6/91.1	90.5	95.8	96.7	70.5	89.2	88.4	91.8	89.3

Table 2: GLUE test set results obtained from the GLUE leaderboard. We perform hyperparameter search for each task with ten random seeds and use the best development set model for test predictions. All results are from vanilla single-task fine-tuning (no ensemble, task-specific tricks, etc.).

בשוואה של ביצועי מודל COCO-LM, בכל אחת מהוריאציות שלו, ביצועי המודל עלוי על ביצועי כל אחד מהמתחרים:

עלות ויעילות האימון (זמן GPU הנדרש לאימון המודל), COCO-LM הצליח להגיע לאחוזי דיק זחים למודלי ELECTRA ו RoBERTA תוך שימוש ב-50%-60% זמן ה-GPU.

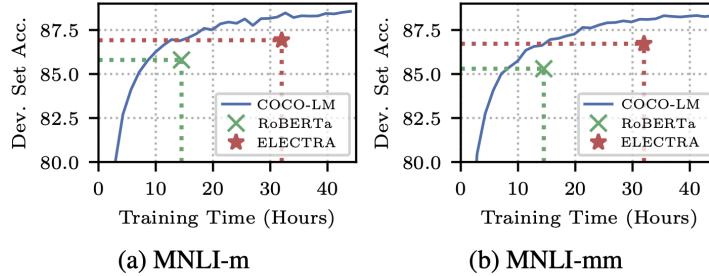


Figure 3: COCO-LM_{Base} on MNLI Dev. (y-axes) at different pretraining hours on four DGX-2 nodes (64 V100 GPUs). The final training hours and accuracy of RoBERTa (Ours) and ELECTRA (Ours) measured in the same settings are marked.

כמו כן, בבחינה של גרסת+ Large++ של COCO-LM המודל הציג ביצועים זחים למודל Megatron (בגראסאות של 1.3B ו- 3.9B פרמטרים) במבחן MNLI, תוך שימוש בפחות מ- 10% מכמות הפרמטרים של המודל.

מבחני ablation :

החדשניים המרכזיים במאמר הוו: הצגה של שתי פונקציות לואו חדשות למודל השפה, פונקציית לואו למידה ניגודית של רצפים (Sequence Contrastive Learning, SCL) ולואו למידה של מודל שפה מתקן (Corrective Language Modeling, CLM). בוחינת ההשפעה של כל אחד מהרכיבים הללו נעשתה על ידי מבחני ablation.

השפעת רכיב הלמידה הניגודית:

לצורך בוחינת השפעת רכיב הלמידה הניגודית (SCL) על ביצוע המודל, החוקרים בדקו את השפעת אחוז הקיצוץ (cropping) של הטקסטים וכן את השפעת הלמידה הניגודית על דמיון המשפטים.

החוקרים מצאו שקיצוץ של 10% מהמשפטים שהמודל במלבד הלמידה הניגודית, הביאה לביצועים הטובים ביותר של המודל (שיעור של בין 0.5 ל-0.7 נק' בציון הממוצע של מבחני GLUE בהשוואה לקיצוץ של 0% ו-30% בהתאם).

בנוסף, החוקרים בוחנו את ההשפעה של הלמידה הניגודית על ייצוג דמיון בין טקסטים. דמיון בין טקסטים נמדד באמצעות cosine similarity והוצג באמצעות הורדה של השיכונים המייצגים את הטקסטים למימד נמוך בעזרת שס-t.

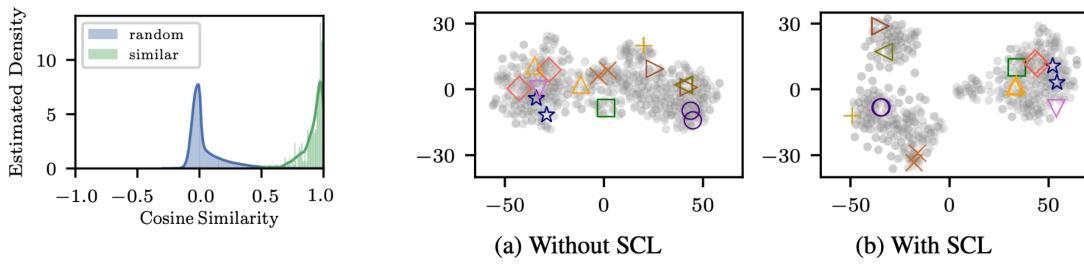


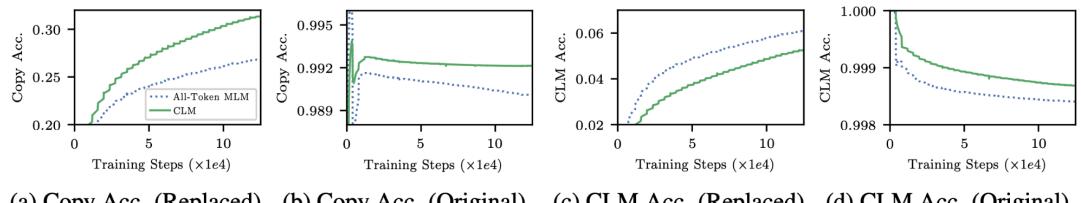
Figure 5: Cosine similarity of sequence pairs randomly sampled from pretraining corpus and most similar pairs from STS-B using [CLS] from COCO-LM_{Base}.

Figure 6: The t-SNE of sequence representations learned with or without SCL. The points are sampled from the most semantically similar sentences pairs from STS-B (with 5-score labels). The [CLS] embeddings are not fine-tuned. Some randomly selected similar pairs are marked by same shapes.

כפי שניתן לראות, הלמידה הניגודית הביאה למ מבנה יותר טוב של המרחב הלטוני, שבו טקסטים בעלי דמיון גבוה נוטים להתקבץ לקלאסטרים.

השפעת רכיב למידת מודל שפה מתוקן.

השפעה של רכיב למידת מודל השפה המתוקן (CLM) נעשה ע"י בוחנת דיקוק המודל במשימה של תיקון טקסט שהוחחת (corrupted), גם באחוז דיקוק כאשר המודל נדרש לתקן טוקנים שהוחחתו, וגם בשימור טוקנים קיימים (כאלה שלא הוחחתו והמודל נדרש רק להעתיק אותם למקום המתאים).



(a) Copy Acc. (Replaced) (b) Copy Acc. (Original) (c) CLM Acc. (Replaced) (d) CLM Acc. (Original)

Figure 8: The copying accuracy and the language modeling accuracy (*y*-axes) of CLM and All-Token MLM at different pretraining steps (*x*-axes, in 10K scale). The accuracy is averaged on tokens that are replaced by the auxiliary Transformer (Replaced) or those from the original input text (Original).

רכיב ה-CLM הראה שיפור הן ביכולת לתקן טוקנים שהושחתו, והן ביכולתו לשמר טוקנים, בהשוויה למודל מיסור סטנדרטי (MLM).

סיכום:

המאמר מציג מודל שפה חדש בשם LM-COCO, שעושה שימוש במודל שפה מתקנת ובלמידה ניגודית. המחברים מאננים מראים מודלים על רצפי טקסט פגומים, וכך מראים ש-LM-COCO עולה בכיצועיו על השיטות הקיימות במדדי GLUE, תוך כדי ניצול עיל יותר של משאבי מחשב ופרמטרי רשת.

הפօוט [נכט בערבי](#) ([מichael erlihson](#), PhD, Michael Erlhison) ו-[משה משען](#).

Review 17: CoMatch: Semi-supervised Learning with Contrastive Graph Regularization

פינת הסוקר:

המלצת קריאה ממיק: מאוד מומלץ.

בahirot כתיבה: בינוי פלאו

רמת היכרות עם כלים מתמטיים וטכניקות של DL/ML הנדרשים להבנת מאמר: הבנת העקרונות של למידה ניגודית (contrastive learning) וידע בסיסי בגרפים

ישומים פרקטיים אפשריים: הפקה של ייצוגים חזקים של דאטה עבור משימות של unsupervised/semisupervised learning

פרטי מאמר:

lienק למאמר: [זמן להורדה](#).

lienק לקוד: [זמן כאן](#)

פורסם בתאריך: 21.03.21, בארכיב.

הציג בכנס: לא הצלחתי לאתר

תחומי מאמר:

Semi-Supervised Learning (SmSL) •

כלים מתמטיים, מושגים וסימונים:

- Self-Supervised Contrastive Learning (SSCL)
- SSL/SmSL מבוסס על מינימיזציה של אנטרופיה
- SmSL המבוסס על גרפ של דמיונות
- פסאודו ליבלים (תוצאת הרצת רשות סיווג על דאטה לא מותיא)
- עברו פסאודו ליבלים
- יישור התפלגות (distribution alignment)

תמצית מאמר:

המאמר משלב 4 גישות פופולריות מעולמות של SSL ו-SmSL:

1. רגולרייזציה על בסיס עקביות:

שיטה זו מבוססת על הנחה שההסתברויות של ליבל עבור דוגמא נתונה לפני ואחרי אוגמנטציה, אמורים להיות קרובות. למשל בדומין של התמונות היגיון מאחורי גישה זו הימן מאד פשוט וטבעי: מכיוון שאוגמנטציה איננה משנה את התוכן של תמונה אלא רק את סגנוןיה, היא לא אמורה להשפיע על התפלגות פלט המטוגן. עקרון זה ניתן לתרגם למשל למינימיזציה של קروس-אנטרופי או מרחק ריבועי בין החיצויים של הדוגמה המקורית לגרסה שלה לאחר אוגמנטציה.

2. מינימיזציה של אנטרופיה של פלט המטוגן:

כאן אנחנו רוצים לבנות מסווג שמצויא "חיצויים בטוחים" לדוגמאות מהדעתהスト כולם כאלו של ליבל אחד מקבל הסתברות גבוהה ממשמעותית מכל האחרות. זה כמובן שկול למינימיזציה של אנטרופיה של פלט המטוגן. ניתן להשיג את זה בין השאר ע"י מינימיזציה של פלט הרשות עבור דוגמאות לא מותיגות (בצורה מפורשת) או ע"י בניית פסאודו ליבלים בעלי אנטרופיה נמוכה על דוגמאות לא מותיגות ואיימון של המטוגן עליהם.

3. Self-Supervised Contrastive Learning (SSCL):

הנחה הבסיס בגישה זו אומרת שיצוג חזק של דאטה(במרחב בממד נמור) מסוגל להפריד בין זוגות של הדוגמאות דומות לבין זוגות של דוגמאות רנדומליות. אחת הנסיבות הפופולריות של פונקציית מטריה במאמרי SSCL נקראת InfoNCE. ניתן להראות כי ככל שלios InfoNCE קטן יותר, המידע הדדי בין הדוגמא במרחב המקורי לבין ייצוגה במרחב מממד נמור עולה. זה כמובן מצביע על אובדן פחות אינפורמציה בין הדאטה המקורי לבין ייצוגה כلومר הייצוג יהיה פחות לוסי ומיצג את הדאטה בצורה מדויקת יותר. חשוב לציין שהאימון מתבצע במרחב הייצוג ולא במרחב המקורי, כלומר הלוס מחושב על ייצוגים במרחב מממד נמור. לעומת זאת זוג של דוגמאות קרובות (למשל שתי אוגמנטציות של אותה דוגמא) ומספר דוגמאות רנדומליות ומנסה למקסם את היחס בין אקספוננט של דמיון של הזוג הקרוב לסכום הדמיונות בין לבין דוגמאות רנדומליות.

4. SSL המבוסס על גרפ של דמיונות:

כאן בונים גרפ של דמיונות של דוגמאות מהדעתהスト כאשר קודקודים של דוגמאות קרובות (תחת איזושהי מטריקה - במרחב המקורי או במרחב של ליבלים) מחוברים עם קשת במשקל גבוה, כאשר הקודקודים של דוגמאות רחוקות מחוברים בקשות בעלות משקל נמור או לא מחוברות כלל. לאחר מכן מאמנים ייצוגים של דאטה במרחב מממד נמור תוך כדי התחשבות ב"טופולוגיה של הגרפ". ב�וילם אחרות דוגמאות קרובות אחת לשניה (מבחינת הגרפ) יאומנו לקבל ייצוגים קרובים.

הסבר של רעיונות בסיסיים:

המאמר מציע שיטה, הנקראת CoMatch, שלמענה בנויה על שילוב של 4 גישות אלו. CoMatch מנצלת את הייצוג של דוגמאות למרחב לטנסי (מייד נמור) Z ובמרחב הליבלים Q ומצבעת אימון בהתבסס על שני גורפים של דמיונות הנבנים בהתבסס על קשרים בין דוגמאות במרחבים אלו. נציין כי Q הינו מרחב הפלטים של רשות הסיווג כלומר הוא מכיל וקטורי הסתבריות של הליבלים.

از איך זה בעצם נעשה? קודם כל בואו נבין את המבנה של פונקציה הלוס של CoMatch.

פונקציית לוס:

נתחילה מזה שנזכר CoMatch הינה שיטה של LSms כלומר יש לנו דאטסהט עם דוגמאות מתוויות הנקרא X, והדאטסהט של דוגמאות לא מתוויות U. נסמן את הגרף שנבנה מעל המרחב הלטני Z ב- G_{emb} , והגרף על מרחב ליibiliים Q יסומן ב- G_{lab} . עכשו נוכל לעבור לתיאור הרעיונות העיקריים של המאמר:

המאמר מציע לאמן 3 רשותות:

- הרשות המקודדת f שבונה ייצוג מקדים של הדטה, המשמש גם כשלב מקדים לבניית של הייצוג Z גם לפועלות סיווג עצמה.
- רשות, הבונה ייצוג למרחב הלטני Z שמופעלת אחרי f, המסומנת ע"ג (פולטת ייצוגים מנורמליים).
- רשות סיווג h שמטרתה להוציא וקטורי הסתבריות של ליibiliים (גם מופעלת אחרי f).

כעת נתאר פונקציית לוס, המוצעת במאמר. היא מורכבת מ-3 חלקים:

1. **X_L**: קיטוט-Antroropi לוס רגיל על דוגמאות מתוויות. כאן הלוס מחושב על דוגמאות מתוויות בעברית אוגמננטציה חלשה. הלוס מחושב בין החיזוי של הדוגמא לאחר אוגמננטציה לבין הליבל של התמונה המקורית.

2. **Scls_L**: קיטוט-Antroropi לוס בין פסאודה ליibiliים של דוגמא לא מתוית לבין החיזוי עבור אותה דוגמא לאחר אוגמננטציה חזקה. נציין כי רק פסאודה ליibiliים מעלה סף מסוים נלקחים בחשבון בחישוב הלוס במטרה לא לקנוס את המודל על הדוגמאות שלא הצלחנו לבנות להם פסאודה ליibel "אמין", כולם בעל אנטורופיה נמוכה ([FixMatch](#)). על איך בונים את הפסאודה ליibiliים האלו נדון בפרק הבא.

3. **ctr_L**: הלוס הקונטרsty (בסגנון InfoNCE) הבוני על גрафי הדמיונות על מרחבי Z ו-Q. נסביר את המבנה של לוס זה בהמשך.

כעת בואו נתעמק באיך בונים את הפסאודה ליibiliים q הנחוצים לחישוב של $Scls_L$.

צורה של פסאודה ליibiliים:

קודם כל עברו דוגמאות מתוויות הפסאודה ליibel מוגדר בתור ליibel האמיתית (ground-truth) שלהם. על כל דוגמא לא מתוית מפעלים אוגמננטציה חלשה ומחשבים את ההתפלגות החזואה של הליבלים עבור כל אחת מהדוגמאות. לאחר מכן מבצעים "ישור התפלגות" (DA) שמיועד למנוע מהתפלגות הליבלים לקיטוט לתת-קבוצה של הליבלים. בשביל כך מחשבים ממוצע נוע w_k (על פני האיטרציות של אימון) על כל החיזויים של הדוגמאות הלא מתוויות. למעשה w_k המהווה שערור של שכיחות הליבלים בדאטסהט. לאחר מכן מחולקים את וקטורי ההסתבריות החזיות w_k של כל דוגמא ב- w_k . נציין שהדבל-מ-[ReMixMatch](#), וקטורי שכיחות הליבלים הנגזר מהדוגמאות המתוויות לא נלקח בחשבון כאן.

כעת מחשבים גם את הייצוגים הlatent'ים w_z של הדוגמאות ע"י העברתם דרך הרשת המקודדת f ורשת הייצוג g . שומרים w_z יחד עם וקטור התפלגות החזיות w_k במאגר של דוגמאות B . עתה נסביר איך מאנים רשות סיווג h , המשערת פסאדו ליבל b_q (התפלגות מעלה מרחב הליבלים) של דוגמה לא מתויגת. כדי לאמן את h , המאמר מנסה בעית אופטימיזציה עם פונקציית מטרה המורכבת מסכום קמור (עם מקדים המסתכניםים -1) של שני מחוברים. בפועל לכל אטץ' יש לנו סכום קמור של:

- סכום הריבועים של המרחקים של פלט הרשת המסווגת h (התפלגות מעלה ליבלים) עבור דוגמא w_n לבין הפלטים עבור כל הדוגמאות a_w מ- B , כאשר כל מרחק צה' משקל בדמיון המנורמל a_k בין הייצוג w_z של w_n לבין הייצוג latent'י של a_w . המטרה של איבר זה לקרב את התפלגות של פסאדו ליבלים עבור דוגמאות קרובות במרחב הייצוג. כאן דמיון בין הייצוגים מוגדר כאקסקפונט של המכפלה הפנימית בין הייצוגים (המנורמל בסכום של כל הדמיונות עבור הדוגמאות B).
- מרחק ריבועי בין חיזוי עבור דוגמה w_k לבין b_q (כדי לא לשנות את התפלגות פסאדו ליבלים יותר מדי)

לביעית אופטימיזציה זו יש פתרון מדויק זהה למעשה סכום משקל של w_k ו- a_k כאשר המקדם לפני a_k הוא הדמיון a_k .

החלק האחרון בפאלל שטרם התייחסנו אליו הינו הלוי $uctr_L$, המבוסס על גרפי דמיון מעלה מרחבי הייצוגים Z והלייבלים Q .

מבנה של $uctr_L$: לכל אטץ' בונים גרף lab_G מעלה מרחב Q כאשר משקל הקשת בין דוגמאות (קודקודים) מוגדר ע"י הדמיון (מכפלה פנימית) בין הפסאדו ליבלים של הדוגמאות (משקל של קשת עצמית מוגדרת להיות 1). אם ערכו של דמיון הוא קטן מסוף מינימלי, הקודקודים של דוגמאות אלו לא מחוברים. לאחר מכן בונים גרף G_{emb} מעלה מרחב הייצוגים. משקל קשת עצמית של קודקוד המתאים לדוגמא w ב- G_{emb} מוגדר כדמיון בין הייצוג של שתי אוגמנטציות חזקות של w (הדמיון הוא המכפלה הפנימית בין הייצוגים). הקשת בין כל זוג אחר של קודקודים מוגדרת כדמיון בין הייצוג של הדוגמא, המתאימה לקודקוד הראשון (לאחר אוגמנטציה חזקה) לבין הייצוג של הדוגמא מהקודקוד השני. לאחר מכן מנורמלים את הקשתות עבור שני הגרפים.

ועלכשו בא הקטע המגביב של המאמר (לפחות עיני) זהה בנית הלוי המשלב את שני הגרפים הללו. מאנים את את הייצוגים הדוגמאות שמהם נבנה גרף G_{emb} , כך שהוא (הgraf!!) יהיה כמו שייתר דומה מבחינה משקל' הקשתות ל- lab_G . לו זו מרכיב משני חלקיים:

- הלוי ניגוד' (contrastive) בין הקשתות העצמיות של lab_G . בדומה ללוויים ניגוד'ים דומים הוא דוחף את המודול לתת הייצוגים דומים לאוגמנטציות שונות של אותה דוגמא.
- החלק השני של הלוי "דוחף" הייצוגים של לדוגמאות עם פסאדו ליבלים דומים, להיות דומים (!!)(כלומר גורמים לקשת ביניהם ב- lab_G להיות בעל משקל גבוה). לדעתי זו אחת הנקודות הכי חשובות במאמר וגם הסיבה העיקרי לכך ש-CoMatch הצליחה להגיע לביצועים טובים.

הישג מאמר:

המאמר מראה שיפור בביצועים בכמה שימושות SmSL קלאסיות מעל שיטות עכשוויות כמו [FixMatch](#) ו- [MixMatch](#).

דאטהסטים: CIFAR100, STL10

ג.ב. המאמר מציע שילוב אלגנטי של 4 שיטות אימון מעולים LSMs. מאוד אהבתית את השילוב של גרפי דמיון מעל מרחבי ייצוג ומרחב הליבלים בחישוב של הLOS הניגודי. עם זאת המאמר הראה את עליונות של CoMatch רק על שני דאטהסטים יחסית קלים. הייתי רוצה לראות את ביצועיה של גישה זאת לדאטהסטים יותר מורכבים ומקרה שהוא יבוא בהמשך.

Review 18: Contrastive Learning Of Medical Visual Representations From Paired Images And Text

פינט הסוקר:

המלצת קריאה ממתק: חובה לעוסקים בתחום של צילום רפואי, לאחרים מומלץ מאוד.

בהירות כתיבה: גבוהה.

רמת היכרות עם כלים מתמטיים וטכניקות של DL/ML הנדרשים להבנת מאמר: היכרות עם טכניקות בסיסיות של למידת ייצוג (representation learning).

ישומים פרקטיים אפשריים: שיפור אינטואיטיביות של רשתות על דата מהדומין הרפואי.

פרטי מאמר:

lienק למאמר: [זמן-can](#)

lienק לקוד: [לא רשמי 1](#), [לא רשמי 2](#)

פורסם בתאריך: 02.10.2020, בארכיב

הציג בכנס: ICLR 2021

תחום מאמר:

- למידת ייצוג (representation learning) לצילומים רפואיים

כלים מתמטיים, מושגים וסימונים:

- Noise Contrastive Estimation - NCE
- Contrastive Visual Representation Learning from Text - ConVIRT

תמצית מאמר:

המאמר מציע שיטה בשם ConViRT (Contrastive Visual Representation Learning from Text), לבניית "יצוג במילד נמור (לטנטי) של צילום רפואי תוך שימוש בגישה הנקראית (Noise Contrastive Estimation) NCE). החידוש שבביא המאמר הוא שימוש ב-NCE לבניית "יצוגים עברו שני אופינים של צילום רפואי **בו זמן**: הראשון הוא ייצוג של צילום עצמו והשני הוא ייצוג של כתרתת (תיאור) טקסטואלי של הצילום.

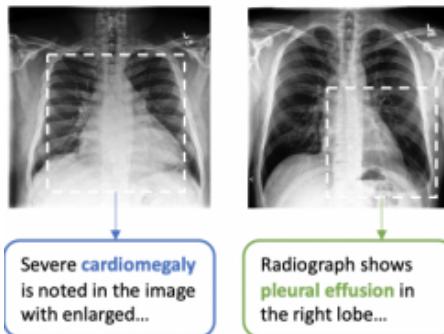


Figure 1: Two example chest radiograph images with different abnormality categories, along with sentences from their paired textual report and example views indicative of their characteristics.

רעיון בסיסי:

להבדיל מ-NCE המקורי המאמר מנסה לבנות "יצוגים של צילום ושל התיאור הטקסטואלי" שלו כך שהייצוג של צילום יהיה "דומה (קרוב) יותר" (אחרי טרנספורמציה מסוימת) לייצוג של תיאור הצילום שהוא מופיע עליו מאשר לתיאור של כל צילום אחר. באופן משלים כל ייצוג של תיאור צריך להיות כמה שייותר "קרוב" לייצוג הצילום שהוא מתאר מאשר לייצוג של כל צילום אחר (זו הסיבה המחברים קוראים לגישה שלהם דו-כיוונית במאמר. לדעתם של המחברים גישה "דו-כיוונית" זו מאפשרת להגיע לייצוג צילום המכיל בתוכו תכונות "סמנטיות חזקות מהתיאור שלו").

תקציר מאמר:

יצירת דאטאסתים מתוארים איקוטיים בעולם צילומי רפואיים היא יקרה מאד. רוב הדאטאסתים המתוארים הם לא גדולים שמקשה מאד על אימון מודלים (הכוונה לרשותות נוירונים) בעלי יכולת הכללה טובה. מצד שני ניסיונות להשתמש בייצוגים מאומנים על דאטאסתים מדומינניים אחרים (כמודל pretrained וכיוון על דאטאסטן קטן מהדומין הרפואי לאחר מכון) בדרך כלל לא מובילים לייצוגים חזקים בדומין הצילומים הרפואיים. הסיבה לכך היא הבדלים אינגרנטיים מהותיים בין האופינים של תכונות טבעיות בין צילומים רפואיים. מצד שני שימוש בגישה self-supervised לבניית "יצוגים בדומין הרפואי נתקלים גם כן בעקב הבדלים ויזואליים די קטנים בין צילומים רפואיים מקלאסים (קטגוריות) שונות).

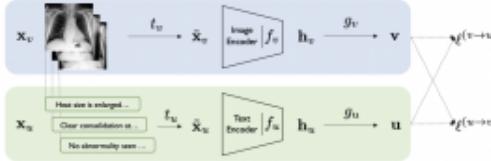


Figure 2: Overview of our ConViRT framework. The blue and green shades represent the image and text encoding pipelines, respectively. Our method relies on maximizing the agreement between the true image-text representation pairs with bidirectional losses $\ell^{(v \rightarrow u)}$ and $\ell^{(u \rightarrow v)}$.

כדי לחת מענה לשוגיה זו, המאמר מציע לנצל>Data טקסטואלי המופיע מעל צילומים רפואיים לבנייה של ייצוגים עשרים יותר. השיטה המוצעת במאמר - Contrastive Visual Representation Learning from text - ConViRT מנסה "לקרב" ייצוגים של צילום ותיאורו ו"להרחיק" עד כמה שניתן ייצוגים של זוגות אקראים של (צילום, תיאור). בעצם ConViRT מhhואה הרחבה "קרוס-דומיינית" (cross-domain) של NCE קלאסי. כולם ConViRT בונה ייצוגים בשני דומיינים שונים בו זמניות להבדל מ-NCE שעשו זאת בדומין אחד. למעשה הרחבה זו נותנת מענה לשוני ויזואלי קטן בין צילומים רפואיים מקטגוריות שונות, המקשה על שימוש ב-NCE סטנדרטי עבור דומיין זה. כפי שמקובל בדומיינים אחרים, מאמנים את ConViRT על כמה אדרהטים גנריים מהדומין הרפואי (pretrain) ולאחר מכן מכילים את המודול למשימת downstream (פין טיונינג).

הסבר קצר על NCE

בשביל להבין איך עובד NCE בשני דומיינים בו זמןית,בואו נזכיר מה זה NCE קלאסי. הנחת היסוד ב-NCE אומרת כי ייצוג חזק בהכרח "מסוגל להפריד" בין זוג דוגמאות קרובות (דוגמאות הקשורות או שתיהן אוגמנטיות של אותה דוגמא) לבין זוגות של דוגמאות רחוקות (כגון רנדומליות). כולם דמיין במרחב המקורי בין דוגמאות צריך להיות מתורגם למרחב הייצוגים שלהם. כולם ייצוגים של דוגמאות דומות צריכה להיות קרובות ואילו ייצוגים של דוגמאות לא דומות צריכה להיות רחוקים. בין השימושים של טכניקה זו ניתן למנות פונקציית loss (של דוגמא נתונה) העובר שהשתמשו בו לבנייה של word2vec. ניתן להוכיח כי הקטנות ערך של פונקציית loss (של דוגמא נתונה) בין כורה מסוימת של NCE (הנקראת InfoNCE), שבה גם משתמשים במאמר זה) מובילה לעלייה במידע הדדי בין הדוגמא במרחב המקורי לבין ייצוגה במרחב מממד נמוך. עלייה זו מבובן מabitעה על אובדן פוחות אינפורמציה בין דאטה מקורי לבין ייצוגה במימד נמוך לעומת הייצוג יהיה פחות לוטי ויכיל יותר מידע של הדוגמא. חשוב לציין שהאימון מתבצע במרחב הייצוג ולא במרחב המקורי כולם הloss מחושב על הייצוגים במרחב מממד נמוך.

اذ איך נראה פונקציית loss של NCE המקורי?

לדוגמא נתונה בונים זוג (חובי) של דוגמאות דומות (קרובות) 1_s ו-2_s (למשל אוגמנטיות של אותה תמונה). לאחר מכן בוחרים מספר דוגמאות רנדומליות ומרכזים זוגות מ-1_s ו-2_s עם הדוגמאות האלה. פונקציית מטריה היא היחס של דמיין של הזוג הקרוב (חובי) לסכום הדמיונות בין הדוגמאות רנדומליות (שליליות) והמטרה היא למקסם פונקציה זו. צריך לציין כי ככל יש מושגים יותר זוגות שליליים בפונקציית loss של NCE הוא גבוה יותר, ניתן להשיג ערך גבוה יותר מידע הדדי בין דוגמא וייצוגה במימד נמוך באמצעות מזעור של פונקציית loss (מקסום של פונקציית מטריה).

קרוס-דומיינית NCE של ConViRt

במקום לבנות זוגות מאותו דומיין ConViRt בונה זוגות מדומיינים שונים (מהדומין של תמונות ומהדומין הטקסטואלי). כולם לוקחים צילום וחלק מהתיאורו שלו ובוניםanza זוג חובי. אחר כך בונים זוגות רנדומליים של צילומים והתיאורים שלהם. מבובן משתמשים באוגמנטיות של צילומים לצורך לבנות זוגות חיובים. נגד לוקחים צילום, עושים לו crop ובונים זוג חיובי עם חלקים שונים של תיאורו (פושט דוגמים משפטים מתיאור הצילום באופן רנדומלי).

אחרי שbowנים את הזוגות החיבויים והשליליים מעבירים כל אחד דרך הרשת המקודדת שלו (אחת לצילום והשנייה לטקסט). לאחר מכן בונים מיני-באטץ המכיל זוג חיבוי אחד והשאר הם זוגות שליליים. את הצילום מעבירים דרך המקודד שלו (המאמר השתמש ב-ResNet50) ואת הטקסט מעבירים דרך המקודד שלו (כמו שאתם יכולים לנחש זה לא אחר אלא BERT). לאחר מכן לוקחים את הפליטים של שני המקודדים האלה ו"מטילים" אותם על מרחב מאותו מיד כדי שנitin יהיה להשוותם (מעבירים את שניהם דרך רשת בעלת שתי שכבות - מבון כל אחד מועבר דרך הרשת שלו). לאחר מכן מחשבים דמיון בין הפליטים באמצעות מרחוק הקוסינ' (cosine). בשלב האחרון מציבים את המרחקים האלה לשתי פונקציות לוס של InfoNCE: בראשונה המכנה מכיל את סכום אקספוננטים של כל המרחקים בין כל הזוגות המכילים את התיאור מהזוג החיבובי וצלומים רנדומליים כאשר השני מכיל את המרחקים בין הצלום מהזוג החיבובי לשאר התיאורים מהמיני-באטץ. המונה בשני האיברים הוא המרחק בין הייצוגים של הזוג החיבובי. הלווס הסופי הינו סכום של שני הלוסים האלה.

הישגיו מאמר:

המחברים ביצעו אימון pretrain של ConViRT על שניatasets: MIMIC-CXR, ועל הדאטאסת rhode island hospital-musculoskeletal. לאחר מכן כילו את המודל המאומן לכמה סוגים של שימושות:

Table 1: Results for the medical image classification tasks: (a) linear classification; (b) fine-tuning setting. All results are averaged over 5 independent models. Best results for each setting are in boldface. COVIDx 1% setting is omitted due to the scarcity of labels in COVIDx.

Method	RSNA (AUC)			CheXpert (AUC)			COVIDx (Accu.)			MURA (AUC)		
	1%	10%	all	1%	10%	all	10%	all	1%	10%	all	
<i>General initialization methods</i>												
Random Init.	55.0	67.3	72.3	58.2	63.7	66.2	69.2	73.5	50.9	56.8	62.0	
ImageNet Init.	82.0	85.4	86.9	75.7	79.7	81.0	83.7	88.6	63.8	74.1	79.0	
<i>In-domain initialization methods</i>												
Caption-Transformer	84.8	87.5	89.5	77.2	82.6	83.9	80.0	89.0	66.5	76.3	81.8	
Caption-LSTM	89.8	90.8	91.3	85.2	85.3	86.2	84.5	91.7	75.2	81.5	84.1	
Contrastive-Binary	88.9	90.5	90.8	84.5	85.6	85.8	80.5	90.8	76.8	81.7	85.3	
ConViRT (Ours)	90.7	91.7	92.1	88.9	86.6	87.3	85.9	91.7	81.2	85.1	87.6	
<i>(a)</i>												
Method	RSNA (AUC)			CheXpert (AUC)			COVIDx (Accu.)			MURA (AUC)		
	1%	10%	all	1%	10%	all	10%	all	1%	10%	all	
<i>General initialization methods</i>												
Random Init.	71.9	82.2	88.5	70.4	81.1	85.8	75.4	87.7	56.6	61.6	79.1	
ImageNet Init.	85.1	87.5	90.8	80.1	84.8	87.6	84.4	90.3	72.1	81.8	87.0	
<i>In-domain initialization methods</i>												
Caption-Transformer	89.2	92.1	91.5	81.5	86.4	88.2	88.3	92.3	75.2	83.2	87.6	
Caption-LSTM	87.2	88.0	91.0	83.5	85.8	87.8	83.8	90.8	78.7	83.3	87.8	
Contrastive-Binary	87.7	89.9	91.2	86.2	86.1	87.7	89.5	90.5	80.6	84.0	88.4	
ConViRT (Ours)	88.8	91.5	92.7	87.0	88.1	90.3	92.4	91.3	86.5	89.0		
<i>(b)</i>												

1. סיווג צילום

.RSNA Pneumonia Detection, CheXpert, CovidX, MURA datasets:

2. מציאת צילום דומה ביותר לצילום נתון (Zero-shot Image-image Retrieval).

Dataset: CheXpert 8x200 Retrieval Dataset

3. מציאת צילום��י דומה לתיאור נתון (Dataset סט כמו הקודם)

בכל המשימות האלה הצלחו המבקרים להשיג ביצועים טובים יותר עם השיטה המוצעת בהשוואה למגוון שיטות pretraining אחרות.

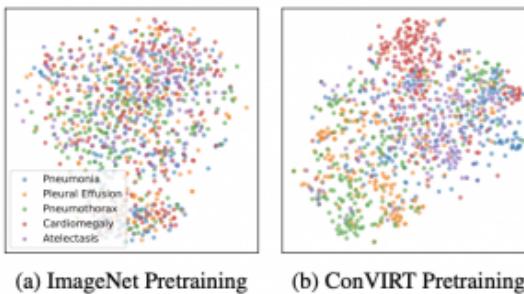


Figure 3: t-SNE visualizations of encoded image representations from different pretraining methods.

ג.ב. מאמר עם רעיון מגניב להתגבר על קשיי בبنית ייצוגי צילומים בתחום הרפואי. כתוב מאד ברור ומדויק.
מומלץ!

Review 19: Deep VULMAN: A Deep Reinforcement Learning-Enabled Cyber Vulnerability Management Framework

פינט הסוקר:

המלצת קרייה מעדן ומיק: מומלץ לעוסקים בתחום ה-*Reinforcement learning* ו**Cybersecurity** ו**Machine Learning**.

בהירות כתיבה:

ידע מוקדם: Reinforcement Learning

ישומים פרקטיים אפשריים: Cyber Vulnerability Management

פרטי מאמר:

لينك لمقالة: [זמן להורדה](#)

لينك לקוד: אין

פורסם בתאריך: 3.10.22, בארכיב.

הציג בכנס: Artificial Intelligence (cs.AI); 2022

תחומי מאמר:

- למידת חיזוקים عمוקה (Deep Reinforcement Learning)
- ניצול משאבים אופטימלי
- תכנון מספרים שלמים (integer programming)

ישומים:

- טיפול יעיל יותר בחולשות במערכות תוכנה תחת אילוץ משאבים מוגבלים

מבוא:

ארגוני מותקפים מדי יום על ידי תוכנים שמנסים לנצל חולשות בראש הארגונית במטרה לגרום נזק לארגון. כדי להילחם בתופעה, על אותם ארגונים לנסות לזהות את החולשות ולתקן אותן לפני שהן מנוצלות על ידי התוקפים. מציאת חולשות הינה משימה קשה, שכן מספר המשאבים המוגבל המוקצה לתיקון חולשות (למשל מחסום באנשי IT) לעיתים קרובות. קושי נוסף הינו מספר המשאבים המוגבל המוקצה לתיקון חולשות (למשל מחסום באנשי IT) שمبرושים שדרוגים למערכות ישנות בעלות חולשות). כתוצאה לכך, חולשות מסוימות לא מטופלות בזמן ומונצחות על ידי תוכנים שמצילים לגרום נזק רב לארגון.

תרחיש זה מעלה את הצורך בהיליך ניהול אוטומטי של מציה ותיקון חולשות. תהליך זה מתחילה על ידי תוכנות ששורקות את הרשות אחר חולשות מוכרות (למשל כאלו הנמצאות בסיס הנתונים [NVD](#)). סריקה כזו תחזיר כפלט דוח המכיל את החולשות שהתגלו ומאפיינים נוספים כגון: המכמה אליה נמצאה החולשה, תיאור החולשה וכדומה. צוות אבטחת הסיביר של הארגון (CSOC) משתמש בדוח זה כדי להקצות משאבים לצורך תיקון החולשות. תהליך זה של הקצת משאבים מבוצע היום בצורה ידנית או על ידי מערכת חוקים. שיטות כאלו אינן מספקות שכנון לא מתחשבות במגוון גורמים כגון מאפיינים של המערכת אליה נמצאו החולשות. כתוצאה לכך, ניתן מצב שבו משאבים הוקצו לטפל בחולשות פחות קritisיות.

במאמר שנסקור היום, החוקרים מציעים שיטה אשר מتبוססת על שילוב של למידת באמצעות חיזוקים (RL) ותוכנות מספרים שלמים (integer programming) כדי לחתם מענה לשוגיה זו. סוכן RL-RL מקבל את מספר המשאבים מסוכן RL-RL כאשר הינטן האילוץ וטוש החולשות הקיימות, ונסה לבחור את החולשות הקritisיות ביותר שיטופלו על ידי המשאבים שנבחרו.

השיטה המוצעת נקראה **Deep VULMAN** ומטרתה לזהות את החולשות החשובות ביותר שצריכות טיפול בזמן אמת תחת אילוצי משאבים וחוסר ודאות לגבי חולשות חדשות שיכולות להתגלות בעתיד.

הסבר על השיטה:

הסבירה:

כדי ללמד את המדיניות האופטימלית להקצת המשאבים יש צורך בסביבת סימולציה אשר תהיה דומה ככל האפשר לסביבה האמיתית אותה יראה הסוכן במערכות ארגונית לאחר סיום האימון. יצירת סביבה כזו הינה משימה קשה שכן דатаה המתאראת תהייל כי טיפול בחולשות במערכות תוכנה (כגון סוג החולשה, הצוין שלה, מספר

המשאים והזמן שהוקצו לטיפול בה) לא נגיש לציבור הרחב. כדי להתמודד עם הבעיה, החוקרים שיתפו פעולה עם צוות CSOC בארגון גדור (לא ציין שם הארגון מתאימים פרטיות המידע) ומהדатаה שנאסף מארגון זה הכותבים יצרו סימולציה של הסביבה. במצב אמת לא ידוע לנו מתי חולשה מסוימת תגלה על ידי סורקי החולשות וכן החוקרים סימלצוו 3 מצבים שונים של הגעת חולשות למערכת: איטי,BINONI וגובהה. הסביבה מחליפה ביניהם באופן רנדומלי ובנוסף בכל נקודת זמן חולשות שונות נדגמות מהדטה ההיסטורית.

סוכן RL:

סוכן RL הינו אחראי על הקצאת המשאים לטיפול בחולשות. בעיית הקצאת משאים במערכות תוכנה טומנת בה מרכיב של חסר ודותות. למשל אם נקצתה 8 מטר 8 המשאים שלו לטיפול ב-8 חולשות ביום מסוים ויום למשך יתגלו 10 חולשות חדשות שחיבות טיפול מיידי נהיה בעיה. הכותבים מציעים לפטור בעיה זו באמצעות טכניקת של RL.

בעיית הקצאת משאים מודולת באמצעות תהליך קבלת החלטות מרקובי (MDP). בתהליך זה יש צורך בהגדירה של משתנים הבאים: מצב, תגמול, פעולה ומטריצת המעברים בין מצבים, שהוגדרו במחקר זה באופן הבא:

- **מצב** - המצביע את המידע שזמן לsocion בזמנ t. CAN מידע זה מכיל מאפייני החולשה כגון: קריטיות החולשה, רמת החשיבות של המcona עליה התגלשה, האם החולשה התגלתה על ידי מערכות ההגנה של הארגון וציון CVSS-[שלמה](#).
- **פעולות** - הפעולות שהsocion יכול לבצע בזמן t: להקצות משאים נוספים או לא להקצות משאים כלל. כלומר, הפלט הינו מספר בין 0 למספר המשאים המקסימלי.
- **מטריצת המעברים** - מידול ההסתברויות של מעבר ממצב במצב בעיה זו הינה משימה קשה ולכן החוקרים החליטו לא לעשות זאת בצורה מפורשת.
- **תגמול:** הדרך של הסוכן לדעת האם הפעולה שביצעה בזמן t הינה טובאה או רע. בעיה זו התגמול הוגדר להיות לפי הנוסחה הבאה:

$$r_t = w_1 * r_t^1 + w_2 * r_t^2$$

כאשר r_t^1 קריטיות החולשה שתוקנה ו- r_t^2 הוא מספר המשאים שנוצלו בזמן t. שתי המשקלות w_1 ו- w_2 הין פרמטרים השולטים בחישוב היחסית של כל תגמול.

הSOCN בו השתמשו הכותבים משתמש באלגוריתם [PPO](#) לאיתור המדיניות האופטימלית להקצאת המשאים. אחת הסיבות לשימוש בגישה זו היא גודל עצום של מרחב המצבים והפעולות האפשרות שלא מאפשר שבירתם בזיכרון. כתוצאה לכך אי אפשר להשתמש בשיטות סטנדרטיות כגון [Q-Learning](#) בשביל למידת a(Q). כדי להתגבר על סוגיה זו החוקרים משתמשים ברשת נירונים לשערוך של a(Q) בצורה מקוונת.

מודל תכנון מספריים שלמים (integer programming):

בעיה של בחירת cholשות שיטופולו, בעזרת המשאים שהוקצו על ידי סוכן ה-RL, מנוסחת במאמר כביעה אופטימיזציה קומבינטורית. משתני אופטימיזציה i הם בינהירים כאשר ערך 1 מסמן שהמשaab נבחר לטיפול

בחולשות ו-0 מסמן שמשאב זה לא נבחר. פונקציית המטרה כאן היא האימפקט הכללי על המערכת בעקבות טיפול בחולשות שיבחרו; ואת האימפקט זהה מנסים למקסם. בambilים פשוטות אלו מנסים לתקן כמה שיותר חולשות בעלות מאפיינים קרייטיים עם המשאים שהוקצו על ידי סוכן-RL.

כעת נעבר לניסוח המתמטי של הבעיה. פונקציית המטרה מוגדרת באופן הבא:

$$y = \text{Max} \frac{\sum_{j=1}^J \sum_{i=1}^I v_{ij} * z_j}{\sum_{j=1}^J z_j}$$

כאשר v_{ij} הינו ערך (חשיבות) של מאפיין $I, \dots, 1 = i$ של חולשה $J, \dots, 1 = j$. כאן I מסמן את מספר המאפיינים של החולשה כאשר J הוא המספר הכללי של החולשות. למעשה פונקציית המטרה של ה"חשיבות הממוצעת" של כל החולשות שטופלו פר משאב שהוקזה לטיפול.

הailoz נראה כך:

$$\sum_{j=1}^J S_j * z_j \leq a_t$$

כאשר S_j הוא הזמן שנדרש לתקן של חולשה j ו- a_t הוא משך זמן המשאים, המוקצים באמצעות סוכן RL, שזמןנים לנו. המשמעות של ailoz זה היא לא לאפשר להקצות משאים ליותר זמן מהם מוקצים לנו. נזכיר כי המטרה כאן היא למצוא קומבינציה של ערכי i מהמקסימים את פונקציית המטרה ומקיימים את ailoz.

המחברים פותרים בעיית אופטימיזציה זו באמצעות גישת הנקראט תכונות מספרים שלמים. שיטה זו היא משפהה של שיטות מתמטיות שמטרתן היא לפתור בעיות אופטימיזציה כאשר חלק מה משתנים הם דיסקרטיים, למשל יכולם לקבל ערכים טבאיים בלבד. בעיות כאלו הן בדרך כלל קשות הרבה יותר מביעות אופטימיזציה עם ailozים בהן כל המשתנים הם רציפים.

תרשים כללי של המערכת:

כאשר מגיעה חולשה חדשה, המאפיינים שלה נשלפים ממסד הנתונים הנחוצים להגדרת המצב (state) שלה. מצב זה נכנס כקלט לסוכן-RL שמחשב את מספר המשאים שצריך להקצות בנקודת זמן זו, כדי להתמודד עם כל החולשות שהתגלו. פלט זה נכנס כקלט למודל התכונן המספרים השלמים שמצויא כפלט רשיימה של חולשות הדורשות מענה מיידי. החולשות מתוקנות ותגמול מחושב עבורן מזוזם חוזה לסוכן-RL והתהילך חוזר על עצמו עד התכוננות.

סביבת האימון:

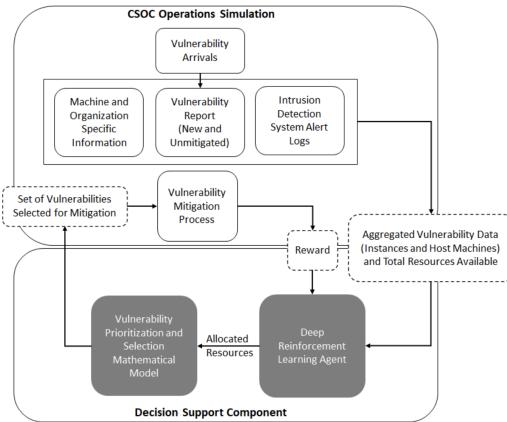


Figure 1: Deep VULMAN Framework for Cyber Vulnerability Management.

החוקרים שיתפו פעולה עם צוות ה-CSOC של ארגון גדול, (מטרי אבטחה שלו לא נחשף), כדי לקבל גישה לדאטה שלו. הדאטה הכליל מידע על חולשות שהתגלו בארגון במשך שנתיים כדוגמת: תיאור החולשה, CVSS ציון, קריטיות החולשה וקודמה. בנוסף, הדאטה כולל מידע על מכונות ברשות. לבסוף, נאספו גם התראות שעלו מכל הגנה שונים של הארגון (IDS). כל אלו שימושו את החוקרים ליצור הדאטasset של החולשות שעלו ביסוסו הכותבים את מחקרם. החוקרים הפעילו מנגנון preprocess שככל מתן ציון נומריע לעל:

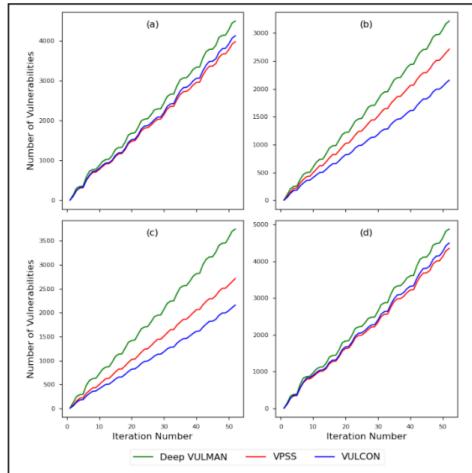
- חשיבות מכונה (למשל מכונה שעלייה יושב SQL DB תקבל ציון גבוה יותר מחשב אישי רגיל).
- דרגת ההגנה של מכונה (למשל האם קיימ אנטי וירוס על המכונה, האם היא מאחוריו חומת אש וקודמה).
- חשיבות המכונה כלפי הארגון (לא ציון מה זה כולל או איך חשוב).

מדאטasset זה החוקרים יוצרים סביבת סימולציה המדמה סביבת CSOC אמיתית. קצב הגעת החולשות למערכת מודל על ידי התפלגות פואסן, התפלגות שנuada למدل תהליכי התרחשויות של אירועים בלתי תלויים בקצב הגעה ממוצע קבוע. קצב הגעת החולשות השתנה כל שבוע והוא לאחד מבין המודדים הבאים: נמוך, בינוני, גבוה.

נזכיר כי כאשר משאב מסוים נבחר לטיפול בחולשה מסוימת על ידי Deep VULMAN, הוא (המשאב) יהיה תפוק עד שלא יסימן לטפל בה ועד אז אי אפשר להשתמש בו לטיפול בחולשות אחרות.

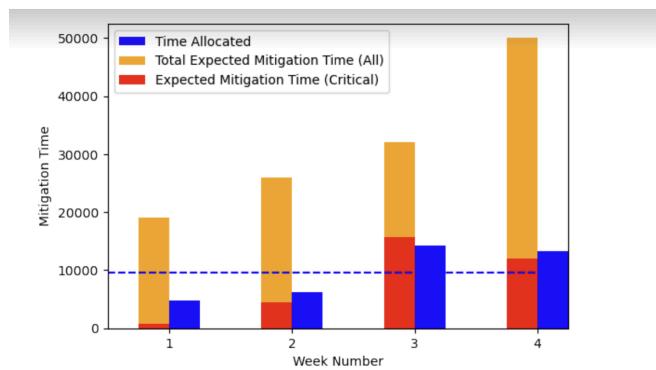
הישגי מאמר:

הגישה המוצעת השווה מול שיטות אחרות של בחירת חולשות לטיפול. השיטות שנבחנו להשוואה זו הינם: VPSS, VULCON ושלפי הספרות מהוות את השיטות הנפוצות ביותר (משמעות הדבר שהיא מושגתה בתיאור של הגרפ = שבוע). ההשוואה בין השיטות כאן מתבצעת על בסיס כמה אונומליות המטופלות.



- מצב a מתאר את מספר החולשות שנאספו ממכונות בעלי חשיבות גבוהה.
- מצב b מתאר את מספר החולשות שנאספו ממכונות בעלי חשיבות נמוכה.
- מצב c מתאר את מספר החולשות שנאספו ממכונות בעלי חשיבות לארגון (כלומר סובייקטיבית לארגון ולא אובייקטיבית כמו מצב a).
- מצב d מתאר את מספר החולשות שנאספו ממכונות שעליין על התראות מערכות ההגנה השונות.

התוצאות מראות בבירור שככל שלב ובכלי סביבה VULMAN הצלחה ל汰עד יותר חולשות קריטיות מאשר השיטות האחרות. כתבי המאמר מצבעים על כך ש-VULMAN השיגה את התוצאות הנ"ל על דата אשר לא התאמנה עליון.



בشرطוט הנ"ל ניתן לראות סימולציה של חודש ימים כאשר בכל שבוע קצב הגעת החולשות משתנה. למשל קצב הגעת החולשות בשבוע הראשון נמוך מהשבוע השני. העמודה הכתומה מתארת את הזמן הצפוי הנדרש לטיפול בכל החולשות שהתגלו באותו שבוע והעמודה הכהולה מתארת את מספר המשאבים ששוטק ה-RL הקצה כדי להתמודד עם אותן חולשות. העמודה האדומה מתארת את מספר החולשות שסומנו כקריטיות מתוך סך החולשות באותו שבוע. לבסוף הקוו הכהול מתאר מצב תיאורטי בו התפלגות הקצאת המשאים היא אחידה בין השבועות. אסטרטגיה זו של התפלגות אחידה היא מה שנוהג בשיטות האחרון (VPSS & VULCON).

מהתוצאות ניתן לראות כי בשבוע הראשון VULMAN הקצה פחות משבבים כדי להתמודד עם קצב הגעת החולשות ממשום שהוא שקצב זה הוא נמוך ואין צורך בהקצת כל במשבבים. אסטרטגיה זו השתלמה שכן בהמשך קצב הגעת החולשות התרגבר ול-VULMAN היא יותר משבבים פנויים להשתמש וכן הוא ניצל את רובם כפי שניתן לראות בשבוע 3 ו-4.

סיכום:

במאמר הוצגה מערכת VULMAN, המיועדת לזהות ודרוג חולשות במערכות תוכנה בארגון כדי שיוכלו לקבל טיפול תחת אילוץ של מספר משבבים (לטיפול החולשות) מוגבל. הגישה המוצעת כוללת שימוש בסוקן RL שמאומן להקצות את המשבבים באופן אופטימלי. בנוסף משתמשים ב-Integer Programming לבחירה את התראות(חולשות) שדרושות טיפול מיידי. הניטויים והמידע שנאוסף היו בשיתוף עם צוות CSOC בארגון גדול וביבת הסימולציה שנבנתה מדמה כיצד אמינה את המתරחש במערכות תוכנה של ארגון. הניטויים מראים ש-VULMAN לומד כיצד לקבל החלטות "מושכלות" בסביבה בעלת חוסר ודאות גבוהה כמו סביבת CSOC שנבע מיכולתו להקצות משבבים בצורה חכמה יותר מאשרות האחרות.

שיטת פעולה: הסקירה נכתבת יחד עם עדן יבן.

Review 20: DETReg: Unsupervised Pretraining with Region Priors for Object Detection

פינת הסוקר:

המלצת קריאה ממיק: חובה לעסוקים בזיהוי אובייקטים בתמונות.

בהירות כתיבה: גבוהה.

רמת היכרות עם כלים מתמטיים וטכניקות של DL/ML הנדרשים להבנת מאמר: נדרשת היכרות עם DeTR, שיטות למידת יציג בצורה unsupervised וטרנספורמרים.

ישומים פרקטיים אפשריים: שימוש pretraining של מודל לזהות אובייקטים בדומיינים עם כמות מועטה של דата מתויג.

פרטי מאמר:

[lienek למאמר: זמן להורדה](#).

[lienek לקובץ: זמן כאן](#).

פורסם בתאריך: 21.06.08, בארכיב.

תחומי מאמר:

- זיהוי אובייקטים בתמונה (Object Detection)

ידע מוקדם:

- למידת יציג של>Data לא מותיג (representation learning)
- [Region proposals](#)
- [Detection with transformers \(DETR\)](#)
- סקירה של עברית, [SwaV2](#) (סקירה של רחל שלום באנגלית)
- טרנספורמרים למשימות הראייה הממוחשבת (בפרט למשימות זיהוי אובייקטים)
- [Selective Search](#)
- אלגוריתם התאמת הזוגות ההונגרי ([Hungarian bipartite matching algorithm](#))

מבוא:

זיהוי אובייקטים בתמונה הינה משימת ראייה ממוחשבת קלאסית שמטרתה איתור מקום של אובייקטים בתמונה בנוסף לזיהוי הקטgorיה של כל אובייקט. בדרך כלל נדרש דאטהסט מותיג גדול כדי לאמן רשת לזיהוי אובייקטים בתמונה בדיק גבורה (הדיוק מתייחס גם למיקום וגם לקטgorיה של האובייקטים). דאטהסט מותיג לשימוש זיהוי אובייקטים מכיל תמונות עם bounding boxes (BB) לכל אובייקט והקטgorיה שלו כאשר מסpter האובייקטים בתמונה עשוי להיות די גדול. בניית דאטהסטים אלו יכולה להיות עסוק די יקר. עקב כך נוצר צורך בبنית יציגים טובים של תמונות שנitinן ללמידה אוטומטית בקרה (קרי ללא דאטה מותיג) לצורך pretraining של מודל לזיהוי אובייקטים. יציג "טוב" של תמונה בקרה להקטין בקרה משמעותית גודל דאטהסט הנדרש לאימון (למעשה לכיו- fine-tuning) של מודל לזיהוי אובייקטים.

בשנים האחרונות יצאו מחקרים רבים המציעים שיטות למידת יציג של תמונה ללא דאטהסט מותיג. לעומת זאת המאמר שיטות אלו לא מצליחות לבנות יציג של תמונה שהוא "מושוגט" לשימושו של זיהוי אובייקטים. ככלומר יציגי תמונות הנבנימים באמצעות הקיימות לא מצליחים "לדחוף" כמהות מספקת של "מידע רלוונטי" לזיהוי אובייקטים בתמונה לocketor היציג של התמונה. יתרון שהסיבה לכך היא שונות גדולה בין אופיים של תהליכי למידת (אימון) יציג supervised של תמונה לבין תכונות הנחוצות (במאמר קוראים להם תכונות object) בעבר משימת זיהוי אובייקטים. בגודל המתרה של שיטות אימון של יציג supervised הקיימות היא "לקרב" יציגים של תמונות דומות ולהרחיק יציגים של תמונות לא דומות. נראה יציג בעל תכונה זו לא מכיל מספיק מידע רלוונטי לשימוש זיהוי אובייקטים.

למייבן ידעת, לא קיימת שיטה לבניית יציג של תמונה בקרה supervised, המאומנת על משימה "דומה" לזריהוי אובייקטים.

תמצית מאמר:

המאמר הנזכר מציע שיטה, הנקראת DETReg לבניית יציג של תמונה כך שהוא יוכל מידע רלוונטי לשימוש זיהוי אובייקטים (כלומר מידע על מיקום וסוג האובייקט). השיטה המוצעת היא למעשה זיהוי אובייקטים בתמונה.

אבל איך ניתן לבנות משימה כזו כאשר אין ברשותנו נתונים מותיגים? המחברים השתמשו בשיטה קלואסית (שהוצעה עוד ב-2013) לזרוי אובייקטים בתמונה הנקראת [Selective Search](#) או בקיצור SS. המאמר מציע לנצל BB-ים (ללא קטגוריה של אובייקט) המחשבים באמצעות SS למטרת pretraining של DETReg.



Figure 1: **Prediction examples of unsupervised pretraining approaches.** Recent methods, shown in (a) and (b), do not learn “objectness” during the pretraining stage. In contrast, our method DETReg (c) learns to localize objects more accurately in its pretraining. The included prediction examples were obtained after pretraining and before finetuning with annotated data.

אבל זה לא מספיק בשביל לאמן ייצוג חזק לזרוי אובייקטים! צריך לזכור כי המטרה של אימון הDETReg היא לבנות ייצוג של תמונה המכיל אינפורמציה על מיקומים ועל סוגים של האובייקטים בתמונה (זו למעשה המטרה של משימת זרוי אובייקטים). מידע על מיקום האובייקטים מועבר באמצעות BB-ים המסופקים באמצעות SS. סעיף נשאלת השאלה איך “להעביר מידע על **סוג האובייקטים** ליצוג התמונה” במהלך הDETReg? המאמר מציע מונסה לכפות על ייצוגים של BB-ים (שהם למעשה פאצ'ים של תמונה), הנבנים באמצעות Reg להיות קרובים לייצוגים של BB-ים המוצעים ע”י SS.

אבל באיזה ייצוג נשתמש כדי “להעביר” ל-DETReg את האינפורמציה על סוג האובייקט בכל BB? צריך כי שיטות supervised מצליחות להפיק ייצוג של תמונה המכיל מידע על סוג האובייקטים בתמונה. למעשה ייצוגים של תמונות עם אותו סוג של אובייקטים (שייכים אותה קטגוריה) “קרובים” במרחב הייצוג כאשר אלו של התמונות מקטגוריות שונות רחוקים יותר. למעשה ייצוגים של תמונות מאותו אוסף קטgorיה מהווים קלאסרים למרחב הייצוג והקלאסרים של קטגוריות שונות “מופרדים” זה מזה.

המאמר בחר בשיטה הנקראת Swa-V ליצוג של BB-ים המופקים באמצעות SS. ד”א, [סקרטיה מאמר זה בעבר](#) ובנוספּ [יש סקירה מעוללה של Rachel Shalom](#) באנגלית למי שרצה להבין את השיטה המעניינת זו(V-Swa) לעומק. זאת אומרת “התוצאות” שעלו הם מאמון DETReg הם:

1. BB-ים המחשבים באמצעות SS.
2. ייצוגי Swa של BB-ים אלו.

לב הרעיון של DETReg הוא ללמד ייצוג של אובייקטים תמונה כאשר מטרת האימון היא:

1. להפיק BB-ים דומים לאלו המופקים באמצעות Selective Search.
2. לכפות על ייצוגי Swa של BB-ים “מתאימים” (יפורט בהמשך) של SS ו-DERTeg להיות קרובים.

תקציר המאמר:

לאחר שהבנו את הרעיון העיקרי של המאמר הנסקר, נתבונן בדעת בפרט האימון של DETReg. למעשה תהליך האימון מורכב משני שלבים:

1. הפעלת אלגוריתם SS על תמונות מהdataset (לא מותיג).

נציין כי SS פולט מספר רב של BB-ים כאשר רובם מכילים רק חלק מסווג אובייקט או לא מכילים אובייקטים כלל. עקב לכך המאמר מציע לאחד את האזוריים המוצעים (region proposals) על סמך הדמיון ביניהם. דמיון זה תלי

בקרבה בין המאפיינים שלהם (כגון צבע, טקסטורה, צורת האיחוד ביניהם וכדומה). המאמר מציע מספר אסטרטגיות לבחירה של מועדים לאיחוד (Top-K, k-random וחת ש邏輯 sampling importance sampling) בהתבסס על הציון של האיזורים).

הערה: ראה פרק "הסביר על מושגי היסוד" להסביר קצר על SS.

2. אימון של BB-s שהתקבלו בשלב 1.

לאחר שבנו "דאטסהט מתויג", נותר לנו "רָק" לאמן את הרשות עליו.

למעשה נותר לנו לתאר רק את הארכיטקטורה ואת פונקציית הלוס של DETReg. המחברים בחרו להשימוש בארכיטקטורה שהוצעה במאמר [Deformable DETR](#), שהוא שכולל מאמר מפורסם של קבוצת מחקר AI-Al, הנקרא [DETR](#) (لتיאור קצר של הגישה של DETR ראה פרק "הסביר על מושגי היסוד"). DETR מציע להקטין את הסיבוכיות החישובית של DETR באמצעות חישוב משקל self-attention באופן יותר לוקאלי שבפועל מקטין את מספר החישובים באופןדר ובძקorder של הטרנספורמר. כאמור DETReg משתמש בארכיטקטורה של [Deformable DETR](#) ל-[pretraining](#) כאשר הדאטסהט הוא הפלטים של SS לאחר האיחוד.

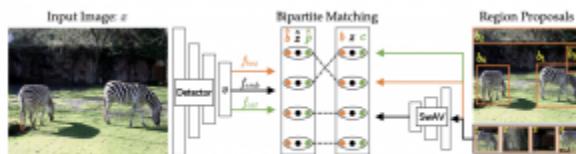


Figure 2: The DETReg pretext task and model. We pretrain a Deformable DETR [59] based detector to predict region proposals and their corresponding object embeddings in the pretraining stage.

הדבר האחרון שנשאר לנו לדבר עליו זו פונקציית loss של DETReg. היא מורכבת מסכום משוקל של שלושה lossים הבאים:

- **loss על המיקום של BB:** משתמשים בו - [Generalized Intersection Over Union \(GIoU\)](#) - די סטנדרטי בסך הכל ().
- **loss על ייצוג SwaV של הfatץ' של התמונה המוגדר באמצעות BB:**

מחושב כנורמה L1 של ההפרש בין ייצוגי SwaV של DETReg לבין אלו של ה-*ground truth* (שהופקו באמצעות SS).

• **loss על קטגוריה של אובייקט:**

כאן נראה שיש לנו בעיה. הרוי SS לא מוציא לנו קטgorיה אלא רק BB-ים. המחברים מצאו פתרון אלגנטiy לסוגיה חזז. הם הניחו כי מספר ה-BB-ים של DETReg פולט (נסמן אותו ב-N) הוא יותר גדול ממספר ה-BB-ים המופיעים באמצעות SS (נסמן אותו ב-M). אז המחברים הוסיפו M-N פסאדו-BB-ים ל-SS ותייגו אותם עם קטgorיה 0, כאשר ה-BB-ים האמיתיים קיבלו ליביל 1. כעת Reg מנסה לחזות הסטברויות לשתי קטגוריות בלבד - BB המכיל אובייקט אמיתי (לייביל 1) ו-BB עם הרקע (לייביל 0). באופן זה המשימה של "זיהוי קטgorיה" הופכת לבעית סיווג ביןארית כאשר פונקציית loss עבורה היא [Focal Loss](#).

הערה: DETR המקורי משתמש בקטגוריה של רקע ל-BB-ים ללא אובייקט בתוכם (מספר BB-ים בפלט של DETR הוא קבוע).

הסבר על מושגי היסוד במאמר:

הסבר על Selective Search

שיטה זו מאתרת "אזורים החשודים להימצאות אובייקטים בהם". אזורים אלו מחושבים באמצעות תהליכי איטרטיבי שמקבץ באופן היררכי אזורים קטנים יותר על סמך הדמיון והקרבה שלהם. SS לא דרש אימון ולא נדרשת התערבות אנווית כדי להפעיל אותו (כמובן קיימים מימוש בפייטון). SS מוציא גם ציונים לכל BB שמודד סבירות של הימצאות האובייקט שם (למעשה האלגוריתם ממין את האיזורים לפי הצפוי של הימצאות אובייקט בו).

תיאור קצר של DETR:

המאמר המקורי DETR מציע לשימוש בטרנספורמרים (כולל אנקודר דקודה) לבניית מודל לזהוי אובייקטים בתמונה (בצורה supervised). נזכיר הפלט של DETR הוא סט S_{mod} של BB-ים עם ייחד עם התפלגותן מעל הקטגוריות של אובייקט בתוך BB. לאחר מכן מנק DETR משתמש באלגוריתם התאמת הזוגות ההונגרי (Hungarian bipartite matching algorithm) שמחפש "התאמה מקסימלית" (מבחינת מיקום וקטgorיה) בין סט S_{gt} של BB-ים (עם הקטגוריה האמיתית ground truth) לבין סט של BB-ים שזוהו באמצעות המודל. לעומת זאת, המטרה היא לבנות את זוגות-BB-ים הדומים ביותר מאיברי S_{mod} ו- S_{gt} . לאחר מכן שזוגות אלו אוטרו, מחשבים פונקציית LOSS שהיא סכום ה"מרחקים" של הזוגות שנבננו (מרחיק של זוג מודד את מידת השוני בין מיקום של BB-ים ולבן הקטגוריות של איברי הזוג). ליותר פרטים על DETR ראו את [הסקירה המעליה](#) של אברהם רביב.

הישגיו במאמר:

המאמר מראה כי שבר DETReg ש עבר pretraining על ImageNET מציג ביצועים טובים יותר מאשר שיטות אחרות (כמו VSw2 ו-MOCOv2). במהלך DETReg (לאחר pretraining) הציג ביצועים טובים יותר מהמתחרים כאשר הוא מכיל על חלק קטן של נתונים מותאמים לזהוי אובייקטים.

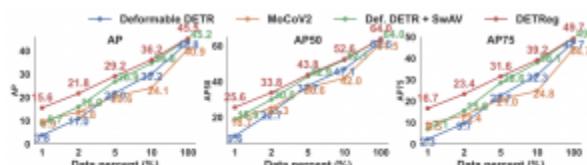


Figure 3: Object detection results finetuned on MS COCO train2017 and evaluated on val2017. DETReg consistently outperforms previous pretraining approaches by a large margin. When fine-tuning with 1% data, DETReg improves 5 points in AP over prior methods.

ג.ב.

מאמר עם רעיון מגניב המאפשר pretraining של מודל לזהוי אובייקטים בתמונות ללא DATA מתואג. הגישה המוצעת הצליחה לשפר בצורה משמעותית את ביצועי המודל לאחר Ciou (גם על נתונים קטנים).

Review 21: SafeDiffuser: Safe Planning with Diffusion Probabilistic Models

פינת השוקר:

המלצת קריאה מיניב ומיק: קריאה מומלצת לאוהבי מודלים גנרטיביים שמבינים קצר בברכה בהירות כתיבה: גבואה/בינוי/נמוכה וכאלא.

ידע מוקדם:

- מודלי דיפוזיה גנרטיביים (DDPM)
- יסודות של למידה באמצעות חיזוקים (reinforcement learning- RL)
- רקע בתכנון מישיות עם שיטות RL

ישומים פרקטיים:

- רובוטיקה
- ניווט

פרטי מאמר:

لينק למאמר: [כאן](#).

קוד: [כאן](#)

קובץ: [כאן](#)

פורסם בתאריך: 21/12/2022 (v2, בארכיון)

הציג בכנס: ICML 2022

תחומי מאמר:

- למידה מחיזוקים (RL)
- מודלי דיפוזיה גנרטיביים (DDPM)
- תכנון מישיות על שיטות RL

כליים מתמטיים, מושגים וסימונים:

- הסרת רעש(denoising) הדרגתית בתהליכי דיפוזיה גנרטיביים
 - דגימה מונחית מסווג(classifier guided) במודלי דיפוזיה
 - אופטימיזציה פונקציית התגמול(reward) בעיות RL
 - דגימה מסט של מסלולים(trajectories) כפונקציה של התגמול
-

מבוא:

בעיות תכנון

בעיות תכנון דורשות מציאה של סדרת פעולות כך שהסוכן ינוע מ מצב התחלתי אל מצב סופי באופן רצוי (אופטימלי). בד"כ המשימה מנוסחת בהקשר של ניווט (כמו מצא לי מסלול מנק' א' לנק' ב'), אך לעיתים בעיות תכנון מופיעות גם בהקשרים אחרים כמו:

- מציאת סדרת טיפולים רפואיים שתמקסם את סיכוי ההחלמה של מטופל
- מציאת מדיניות להציג פרסוםאות באתר שתמקסם את הלחיצות.

סקירה זו תתייחס בעיקר להקשרי הניווט, ולטוקן שלנו נתיחס כרובוט. את המטרה שלו הרובוט לבצע ניתן להגדיר באמצעות פונקציית תגמול(reward), כאשר מטרתו של הטוקן היא לבצע את הפעולות שייבנו לו תגמול מקסימלי. תכנון ניתן לבצע באמצעות למידה, למשל למידה מחזוקים, או באמצעות אלגוריתמים כלליים הבקרה והתכנון.

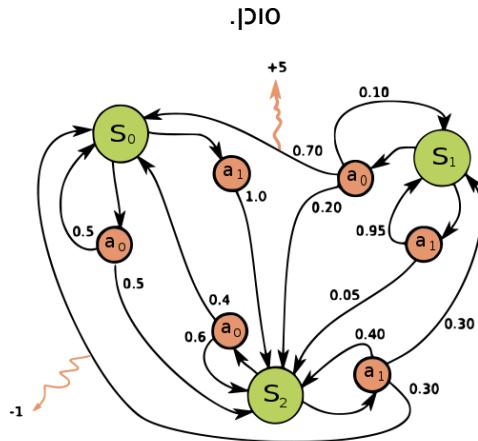
בניסוח מתמטי מצב s_i הוא וקטור המתאר את הטוקן והסבירה שלו בנקודת זמן t והפעולה a_i היא וקטור המיצג פעולה של הטוקן באותה נק' זמן. התוצר המבוקש של תהליך התכנון הוא מסלול $[s_0, a_0, s_1, a_1, \dots, s_{t-1}, a_{t-1}, s_t]$ שזהו מסלול באורך t המכיל סדרה של מצבים ופעולות כך שהפעולה a_i מעבירה את הטוקן מה המצב s_i אל המצב s_{ti+1} , עד שנגיע למצב הסופי s_t .

מושגי יסוד של למידה עם חיזוקים:

טוקן: הישות בעולם שלנו ש צריכה להחליט את הפעולות שעלייה לבצע כדי להגיע אל היעד.

Reward: התגמול שהטוקן מקבל על פעולותיו השונות. המטרה בתכנון היא למקסם את התגמול המctrבר.

MDP (Markov Decision Process): תהליך סטטיסטי בזמן בדיד המתאר התקדמות של טוקן בין מצבים בסביבה מסוימת התקדמות התהליך תלויות בהסתברויות מעבר בין מצבים, אך גם בהחלטות המתקבלות ע"י



דוגמה לתהיליך MDP - בו המעבר מ מצב s_i למצב s_j תלוי בהסתברויות המעבר המושרות מבחירה הפעולה a_i . שימושו לב Ci ההסתברויות תלויות ארך ורך במצב הנוכחי ובפעולה שנבחרה - זהה "הנחה המרקבויות".

תמצית מאמר:

מכיוון שהמאמר הנסקר הוא שדרוג של [מאמר זה של סרגי לין](#) האגדי ושותפיו, נתחילה את סקירתנו עם התיאור של הרעיון המקורי העקריים ואז נמשיך עם הסבר על החידושים שהוצעו במאמר הנסקר. לנוחות נקבע למאמר זה המאמר המקורי. במאמר המקורי המחברים מנסים לפתור את בעיית תכנון המסלול לא באמצעות שיטות סטנדרטיות של RL החווות מצב אחריו המצב אלא חודם את כל המסלול יחד (trajectory). המסלול מוגדר כסדר כנובן חשוב כאן של זוגות (s_i, a_i) , $i=0, \dots, N$ כאשר s_i מסמן את הייצוג (שיכון או embedding) של המצב i ו- a_i היא היצוג של הפעולה i . למעשה ניתן להתבונן בסדרה זו בתור תמונה Nx2 כאשר השורה הראשונה של "היפיקסלים" היא ייצוג המצביעים כאשר השניה מהווה את ייצוג הפעולות.

המחברים מציעים להציג את בעיית תכנון המסלול כבעיה גנטטיבית שמטרתה היא ליצור מסלולים "טובים" חדשים בהינתן דאטasset של מסלולים בעלי תגמול כולל גבוה ומסלולים פחות טובים בעלי תגמול כולל נמוך יותר. כאמור במקומות לבנות מסלול שלב אחריו שלב אנו מאמנים מודל לבנות את כלו כמקרה אחד. איך עושים זאת? כאמור בדומה למודול דיפוזיה גנטטיבים מאמנים מודל הידוע לבנות רוש במסלול המורעש בהדרגה. ככל מרעישים את המסלולים במנוגת קטנות של רוש (איטרציות) ומאמנים מודל חדש לחזות את הרוש המוסף בכל איטרציה. אז כאן עושים זאת לכל מסלול ובסיום המודל מייצר מסלול חדש מרעש טהור על ידי הורדה הדרגתית של הרוש ממנו.

במאמר [safediffuser](#) הכותבים ממשיכים את הקונספט צעד אחד קדימה - מעבר לתוכנו המסלול, השיטה שהם מציעים מסוגלת לשלב אילוצים בתהיליך התכנון.قولו במאמר זה המטרה היא למנף גישה דיפוזיונית לבניית מסלול הסוכן במלואו תוך כדי **עמידה באילוצים הנדרשים**. שיטתה זו חשובה מאוד בתרחישים בהם בטיחות היא קריטית - לא נרצה לייצר לרכב אוטונומי מסלול שמתעלם מתחררים או נסוע נגד כיוון התנועה. הגישה נשענת על שילוב של צעדי "תיקון" במקביל לצעדי הדיפוזיה, שיובילו אותנו לתוצאות שבאהרכה עוננות על האילוץ תוך שמירה על קרבה ל- trajectory המתkeletal ללא אכיפה של אילוצים (כמו שהוצע במאמר המקורי).

תכנון באמצעות למידה

- בשנים האחרונות צצו מספר שיטות לתוכנן מבוססות למידה, העיקריות בהן:
למידה מחיזוקים (Reinforcement Learning): בה מטרת האלגוריתם היא למצוא מדיניות שתמקסם אות Reward(חיזוק) מסוים.
- **למידה מחיקי (Imitation Learning)**: בעית למידה מפוקחת (supervised learning) בה המודל מאומן לבנות מסלול דומה כמה שיוטר למסלולים בדעתהsett הנתון לו.

ישן מספר בעית בשיטות אלו, כמו דרישת לאינטראקציות רבות עם הסביבה הנחוצות ללמידה של מדיניות טובה בלמידה מחיזוקים, יכולת הכללה בעיתית וקושי לגחום למודל לכבד אילוצים המערכת הרצויים. באפליקציות כמו נהיגה אוטונומית וניתוחים רפואיים לא נרצה להשתמש ברשות שבניהה תוצאות מעולות אם ישנו סיכון במרקורי קצה מסוימים הרשות תחולט על עצם שבודדות גבואה יגרום לנזק. באלגוריתמים קלאסיים לרוב ניתן יחסית בקלות למנוע התנהוגיות לא רצויות ע"י הגדרה ואכיפה של אילוצים רלוונטיים (מהירות מקסימלית, איזורים אסורים, ועוד) אך ברשותנו נירונים זה עדין די בעיתו.

למידה מחיזוקים (Reinforcement Learning)

בלמידה מחיזוקים הסוכן לומד מדיניות טובה תוך כדי אינטראקציה עם העולם, ודרך האינטראקציה יכול לנסות פעולות חדשות ולראות מה השפעתן על התגמול. בעית RL בדרך מנוסחות בתור (Markov Decision Process) - תהליך מרקובי בו המצב הבא ובתהליך תליי אך ורק במצב הנוכחי ובפעולה הנוכחית. בהתאם, כך גם מנוסחות המדיניות הנלמדת - בהינתן מצב מסוים המדיניות תחזיר את הפעולה הטובה ביותר ביותר (מבחינת התגמול הכלול) במצב זה.

כמו כן, החלטות מתבצעות בצורה סדרתית - בזמן הטעט הסוכן בכל נק' זמן יקבל החלטה על פעולה אחת, יבצע אותה, ורק אחרי שהגיע במצב הבא יחליט על הפעולה הבאה. סכמה זו אופיינית לאלגוריתמי free Model, שלא חוזרים מראש איך הסביבה משתנה בעקבות הפעולה שנבחרה.

תהליך האימון מתבסס על שימוש אינטנסיבי בסימולטור, בו מושך מילוני אינטראקציות של ניסוי וטעיה עם הסביבה הסוכן לומד את המדיניות האופטימלית - המיפוי בין המצב הנוכחי לפעולה שתניב את התגמול המctrבר המקסימלי.

Offline RL

אחד הביעות המשמעותיות כו� בלמידה מחיזוקים בהקשרי רובוטיקה היא מציאת מדיניות(policy) אופטימלית על סמך>Datasett קיימן שנאוסף מבעוד, מבלי לבצע אינטראקציות נוספת עם הסביבה. בעיה זו צחה כאשר אינטראקציה עם הסביבה היא מאוד יקרה או מסוכנת, למשל שעות טישה במצל"ט שעולות הרבה כסף או רכב אוטונומי שבשלב הלמידה יכול לסכן את שאר הנהגים אם ניתן לו לנסוע בעצמו לפני שהוא סיים את האימון.

במסגרת RL offline צצים אתגרים חדשים - באימון אופליין אין יכולת לבצע אקספלורציה של פעולות חדשות. למשל, אם המדיניות הגיעה במצב מסוים אין לנו אפשרות להתחילה לנחש פעולות אחרות ולבזוק אותן בסימולטור, כמו ב RL הסטנדרטי. במקרים כאלה הרשות תצטרכן ללמידה פועל אך ורק על פי הדעתהsett הקיים - ובמידה והמצב כלל לא קיים בדעתה, הרשות תצטרכן ללמידה להכליל מצבים דומים.

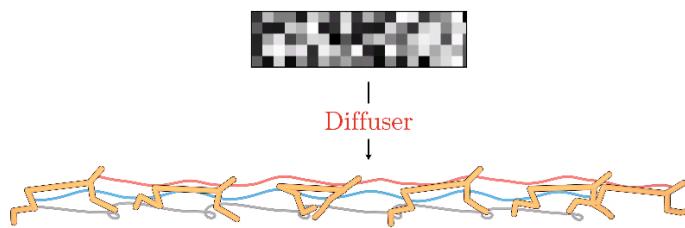
מודלי דיפוזיה

מודל דיפוזיה הוא סוג של מודל גנטטי שלומד ליצור פיסות DATA חדשה מרעיש (בד"כ גאוסי). מודלי דיפוזיה מאומנים באופן הבא: בתהליכי הגדמי מושגים לפיסת DATA מנות קטנות (איטרציות) של רעש עד שהDATA הופכת להיות רעש טהור כאשר המודל מאומן למודד לנוקות את רעש בהדרגות (איתרציה 1+2 לאיתרציה t).

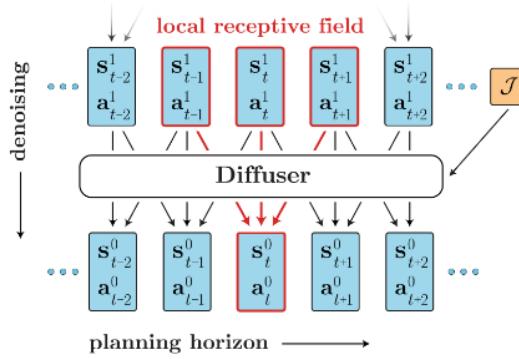
במהלך אינפראנס (גנרטט) מתחילה מרעש טהור ומשתמשים במודל המאומן להסיר רעש בהדרגות עד קבלת פיסת הדטה חדשה.

תכנון בתור בעית יצור תמונה

אם נחשוב רגע על המסלול שאנו רוצים לייצר בתור רשיימה של וקטורי ייצוג (embeddings) של מצב ופעולה, או בעצם מטריצה, ניתן להציג את התהיליך לייצור תמונה שאנו חנו יודעים לעשות מעולה עם מודלי דיפוזיה. למעשה בעית בנייה מסלול ניתן להציג בתור בעית inpainting - בהינתן נקודת התחלתה (העומדה הראשונה במטריצה, שמייצגת את 0^s), מצא את הshallמה של המטריצה כך שנקבל מסלול רצוי. מספר העמודות במטריצה שנבקש הוא בעצם אורכו המסלול, וכל עמודה שהמודול מייצר מיצג מצב שנעבור בו ואת הפעולה שנעשה באותו זמן. באוותה מידת אם נרצה שהמסלול גם יסתים במצב מסוים נבצע inpainting כאשר המצב הראשוני והוסף מקובעים והמודל משלים את היתר.



טכנית, המודל בו משתמשים במאמר מאד דומה למודלי דיפוזיה המשמשים היום לגנרטט של סוגים רבים של דטה ויזואלי כגון תמונות.



העובדת שהרשת המשערת את הרעש הנוסף במודלי דיפוזיה משתמשת בפועלות קוונבולוציה יוצרת כאן תבנית שונה מאוד מאלגוריתמי RL סטנדרטיים. כמו שהסבירנו קודם, באלגוריתמי RL לרוב ישנה הנחה מרקובית - כל מצב תלוי רק ב קודמו (ולא בעבר הרחוק יותר) ובפעולה שנלקחה, וכן התהיליך מתואר כתהיליך MDP. לעומת זאת, כאשר משתמשים במודלי דיפוזיה האינפורמציה הרלוונטיות לכל מצב היא כל האינפורמציה שנכנסה ב-field receptive של הקונבולוציה, כולל מצבים ופעולות שהיו לפני או אחרי המצב הנוכחי. ומה זה משנה בעצם? מודל הדיפוזיה מבצע אופטימיזציה על כל המסלול, מה שלרוב מביא תוצאות Kohärenzיות יותר בהשוואה למסלול המתתקבל ב RL.

?Model Based vs Model Free

עוד אופיין חשוב של השיטה המוצעת הוא שבニアוד לאלגוריתמי RL אחרים הרשות לומדת באופן מרומז מודל של הסביבה. מודל הדיפוזיה מחזיר לנו כבר מההתחלת מסלולם שלם שתוכן \neq צעדים קדימה, שכן ניתן לומר שהרשת מבצעת תכנון אך במקביל לומד לחזות את הפעולות העתידיות. לעומת זאת באלגוריתמי RL המודל לומד לחזות אך ורק את הפעולה הכי טובה עבור כל מצב, אך לא תחזה لأن הפעולה טוביל אותן.

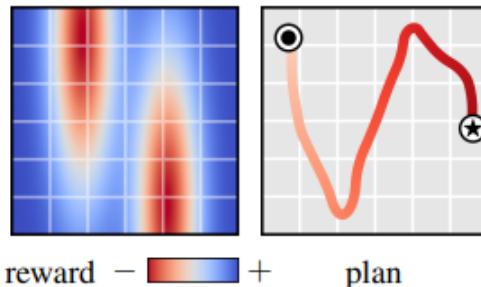
דאטסהט

מאייפה הדטה? המודל מתאמן על אוסף מסלולים שבוצעו מראש והוקלטו. הדאטסהט יכול להיות אוסף הדגומות שבוצעו ע"י מומחה אנושי מעוד מועד. אופצייה נוספת היא לשמר מסלולים שייצר אלגוריתם תכנון קלאסוי. בד"כ אלגוריתמים קלאסויים יכולים להבטיח אופטימליות אך במחיר של זמן ריצה ארוך, שכן השימוש במודל דיפוזיה מאפשר לנו לשמור על זמן ריצה קבוע שmagיע לתוצאות קרובות מאוד למסלול האופטימלי.

אין דרישת על אורכי מסלול או איקוטם. המודל יודע להקליל לאורכי מסלול שונים מסט האימון, מה שעדיין נחשב בעיה פתוחה באלגוריתמי RL *state of the art offline*.

שליטה באמצעות Reward

בשיטת שהגדרכנו עד כה אין לנו שליטה על המסלול המתקבל מהמודל. הרשות מקבלת מסלולים מורעשים בתור מטריצה שמיידה מייצגים את אורך המסלול שנרצה, ונitin במטריצה לקבוע מה יהיה המצב ההתחלתי והסתופי, אבל זו כל השליטה שיש לנו על התהילה. בפועל במשימות מסוימות נרצה שליטה גדולה יותר על המסלול שנוצר - למשל ברכב אוטונומי נרצה מסלול שיcmd לנטיבים ולא יעלה על המדרכה. הדרך שבה המאמר מציע להתמודד עם אילוצים כאלה היא באמצעות reward.



בזמן הה-*inference* (הטגמול reward) על מצבים מזון למודול והוא לומד לבנות מסלול שמקסם את התגמול בזמן ביצוע ה-*inpainting*. ניתן להרכיב את פונקציית התגמול איך שנרצה, מה שנutan הרבה גמישות ביצוע משימות שלא נראה בסט האימון.

אכיפת אילוצים בתחום הדיפוזיה:

cut נסביר על התרומה של מאמר המשך שאותו אנחנו סוקרים כאן:

SafeDiffuser: Safe Planning with Diffusion Probabilistic Models

התרומה העיקרית של המאמר היא הצגת מודלי safe diffusion, המאפשרים אכיפה של אילוצים על המסלולים המתקיים ממודל הדיפוזיה.

איפה ציריך אכיפת אילוצים?

ראשית, נתאר את הדוגמה הבאה:

נניח שנרצה לבנות מודל הדיפוזיה המתכן מסלול נסעה עבור רכב אוטונומי הנוסע בעיר. אספנו נתונים, אימנו את המודל, פרסנו אותו ברכב וקיבלו מסלולים מעולים, אבל נתקלנו בbag מסוכן - לעיתים בזמן פניה הרכב עולה על המדרכה.

קודם כל ננסה לענות על השאלה למה ש"באג" זהה יקרה מלכתחילה? מתמטית, מודל הדיפוזיה ידוע לבצע דוגמה מהתפלגות. לאחר תהליכי האימון המודל למד ליצור מסלול שהוא סביר לתרחיש שביקשנו בהינתן המסלולים שראה בעבר. מכיוון שהתהליך הוא הסתברותי יתכן שעורו תרחישים מסוימים שלא הופיעו הרבה בדתאה, המודל 'יחלט' שעיליה על המדרכה היא פועלה סבירה בהינתן הממצאים הנוכחיים.

אבל למה בעצם לא להשתמש פונקציית התגמול שהציגנו קודם? פתרון אפשרי אחד לסוגיה זו הוא הקצאה של תגמול שלילי מאוד של מינוס אינסופי עבור איזור המדרכה. הוספת תגמול שכזה משנה את הניסוח המתמטי של מודל הדיפוזיה לדוגמה מותנית - דוגמה של מסלול בהינתן פונקציית התגמול נתונה. אבל גם אם נמן את המודל באופן צזה בפועל לא ניתן "להתחייב" כי הוא לא יוביל את המכוון לאיזור המדרכה. זה קורה עקב האופי ההסתברותי של יצירת המסלול באמצעות מודל דיפוזיה (הרי אנו מתחילה את בניית המסלול מדגימת הרעש, וכך). למעשה לא יוכל לשולח את הגעת המסלול לאיזור האסור הזה ב 100% וזה בעיה מאוד רצינית.

אבל איך לאקוּף אילוצים? הכותבים מציעים להשתמש ב- (CBFs) control barrier functions. פונקציות CBF הן פונקציות המסמנות לנו את הממצאים הבוטוחים במרחב הממצאים שלנו. מתמטית נגידיר את הפונקציה ה באופן הבא:

$$h(x_i) \geq 0 \Leftrightarrow x_i \text{ is safe}$$

בתורת הבקלה המתירה לשימוש ב CBFs היא הוספת הפרעה ("תיקון") לפעולות של בקר מסוים כך שהמסלול המתקבל מהבקיר יהיה בטיחותי באופן מוחלט ודטרמיניסטי, אך כמה שיותר קרוב למסלול המקורי שהוא אמר או להתקבל ללא תיקון. הרעיון מאחורי השיטה הוא להשתמש במערכת קיימת שמספקת פתרונות טובים ולהוסיף לה את השינוי המינימלי כדי לפתור בעיות חדשות הכוללות אילוצים, מה שחווסף בתכנון של בקר חדש מופיע. במקרה שלנו נרצה להכניס הפרעה ישירות בתהליכי הדיפוזיה: בכל צעד דיפוזיה t נוסיף תיקון denoising של מטריצה שלנו כך שההווצאה בצעד $t+1$ בהכרח תעמוד בדרישות הבטיחות. נקבל גם המסלול הגרפי מובטח שייעמוד בדרישות הללו. השני שנכנים לצורך הדיפוזיה ימצא ע"י פתרון בעיית האופטימיזציה עם אילוצים (Quadratic Programming) הבאה:

$$\mathbf{u}^{j*} = \arg \min_{\mathbf{u}^j} \left\| \mathbf{u}^j - \frac{\boldsymbol{\tau}^j - \boldsymbol{\tau}^{j+1}}{\Delta \tau} \right\|^2$$

תחת האילוץ שהמסלול המתתקבל מ \mathbf{u}^{j*} הוא מבין הממצאים הבוטוחים, $\exists a \geq 0$ $(\boldsymbol{\tau}^{j+1}).h$.

הישגי מאגר:

המאמר מציג דרך לשלב מודלי דיפוזיה קיימים עם שיטות עדכניות מהתורת הבקלה כדי לפתור בעיות תכנון תחת אילוצים. במאמר מוצגות התוצאות על מספר ביצ'מרקם מפורטים מעולם RL, ורראה תוצאות טובות תוך שמירה על אילוץ מסוים - למשל מניעת התנגשות בזרועות רובוטיות, הגדרת גובה קפיצה מקסימלי ברובוט hopper ועוד. לצפיה באנימציות אנו ממליצים לבקר את [האתר](#).

באופן כללי, עולם התכנון חוווה טרנד חדש של שימוש במודלי דיפוזיה לפתרון מגוון רחב של בעיות מורכבות במיוחד, כמו RL Multi Agent offline ו-RL.

שיתופן פעולה: הபօוט נכתב על ידי [יניב חסידוף ומיכאל \(מייק\) ארליךסון, Michael Erlhson](#).

Review 22: PIX2SEQ: A LANGUAGE MODELING FRAMEWORK FOR OBJECT DETECTION

פינת הסוקרים:

המלצת קרייה מאברהם וממייק: מומלץ מאוד לחובבי לוחובי תחום זיהוי האובייקטים

בהירות כתיבה: גבוהה

ידע מוקדם:

- יסודות של מודלי שפה
- יסודות של שיטות מבוססות רשתות נירונים לזיהוי אובייקטים

ישומים פרקטיים:

- ניתן לישם אותה לבניית מודלים לזיהוי אובייקטים בתמונות.
-

פרטי מאמר:

מאמר: [כאן](#)

קוד: [כאן](#)

פורסם בתאריך: ארכיב, 27.05.2022

הוזג בכנס: ICLR 2022

תחומי מאמר:

- יסודות של זיהוי אובייקטים בתמונות
- מודלי שפה אוטורגסיביים

כליים מתמטיים, מושגים וסימונים:

- טרנספורמרים (אנקודר ודקודר)

מבוא:

זיהוי אובייקטים היא משימה מאוד נפוצה בעולם של ראייה ממוחשבת, ויש לה מספר רב של יישומים מגוונים. ניחח למשל מכונית אוטונומית, שבכל רגע צריכה לזהות את האובייקטים שבסביבתה ולקבל תמונה מצב עדכנית על המתרחש, או לחלוף מצלמה של טלפון נייד שידעת לזהות פנים של בנאדם בצד' לבצע עליהם פוקוס או לתקן רעש רקע, ועוד המן יישומים במגוון תחומיים. משימת זיהוי אובייקטים מורכבת משתי תת-משימות – מציאת המיקום של האובייקט (Localization/Regression) וסיווג האובייקט לקטגוריה (Class) הנקו (Classification). כמובן שנייתן להכליל את משימת Object Detection גם למספר אובייקטים, כאשר במקרה זה על המודל לספק מספר (BB) Bounding Boxes על אחד מהם לזהות את הקטgorיה שלו.

כאמור הפלט של מודל לזיהוי אובייקטים מורכב מミקומי האובייקטים, המtauור באמצעות מלבן (BB) המכיל אותו, והקטgorיה של כל אחד מהם. כל מלבן זה מתואר באמצעות ערכי הקודקוד הימני העליון (x_{max} , y_{min}) וערך הקודקוד הימני התיכון (x_{min} , y_{max}). בנוסף, לכל אובייקט יש ערך נוסף המיצג של המחלקה אליה הוא שייך, ובכך הכל כל אובייקט מתואר באמצעות tuple של חמשה ערכים: {Category, x_{min} , y_{min} , x_{max} , y_{max} }.

מודל לזיהוי אובייקטים צריך לבנות פונקציה לוו המורכבת משני חלקים:

1. **LOSE REGRESSION** שמטרתו לשפר את דיוק של ה-BB שהמודל מספק. איבר זה בפונקציית הלוס "יעניש" את המודל ככל שערכי-h-BB של הפלט יהיו רוחקים מערci-h-BB האמתיים (ground-truth).
2. **LOSE CROSS-ENTROPY** הבודק האם המודל סיוג את האובייקט לקטgorיה הנכונה. בדרך כלל מקובל להשתמש ב-loss cross-entropy, באופן דומה לשימוש בו במשימות סיוג רגילות.

בעבודות אחרות, למשל DETR (סקרנו אותה בעבר), פונקציית המחיר שאמורה לשפר את הרגרסיה(**למה רק רגרסיה**) על ה-h-BB מבוססת על Loss Hungarian. כך גם בעבודות המשך, כמו למשל DETReg (שגם סקרנו בעבר), הבניות על קונספט דומה ומצלחות לשפר את הביצועים של DETR.

הסבר על הרעיון העיקרי של המאמר:

בכל הגישות שתוארו עד כה הפלט היה מיוצג באמצעות tuple שתיארנו קודם, המחזיק ערכים מספריים המיצגים את מיקום h-BB-ים ואיבר נוסף המיצג את המחלקה של האובייקט. במאמר הנסקר המחברים ישמו פרדיגמה שונה לחילוטן ליציג של האובייקטים וגם כן למשימת הזיהוי של מיקומיהם וסיווגם. הרעיון העיקרי של המאמר הוא יציג של מיקום האובייקט ומחלקו באמצעות סדרה (רצף) של מספרים. כל אובייקט בתמונה יתואר באמצעות 5 טוקנים (המייצגים באמצעות ערכים מספריים) ובכך הכל כל האובייקטים בתמונה ייצגו באמצעות סדרת טוקנים באורך של $5 \times$ מספר האובייקטים + טוקן נוסף לסימון של סיום הסדרה, כולם:

(a, a, a, a, a, b, b, b, b, ..., EOS)

(a, a, a, a, a, b, b, b, b, ..., EOS)

התוקנים המייצגים את ערכי הקודקודים הם למעשה הערכים המספריים של הקוארדינטה אותה הם מייצגים (כלומר – x_{min} , y_{min} , x_{max} , y_{max}) והקטgorיה מיוצגת באמצעות טוקן נוסף **נוסף שגם הוא מספר שלם**. כדי לייצג את סוף הסדרה/רצף מוסיפים טוקן של (EOS) שערךו המספרי הוא פשוט 0.

מצין שגודל המילון, המכיל את כל הטוקנים האפשריים, של משימה זו הוא קטן ממשמעותית מזה של מודלי שפה גדולים. למשל לתמונה ברזולוציה 1024×1024 ו- 100 קטגוריות אנו צריכים בסך הכל $100 + 1024 = 1024 + 100 = 1124$ טוקנים.



כיוון שהציגו של האובייקטים הוא רצף ולא כדי שהוא נהוג עד כה, גם החיזוי של המודל נעשה באופן שונה (ואולי זו בעצם המוטיבציה לכך) משמעותית לניסוח זה של בעיית זיהוי האובייקטים). כל המודלים המוכרים מקבלים קלט תמונה והפלט הוא רשימה של האובייקטים והסיווג שלהם, המתקבל **במקרה אחד** ו**בבת אחת**. אמן קיימים מודלים המבצעים זיהוי אובייקטים באמצעות שני ראשים: ראש הרגรสיה (למיקומים של אובייקטים) וראש סיווג (לזיהוי קטגוריה) ויש מודלים שמבצעים את הרגרסיה והסיווג יחד, אך המשותף להם הוא שהפלט מתתקבל בו זמן נתן וכמקרה אחד עברו כל האובייקטים. בעובדה הנסקרת לעומת זאת החיזוי נעשה באופן אוטורגרטיבי, בדומה לאופן בו נעשה שימושים של גנרטום סדרות כמו תרגום או יצירתי טקסט. המשמעות היא שהיא פلت לא נבנה בבת אחת אלא כל פעם המודל מייצר פلت נוספת המבוסס גם על הקלט וגם על איברי הפלט שנוצרו לפניו.

המודל המוצע בכל פעם מספק טוקן אחד בלבד המסמך קואורדינטה של אובייקט או קטגוריה. כל איבר פلت מתבסס גם על הקלט אך גם על הפלטים שנחזו קודם לכן. לכן כל טוקן שנוצר מtabssס גם על המידע החדש (קרי הטוקנים שנוצרו לפניו). באופן זה החיזוי של הקוארדינטות נעשה יותר מדויק כיון שהוא משתמש במידע עדכני כל הזמן. גם חיזוי של קטגוריה מתבסס לא רק על הקלט אלא גם על הקוארדינטות הקודמות שהתקבלו, מה שיכל לתרום בדיקות נוספות. חשוב לציין לב ששימוש טוקן בעל הסתבות הגובה ביותר (モチニティ בהינתן הטוקנים הקודמים) נבחר בתור טוקן הבא בסדרה.

אתגרים המוזכרים במאמר:

הגישה המוצעת להתמודדות עם משימת זיהוי אובייקטים העלתה כМОΒן כמה אתגרים, כאשר חלקם המחברים התייחסו באופן ישיר ואף ביצעו ablation study מكيف.

האתגר הראשון הקשור לטוקן EOS (end-of-sentence) המסמך את סוף הפלט (כאשר המודל תיאור את כל האובייקטים בתמונה). בסיס האימון לכל תמונה יש סדרה המთארת את האובייקטים הנמצאים בה, ובסיום הסדרה יש את הטוקן EOS (שערכו המספר 0) שמסמן שכאן נגמר הפלט. ב-*inference*-*EOS* המודל בעצם נדרש להוציא סדרה של מספרים ובנוסף להוציא את הטוקן EOS בסוף הסדרה אחרי שהוא סייף תיאור של כל האובייקטים שהוא חושב שיש בתמונה. המחברים שמו לב כי לעיתים קרובות המודל מוציא את הטוקן זהה מוקדם מדי, ובכך מפספס אובייקטים בתמונה, והם ניסו כמה גישות כדי להתמודד עם סוגיה זו.

לפנינו נראה את דרכי ההתמודדות ננסח בצורה מעט שונה את הבעיה, בטרמינולוגיה דומה לאיך שהציגנו את אופי הפעולה של המודל האוטורגרטיבי. מודול זהה בכל פעם מוציא טוקן שיש לו את הסתבותות המותנית הגובהה ביותר, **ומה שקרה המודל אمنם זיהה את כל האובייקטים, אך לטוקן של EOS הייתה הסתבותה גבוהה יותר**

מאשר לשאר האובייקטים, ולכן בסדרת הפלט הוא נבחר לפניהם. במקרה זה הסדרה למעשה נעצרת, וממילא אנו לא רואים את החיזוי עבור יתר האובייקטים בתמונה. תופעה זו גרמה לירידה ב-call recall עקב הופעתם של הרבה False negatives (אובייקטים שקיים בתמונה אך המודל לא זיהה אותם). אחת הדרכים להתמודד עם False positive זו היא "להקטין באופן ידני" את likelihood-EOS, אך זה יגרום לעלייה ב-recall (אובייקטים שלא קיימים אך המודל חזה אותם), מה שכמובן מקטין את precision-recall. אמן הטרייד-אוף של precision-recall אינו ייחודי רק לעובדה הזאת, אך פרדיגמה שונה שהמחברים הצליחו לפתור ממשימה זו, אפשרה להם להגיע לביצועים משופרים מבחינת היחס של precision-recall באמצעות 2 טריקים נחמדים של תחילת האימון:

1. הוספה של BB רנדומליים

המחברים הוסיףו של BB רנדומליים כאשר כל BB תוגע עם קטגוריה לא קיימת ("a/n"). המודל מאמין לזרחות BB ככלו עם הקטגוריה הלא קיימת.

2. עיוות של BB קיימים

כאן במקומות מסוימים ב-AFN, המוחברים הציעו "לעוזות" (להזיז או להקטין/להגדיל) BB קיימים ולתיג אותם עם אותה קטגוריה לא קיימת.

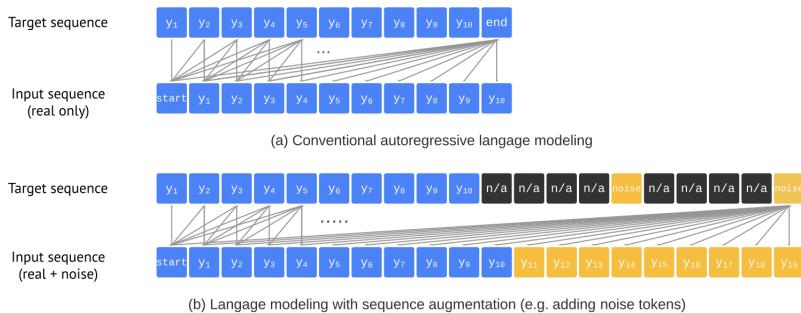


Figure 5: Illustration of language modeling with / without sequence augmentation. With sequence augmentation, input tokens are constructed to include both real objects (blue) and synthetic noise objects (orange). For the noise objects, the model is trained to identify them as the “noise” class, and we set the loss weight of “n/a” tokens (corresponding to coordinates of noise objects) to zero since we do not want the model to mimic them.

נציין כי במהלך האימון הlös על BB-ים לא אמיתיים מתווסף לפונקציית LOSS הרגילה כאשר המודל לא נכנס על זיהוי שגוי של הקואורדינטות של BB-ים אלה.

טריקים אלו מאפשרים לאמן את המודל עם מספר טוקנים קבוע וגובה מסוים בשביל לזרחות את כל האובייקטים בתמונה. בזמן ה-inference לכל אובייקט נבחרת מקטגוריה אמיתיית בעלת הסתברות גבוהה ביותר.

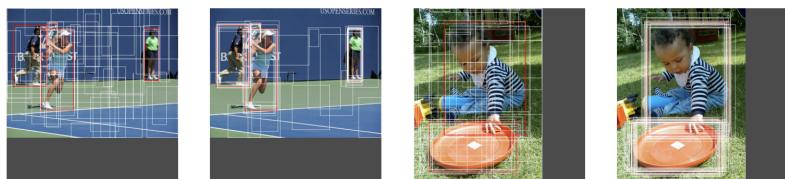


Figure 6: Illustrations of randomly sampled noise objects (in white), vs. ground-truth objects (in red).

בעיה נוספת שעליה מהציג של האובייקטים סדרה היא הסדר בין האובייקטים. מצד האמת, אין משמעות לסדר של האובייקטים ואין אובייקט אחד שנמצא בתמונה בודאות גדולה יותר מאשר אובייקט אחר. מודל שמצוין זיהוי של כל האובייקטים ביחיד באמת אינו מעדיף היחיד על אחר. יציג של האובייקטים סדרה לעומת זאת הוא בעייתי, כיוון שהוא אומר שככל שאובייקט נמצא מוקדם יותר בסדרה כהה ה likelihood שלו גבוה יותר. המשמעות של זה היא שבזמן האימון אנו מכחילים את המודל ללמידה בין האובייקטים ולספק כפלט אובייקט אחד לפני הآخر, למراتות שאין באמת יחס סדר כלשהו. כך למשל אם יש בתמונה כוס ופיל ובסדרה המייצגת אותן הכוו מופיעות לפניו הפיל, אך אם המודל ייחס את הפיל לפני הכוו - תיווצר חוסר התאמה בין ה ground-truth לבין ה detection, ומילא בתהיל' האימון המודל "יענש" על חיזוי צזה למחרות שהוא נכון לחולוטן.

המחברים בוחנו 4 אפשרויות לשידור האובייקטים:

1. סדר רנדומלי
2. מינון לפי גודל האובייקט
3. מינון לפי מרחק אובייקט ממרכז התמונה
4. מינון לפי סדר הקטגוריות

הביטויים הטובים ביותר הושגו כאשר האובייקטים מסודרים בסדר רנדומלי (1). כפי שציינו הממחברים, אין הגיון לאlez את המודל לחזות את האובייקטים דואק באסדר מסוים, ולכן לא מפתיע שאף אחת מפעולות המינון לא הייתה טובה מהאחרות או מסידור רנדומלי, אם כי עדין חשוב לציין שם בסדר הרנדומלי ישנה בעיתיות מובנית.

הישגי המאמר:

המחברים השוו את ביצועי Pix2Seq עם כמה שיטות פופולריות לזיהוי אובייקטים כמו, Faster R-CNN+ DETR ו- Faster R-CNN על דאטסהט קלאסי לזיהוי אובייקטים CoCo. השיטה המוצעתה הצלחה להשיג ביצועים בררי השווה לשיטות הניל מבחן דיק ממוצע (average precision) עבור כמה ספים (thresholds) שונים. בנוסף המאמר בוחן את ביצועי הגישה המוצעת בשתי קונפיגורציות של אימון: אימון מהתחלה pretraining על דאטסהט גדול Object365. עם זאת לא ראייתי השווה עם שיטות יותר עדכניות כמו DETReg.

Method	Backbone	#params	AP	AP ₅₀	AP ₇₅	AP _S	AP _M	AP _L
Faster R-CNN	R50-FPN	42M	40.2	61.0	43.8	24.2	43.5	52.0
Faster R-CNN+	R50-FPN	42M	42.0	62.1	45.5	26.6	45.4	53.4
DETR	R50	41M	42.0	62.4	44.2	20.5	45.8	61.1
Pix2seq (Ours)	R50	37M	43.0	61.0	45.6	25.1	46.9	59.4
Faster R-CNN	R101-FPN	60M	42.0	62.5	45.9	25.2	45.6	54.6
Faster R-CNN+	R101-FPN	60M	44.0	63.9	47.8	27.2	48.1	56.0
DETR	R101	60M	43.5	63.8	46.4	21.9	48.0	61.8
Pix2seq (Ours)	R101	56M	44.5	62.8	47.5	26.0	48.2	60.3
Faster R-CNN	R50-DC5	166M	39.0	60.5	42.3	21.4	43.5	52.5
Faster R-CNN+	R50-DC5	166M	41.1	61.4	44.3	22.9	45.9	55.0
DETR	R50-DC5	41M	43.3	63.1	45.9	22.5	47.3	61.1
Pix2seq (Ours)	R50-DC5	38M	43.2	61.0	46.1	26.6	47.0	58.6
DETR	R101-DC5	60M	44.9	64.7	47.7	23.7	49.5	62.3
Pix2seq (Ours)	R101-DC5	57M	45.0	63.2	48.6	28.2	48.9	60.4

המאמר הציע פרדיגמה חדשה ומעניינת לבניית מודל לזרחי אובייקטים בתמונה שהפלט שלו מיוצר באופן אוטורגרטי. הביצועים של הgesha די דומים לשיטות קלאסיות לזרחי אובייקטים. אני מניח שבקרוב יצאו מאמרם המשכילים גישה זו ומצלחים להציג ביצועים טובים יותר משיטות SOTA.

שיתוף פעולה: סקירה זו נכתבת בשיתוף עם [אברהם רביב](#).

Review 23:

Make-A-Video: Text-to-Video Generation without Text-Video Data

Dreamix: Video Diffusion Models are General Video Editors

פינת הסוקר:

המלצת קריאה ממיק: מומלץ לאלו העוסקים בగנרטט ועריכה של סרטוני וידאו

bahiorot ctiyha: ביןונית ל- Make-A-Video

ידע מוקדם:

- הבנת יסודות של DDPM (כולל איך מגנרטים וידאו מטיקסט)
- עקרונות של גנרטט של סרטוני וידאו

ישומים פרקטיים:

- גנרטט ועריכה של וידאו מטיקסט או מתמונה/וות נתונה/וות

פרטי מאמר:

لينקים למאמר: [זמן להורדה 1](#), [זמן להורדה 2](#).

lienek l'kod: לא מצאתי לשניהם

פורסם בתאריך: 29.09.2022 ו- 02.02.2023, בארכיב.

הציגו בכנס: ---.

תחומי מאמר:

- מודלים גנרטיביים
- מודלי דיפוזיה (DDPM)
- גנרטו וידאו מטקסט

כלים מתמטיים, מושגים וסימונים:

- מודלי דיפוזיה (DDPM)
- טרנספורמרים
- [CLIP](#)
- [Imagen](#)
- [DreamBooth](#)

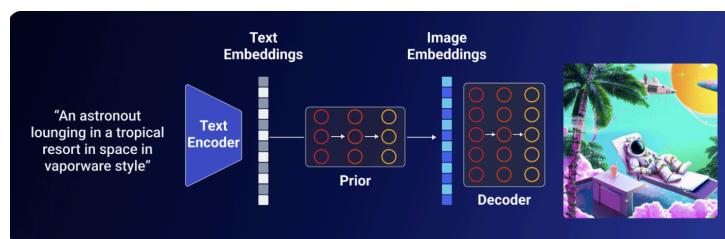
מבוא:

זהה הסקירה הראשונה ב-zsellers deepnightlearners שבה אסקור יותר ממאמר אחד. Make-A-Video הוא מאמר ד' עתיק (יצא לפני 9 חודשים) הוא אחד המאמרים הראשונים בנושא המרתך של Text2Video. המאמר השני משדרג את היכולות שפותחו ב-[Make-A-Video](#) ומציע יכולות חדשות כמו עERICA של וידאו וganerato של וידאו מכמה תמונות.

נתחיל מლס庫ר את Make-A-Video שמרתכו היא לחקות שיטות לייצור תמונות מתייאור טקסטואלי ([DALLE-2](#), [Imagen](#), [Stable Diffusion](#)) ולהתאים אותן לייצור סרטוני וידאו. למעשה המאמר מקנה למודל Text2Image יכולת ליצור סדרה קוהרנטית של תמונות (פרויומים) במילימ"מ אחריות סרטון וידאו.

מודלי Text2Image מבוססי דיפוזיה:

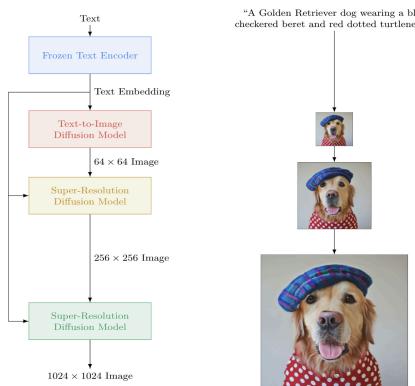
נתחיל מהסביר קצר איך עובדות השיטות לגנרטו DATA מטקסט (Text2Image) כמו אלו שהזכירנו קודם. מודלים אלו מבוססים כולם על מודלי דיפוזיה הסתבוחותיים ([DDPM](#)).



איור 1: אבני בניין של [Stable Diffusion](#)

לרוב מודלי Text2Image מורכבים מהחלקים הבאים:

1. **מקודד של טקסט**: (Text Encoder): מפיך שיכון (embedding) של תיאור התמונה. בדרך כלל לוקחים מודל שפה ענק (LLM) כמו CLIP או T5 ומשתמשים בו כמו שהוא או מכילים במאילר אימון. המאמר משתמש במודל CLIP מאומן לחישוב "יצוג"(=שיכון) של הטקסט ושל התמונה.
2. **מודל הממפה שיכון של טקסט לשיכון של התמונה**, Prior. מודל זה הינו אופציוני ולמשל Imagen לא משתמש בו. Prior בדרך כלל מבוסס על מודלי דיפוזיה (כמו b-2-E2E-E-U) עם ארכיטקטורת Net-Net-U. דרך אגב b-2-E2E-E-U בדקנו ארכיטקטורה אוטורגרטיבית אך טוענת המחברים זה עבד פחות טוב.
3. **מפענה (decoder)**: בונה את התמונה מהשיכון שלה. מודל זה יכול להיות מבוסס על מודל דיפוזיה (כמו b-2-E2E-E-U) או סתם רשות ניירונים כמו b-Hausdorff. שימוש לב שדרקORDER מבוסס מהוות מה שנקרה מה cascaded model, שמורכב מכמה מודלי דיפוזיה המבצעים דגימת יתר (upsampling) כל הדרך לרזולוציה הנדרשת.

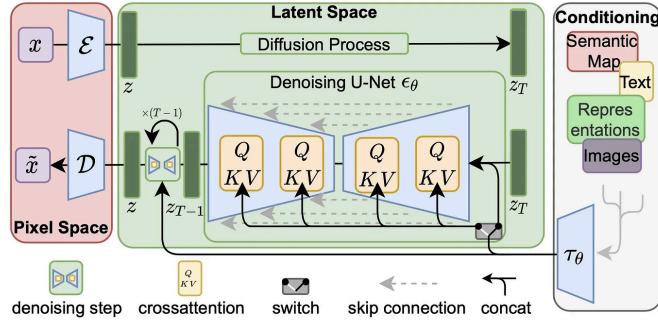


איור 2: Imagen - מודל דיפוזיה cascaded

תיקציר מאמר Make-A-Video

כאמור Make-A-Video הינו שכלל של מודלי Text2Image המאפשר לגנרט וידאו מהתייאור הטקסטואלי. הבעה המהותית ביותר ב亞tor ב亞mon מודל זה היא היעדר דאטאטטים גדולים וזמןים של סרטוני וידאו באיכות גבוהה בעלי תיאור טקסטואלי. המחברים "עוקפים" בעיה זו ומאמנים את המודל שלהם קודם כל על הדאטאטט המכילים תМОנות עם כוורת ולאחר מכון מכילים אותו עם סרטוני וידאו לא מתוארים (ללא תאור).

ארcitקטורת Make-A-Video די מזכירה את מה שתואר בסעיף הקודם. השינוי המהותי היא החלפה של **קונבולוציות דו-מימדיות (2d)** רגילותות שהו ב-UNet (עם attention) שכיכבו ב-Stable Diffusion (ראה איור 3), **בקונולוציות 3d פריקות (3d separable)**. במאמר קונבולוציות אלו נקראות **spatial-temporal**.

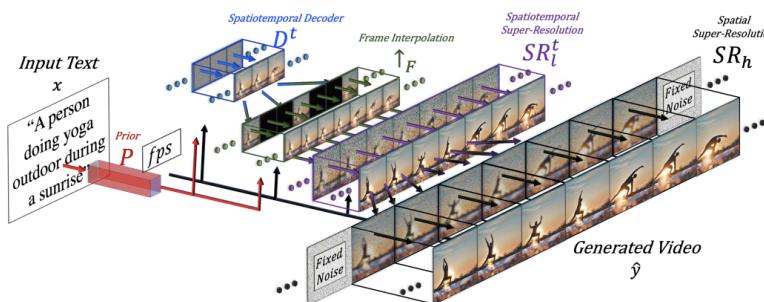


איור 3: UNet עם שכבות ה-*attention*

המימד הנוסף שהתווסף שכבות הקונבולוציה הוא באופן לא מפתח זמן. שכבות אלו מאמנות (מכילות) לשמרת הקוורנטיות והשטף הרציף של הפריים (ראה איור 4).

గנרט וידאו עם Soo Video מרכיב מכמה שלבים:

1. יצירת 16 פריים בגודל 64x64 מהטקסט.
2. ביצוע דגימת יתר למספר פריים לשניה (frame rate - fps)גובה יותר תוך שמירה על הרצולוציה של כל פריים.
3. שלב SR: מבצעים דגימת יתר למרחב הפיקסלים ו/או למרחב הזמן (מעלים מספר פריים לשניה).
4. בשלב SR_h מגדילים רק את רצולוציית הפריים תוך שמירה על אותם fps (אחרת זה יצא כבד מדי מבחינה חישובית לאמן את זה). בסוף התהליך מקבלים וידאו ברצולוציה 768x768 בכמה fps אפשריים (המחברים מבצעים downsampling ל-512x512 בטעונה שזה מורד רעשים של תדרים גבוהים שייצאו לא טוב ברצולוציה 768x768).



איור 4: דיאגרמה כללית של Soo Video

הערה: איור 4 הינו לגמרי ברווח ארה הסבר המעמיק מגע כבר בפרק הבא.

איך מאמנים Soo Video:

האימון של המודל מכיל 3 שלבים עיקריים:

1. **אימון של רשת Prior** המקבלת ייצוג (שיכון) של טקסט לשיכון של תמונה, כולל מיפה שיכון של טקסט לשיכון של תמונה. מודל זה מאומן על דאטסהט של תמונות עם כוורת כאשר השיכון של טקסט והשיכון של תמונה מחושבים עם המודלים המאומנים של CLIP (לא ברור אם מודלים CLIP מאומנים או מוקפאים בשלב זהה). הפרIOR הוא מודל דיפוזיה מותנה (conditional diffusion model) כאשר מקבל שני פלטימ: השיכון של CLIP עבור הטקסט וגם השיכונים של הטוקנים (BPE). לאחר מכן ה-*z*-prior מוקפא ולא מכיל יותר.

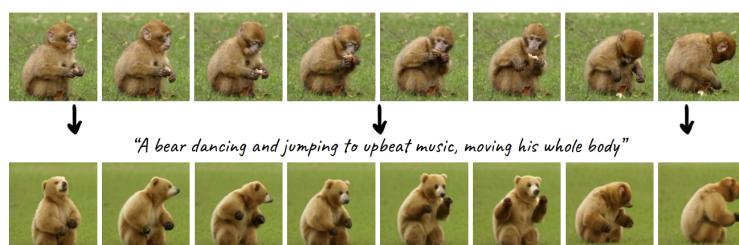
2. **מאימים את הדקודר** (היציר תמונה ברגולציה הנמוכה ביותר 64×64) ושני המודלים של upsampling על דאטסהט המכיל תמונות בלבד. נציין כי הקטל לדקודר מוחשב עם CLIP (מויקף למרות שהמאמר לא מציין זאת במפורש). בשלבים אלו מודל מאומן **לא** שכבות קונבולוציה עתיות (temporal convolution) אלא כמו מודל רגיל לגנרט של תמונות מטקסט. כל המודלים אלו הינם מודלי דיפוזיה מותנים. הדקודר מקבל את הפלט של CLIP (השיכון של התמונה) כקלט וקהליטים לשני מודלים של super-resolution הם הפלטימ של השלב הקודם.

3. מוסיף למודל המאומן בשלב הקודם קונבולוציות עתיות בדקודר ושתי רשות sampling ומכילים אותם עם קטיעי ידאו בלבד (לא כוורת). שכבות הקונבולוציה מתחילה עם משקלים מהשלב הקודם. בשלב הראשון המודל מייצר 16 תמונות לכוורת נתונה ולאחר מכן מבצעים (כלומר sampling) אינטראולציה "רציף" לתמונות אלו כדי להפוך אותם ל偶像 קורנטי. בהתחלה משבכלים את הפרימרים לקבץ פרימרים הרצוי ומתחילה את הקונבולוציות העתיות עם וקטורי hot-one (שקל להפעלת טרנספורמציה זהות/לא לעשות דבר בזמן). כאן האימון מתבצע באמצעות מיסוך של פרימרים מסויימים בוידאו כאשר המודל מתבקש לנחש את הפרימרים הממוסכים.

תקציר מאמר Xōz

המאמר מציע מודל המסוגל לבצע מספר פעולות עם ידאו:

1. ערכית ידאו בהתאם לתיאור טקסטואלי:



2. יצרת ידאו מהתמונה בודדת ותיאור טקסטואלי (המתארת פעולה בוידאו):



3. יצרת ידאו מכמה (מספר קטן) של תמונות ותיאור טקסטואלי:



הכותבים משתמשים במודל שהוצע במאמר [Imagen-Video](#) כמודל בסיס ומכiliaם אותו כדי לאפשר ביצוע של הפעולות הנ"ל. עקרונות המודל של Imagen-Video ד' דומים ל-[Make-A-Video](#) שאותו תיארנו בפרקים הקודמים. שני מודלי אלו מבוססים על אותו העקרונות אך יש להם שלושה הבדלים עיקריים:

1. [Imagen-Video](#) משתמש במודל LXX-5T לבניית שיכון של פרומפט (CLIP)
2. [Imagen-Video](#) לא משתמש ברשות Prior ההופכת שיכון של פרומפט לשיכון של תמונה (וידאו למשה)
3. [Imagen-Video](#) משתמש ב-3 מודלים של [upsampling](#) מרחב (רחלוציה) ועט (מספר פריימרים בשניה) ולא בשניים כמו [Make-A-Video](#).

Dreamix לוקח את המודל של [Imagen-Video](#) ומשתמש בו כדי לעורך וידאו וליצור וידאו מתמונה בודדת ותיאור. איך זה נעשה? למשל למשימת עriticת וידאו, קודם, קודם כל מוסיפים רעש לווידאו, המתאים לאיתריצה t (ראה העירה מתחת לפסקה זו) מסויימת של התהיליך הקדמי של DDPM ומורידים לו רחלוציה מרחבית וגם קצב פריימרים בשניה. לאחר מכן משחררים את הסרטון המשובש הזה לרחלוציה רצiosa (המרחבית-frame rate) כאשר אחד הקלטים הוא הפרומפט. למעשה מודל [Imagen-Video](#) משמש להסרת הרעש ולדיגיטמית יתר של הוידאו המורעש ו- [downsampling](#) עד ליצירה קטע הוידאו המקורי. כדי ליצור וידאו מתמונה בודדת ותיאור פעולה, הכותבים משכפלים את התמונה כמה פעמים. לאחר מכן "מכניסים לתמונות אלו קצת דינמיקה" על ידי הפעלה של טרנספורמציות המדומות תנואה רציפה (שינוי מיקום, כיוון וכדומה) של המצלמה. לאחר מכן מוסיפים רעש ומעבירים דרך [Imagen-Video](#) ליצירה של וידאו נקי ברחלוציה הרצiosa.

הערה: *למעשה t זה לא מספר האיתרציה אלא מספר בין 0 ל-1 כאשר 0 מסמן דוגמא נקייה ללא תוספת רעש ומתחאים לרעש גאוסי טהור - האיתרציה الأخيرة של התהיליך הקדמי).*

הגישה הנאייבית הזו, שלא דורשת יכול של [Imagen-Video](#) לא הצלחה לייצר וידאו באיכות מספיק טובה עבור משימת עriticת הוידאו. הסיבה לכך לדעת המחברים היא אי יכולת לשמור על התוכנות של הוידאו המקורי. כדי להתגבר על בעיה זו, המחברים השתמשו בשיטה שהouceעה-ב-[DreamBooth](#) (חוקרים ישראלים נתלו חלק במחקר זהה). הכותבים של DreamBooth פיתחו שיטה לכיל מודל דיפוזיה Text2Image מאומן כך שיוכל לגנרט תמונות עם אובייקט נתון (גיגד כלב או אגרטל, ראה אויר למטה) - תהיליך זה נקרא [personalization](#).



coil זה מתבצע באופן הבא:

1. בוחרים "שם" לאובייקט באמצעות קידודו עם טוקנים נדרים, כולל טוקנים בעלי שכיחות נמוכה (ראה הערה)
2. מכילים מודל עם תМОנות של האובייקט כאשר הפורומפט מכיל את "השם" הנבחר של האובייקט (a in \$# doghouse).

הערה: בחירה של טוקנים רגילים לקידוד האובייקט ולא קומבינציות נדירות של טוקנים רגילים (כמו `30sbs4a xyz`) מנמקת במאמר (*DreamBooth*) באופן הבא. טוקנים רגילים משוכנים (*embedded*) בנפרד ע"י הטוקנייזר ולכל אחד מהם עשוי להיות פריור חזק. וכך המודל עלול לשנות אותם וזה עלול לעזות את המבנה של המרכיב הלטנטי של הטקסט והישור (*alignment*) שלו עם המרכיב הלטנטי של התמונה.

המחברים של *Dreamix* משתמשים בגישה זו ומכילים את *Make-A-Video* עם הידע המקורי. כאן הכיוול משלב את שני היעדים הבאים:

1. "מלמדים" את *Make-A-Video* לשחרר את הידע או עצמו מהగרסאות המורעשות שלו.
2. לכל פריים בודד "מלמדים" את המודל לשחרר כל פריים נקי מהפרייםים המורעשים אחד אחד.

שני כיולים אלו מתבצעים פעמי אחת לכל וידאו הנערך ולאחר מכן ניתן לעורר אותו כרצוננו. למעשה זה שלב מקדים לפני עריכה של וידאו נתון.

הערה: לא ברור איך בוחרים את הטוקנים הנדרים לשלבים הללו (אם פריים של וידאו ידאו עצמו מוקודד עם אותם טוקנים נדרים).

דגם מ-*Dreamix*:

כמו ברוב המוחלט של מודלי הדיפוזיה הדגימה בהם מתבצעת באמצעות שיטת [DDIM](#). שיטה זו מאפשרת תהליכי מהיר יותר (פחתת איטרציות) של הסרת הרעש (denoising= backward process). האצה זו מאפשרת כאשר משנים את התהליך הקדמי להיות לא מרקובי (x_t תלוי לא רק ב- x_{t-1} אלא גם ב- x_0). המאמר לדעתינו מקבל הרבה פחות תשומת לב ממה שמשמעותו ואני מתקנן לסקור אותו באחת הסקירות הבאות.

ג.ב.

בסקירה הארוכה זו סקרוינו שני מאמרים המציעים מודלים *text2video*. המאמר הראשון מציע שיטה לגנרט וידאו מטקסט, כאשר המאמר השני משכל יכולות אלו ובונה מודל המסוגל לעורר וידאו בהתאם לתיאור הטקסטואלי וגם ליצור וידאו מסדרה של תמונות.

Review 24: RL Prompt: Optimizing Discrete Text Prompts with Reinforcement Learning

פינת הסוקה:

המלצת קרייה ממיק וקרין: שווה קרייה למתעניינים ב-RL ו-NLP

bahiorot כתיבה: בינוי פלוס

ידע מוקדם:

- היכרות עם עקרונות מודלי שפה גדולים
- הבנה בסיסית בהנדסת פרומפטים
- היכרות עם עקרונות של למידה באמצעות חיזוקים (Reinforcement Learning - RL)

ישומים פרקטיים:

- פרומפטים משופרים למודלי שפה

פרטי מאמר:

lienק למאמר: [זמן להודה](#).

lienק לקוד: ---.

פורסם בתאריך: 22.10.22, בארכיב.

הציג בכתוב: ---.

תחומי מאמר:

- מודלי שפה גדולים
- ההנדסת פרומפטים
- למידה באמצעות חיזוקים

כליים מתמטיים, מושגים וסימונים:

- מודלי שפה גדולים - LLMs
- למידה באמצעות חיזוקים - RL
- ההנדסת פרומפרטים - PrEng

מבוא:

פרומפט (prompt, הנקה בעברית) היא דרך תקשורת עם LLM-ים מאמנים. למעשה פרומפט היא טכנייקת ניסוח של השאלות ל-LLM-ים בשפה שהם מבינים שמאפשרת לנו לנצל את הידע החבוי בפורמטים שלהם לביצוע מגוון משימות קצה. יותר ספציפית, פרומפט הוא פיסת טקסט שמכילה לרוב את הגדרת המשימה ולאחר מכן קלט, כך שהמודל שפה יוכל ליצור את התשובה בפורמט האbove עליו - ע"י פתרון בעית "מיסוך" וכו' (masking problem) שמודל שפה "אוהבים". כאמור המודל מתבקש להשלים את המיקומות הממוסיכים בקלט. למשל עבור משימת תרגום, הפרומפט יכול להיראות באופן הבא (למשימת few-shot learning):

```
Translate from English to Spanish.  
English: I like cats.  
Spanish: Me gustan los gatos.  
  
English: I went on a trip to the bahamas.  
Spanish: Fui de viaje a las bahamas.  
  
English: Tell me your biggest fear.  
Spanish:
```

איור 1: דוגמא של פרומפט (נלקח מבלוג)

מושא של הנדסת פרומפטים הפק להיות מאוד פופולרי בשנים האחרונות. יצאו מאות מאמרים המתעניינים גישות להנדסת פרומפטים וגם הסברים למה זה עובד. רוב השיטות להנדסת פרומפטים מנוסחות לאתר פרומפט אופטימלי רך (soft prompt) כЛОמר שיין (embedding) של פרומפט. לשיטה זו יש כמה חסרונותבולטיים:

1. קושי ב-explainability
2. פרומפטים רכים עלולים לא לעבוד עם מודלי שפה שונים
3. לא ניתן לבנות פרומפט אם אין לנו גישה לגרדיאנטים של מודל שפה (למשל כאשר אנו עובדים עם מודל שפה דרך API)

תמצית מאמר:

המאמר שנסקור היום מציע שיטה המאפשרת חישוב פרומפטים עצם ולא וקטור השיכון שלהם. כאמור הפלט של השיטה הוא סדרת הטוקנים הבונים את הפרומפט. שיטה זו לא דורשת ידע על מודלי שפה שעבורו נבנה הפרומפט ועקב כך מאפשרת מציאת פרומפט אופטימלי כאשר מודל שפה נגיש דרך API.

זכיר כי מציאת פרומפט אופטימלי (ולא יציגו) היא בעית אופטימיזציה דיסקרטית (מרחב החישוב הוא מרחב הטוקנים). נבע לכך שאנו לא יכולים לחשב גרדיאנטים (לפחות לא באופן ישיר) ולבצע gradient descent וזה די טבעי שהמחברים בחרו להשתחש בשיטה מלמדיה באמצעות חיזוקים (RL) למשימה זו. אבל איך בכלל מפעלים טכניקות RL למודלי שפה (למשימות גנרטטיב). בשביל כך אנו צריכים להגדיר מה היא פעולה, מצב (state), אסטרטגיה ותגמול. הפעולה כאן היא ייצור טוקן הבא, האסטרטגיה היא בעצם פונקציית softmax המגדירה הסתברות של כל טוקן והtagmol (reward) מודד את הדמיון בין פלט לבין ה-ground truth.

כדי ליצור פרומפט אופטימלי הכותבים מאמנים מודל, שהוא LM מוקפא (לא חייב להיות זהה ל-LLM שעבורו נבנה הפרומפט) עם רשת MLP מאומנת בסוף. רשת זו נקראת במאמר Policy LM (מודל שפה לבנית הפורמטים). המאמר משתמש באלגוריתם RL מסווג policy-hos לאימון של LM Policy, כאשר המטרה לאמן את

ה-MLP ב-LM Policy כך שהיא תמקם פונקציית התגמול. באופן טבעי פונקציית התגמול אומדת עד כמה הצלחנו להפיק תוצאה רצiosa מהפרומט, שנבנו באמצעות LM Policy.

Methods	Frozen LMs	Automated	Gradient-Free	Guided Optimize	Few-Shot	Zero-Shot	Transferable b/w LMs	Interpretability
Fine-Tuning	✗	✓	✗	✓	✗	✗	✗	✗
Manual Prompt Instructions	✓	✗	✓	✗	✓	✓	✓	✓
In-Context Demonstration	✓	✓	✓	✗	✓	✗	✓	✓
Soft Prompt Tuning	✓	✓	✗	✓	✓	✗	✗	✗
Discrete Prompt Enumeration	✓	✓	✓	✗	✓	✓	✓	✓
AutoPrompt (Shin et al., 2020)	✓	✓	✗	✓	✓	✗	✓	✓
RLPrompt (Ours)	✓	✓	✓	✓	✓	✓	✓	✓

Table 1: Comparison of different (prompting) paradigms for using pre-trained LMs on downstream tasks, in terms of several desirable properties. *Gradient-Free* methods do not require gradient information from the prompted LMs, which may be inaccessible or expensive to compute. *Guided Optimize* means the optimization/search is guided by gradient or reward signals, which tends to be more efficient than otherwise (e.g., enumeration). Prompts of discrete tokens (as opposed to embeddings) are often *transferable/reusable* by different LMs. Our approach with RL can optimize prompts using rewards without supervised data (*zero-shot*). *Discrete Prompt Enumeration* selects the best prompt from a large number of candidates (e.g., from paraphrasing or generation, Jiang et al., 2020; Gao et al., 2021; Liu et al., 2021b; Prasad et al., 2022). *AutoPrompt* (Shin et al., 2020) uses gradients to edit the discrete prompt tokens. See §4 and Appendix §C for more discussion.

הסבר של רעיונות בסיסיים:

אחד האתגרים המרכזיים לאימון מודל RL היא בחירה של פונקציית התגמול. כאמור בפרק שלנו פונקציה לתגמול לפורומט נתון מזדעת את "aicות הפרומט", כלומר עד כמה הצלחנו להוציא אליו תשובות טובות מה-LLM. מרחב התגמולים הינו מאד דليل כי התגמול מתקבל רק לאחר סיום בניית הפרומט ולאagemri ברור איך לשער אותו במהלך בניית הפרומט (אחרי כל טוקן). עקב כך הכותבים מציעים שיטת בניית תגמול ייחודית פרט מטה. למשל למשימת הסיווג few-shot המאמר מנסה לא סתם למקסם את הסתברות של קטגוריה היעד אלא מקסם את ההפרש בין הסתברות קטגוריות היעד לבין הקטגוריה בעלת הסתברות מקסימלית בין שאר הקטגוריות. בנוסף הכותבים "מצ'רים" (מגדלים) את LM Policy באמצעות מנגנון חיזוי (ראה פרק 3.1 במאמר להסביר יותר מעמיק).

אחרי שהבנו איך לבנות פונקציית התגמול,icut נפרט איך הכותבים ממקסימים אותה. המאמר בגרסת policy-on-sho של אלגוריתם שנקרא SQL (Soft Q-Learning). נזכיר כי אלגוריתמי policy-on-sho הם סוג של אלגוריתמי RL שבهم הsuton משתמש באסטרטגיה (policy) הנוכחית כדי לקבוע את הפעולות ולומד מtagmolim שהוא מקבל. המשמעות היא שהsuton מעלה את האסטרטגיה על סמן התגמולים מהסביבה, מה שمبיא לastratgy חדשה המשמשת אותו לאחר מכן.

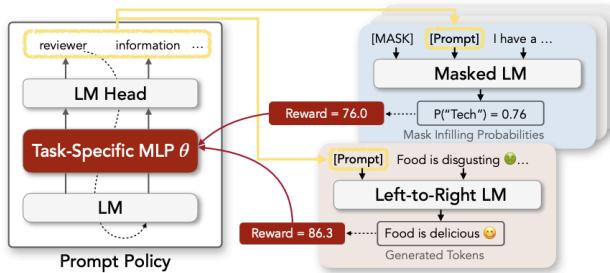


Figure 1: Overview of RL-PROMPT for discrete prompt optimization. All LMs (white boxes) are frozen. We build our policy network by training a task-specific MLP module inserted into a frozen pre-trained LM. The figure above illustrates generation of a prompt (left), example usages in a masked LM for classification and a left-to-right LM for generation (top-right and bottom-right, respectively), and update of the MLP using RL reward signals.

בגدول SQL ממוקם את התגמול הכללי אבל יחד עם זאת מנסה את "האקרואיות" של האסטרטגייה(שהיא בעצם אנטרופיה של התפלגות הטוקנים) . איך מושגים זאת? פשט מושגים איבר אנטרופיה לביטוי של פונקציית התגמול המקורית. בהמשך SQL מנצל את הקשר בין היקלט לשכבה softmax של מודל שפה בין Q-value שהוא תגמול ממוצע למצב (כל הטוקנים עד 1-) ופעולה (הטוקן הנבחר בסיבוב t) נתונים כדי לבנות פונקציית תגמול "נוחה".

כלומר האימון של RLPrompt מתבצע באופן הבא:

1. מכנים את "הגדרת המשימה" ל LM Policy (ראה אפנדייס A2 להסביר מפורט יותר)
2. מזינים את השיכון (embedding) של המשימה - MLP שמודzia לו פרומפט עבור המשימה
3. מכנים פרומפט זה למודל שפה שעבורו אנו מייצרים אותו יחד עם הדוגמאות שיש לנו (few shot learning)
4. מחשבים ערך פונקציית התגמול (וגם Q-value) עבור הפלט של מודל שפה
5. מבצעים עדכון של האסטרטגייה (בגدول מעדכנים את הממשקים של ה-MLP) על סמך הערכים שהיחסבו בסעיף הקודם.

משימות שנבחנו:

השיטה המוצעת ניתנת ליישום עבור מרחב גדול של משימות. במדידה התרցזו בשתי משימות עיקריות: קלסיפיקציה וגינרוט.

1. **קלסיפיקציה: משימת Few-Shot Text Classification:** סיווג של טקסט תוך שימוש במספר קטן של דוגמאות אימון. מדובר על דאטאוטס פופולריים למשימות סיווג סנטימנט וסיווג נושאים בטקסט. משימת הקלסיפיקציה שקופה למשימה של בחרית ה- tokens אשר בפורמט "[MASK] [Prompt] [Input]" ממקסימים את ההסתברות ל MASK token.
2. **גינרוט: משימת Text Style Transfer Text:** בהינתן טקסט מקור, יש לכתוב אותו מחדש בסגנון יעוד. למשל משפט בסנטימנט חיובי שנרצה לכתוב מחדש בסנטימנט שלילי ("האוכל טעים" ← "האוכל מגעל"). המדידה נעשית באמצעות הערכה ידנית של מת'יגים, וכן באמצעות חישוב ציונים של Content (מידת שימוש התוכן), Style (מידת הדיווק בסגנון הרצוי) ו- Fluency (מידת הרהיטות // שטף) עבור הטקסט המגינורט.

ניתוח תוצאות:

עבור משימת קלסיפיקציה, השיטה המוצעת מראה שיפור משמעותית על פני שיטות אחרות כמו Prompt Tuning ו- Instructions, ולמעשה מושגה ביצועים משופרים על כל ה- benchmarks.

עבור משימת הגינרוט, השיטה המוצעת מסוגלת ללמידה פרופטיטים ללא שימוש במידע מתויג. בהשוואה לשיטות אחרות, מدد ה- Content השיג ביצועים מעט נמוכים יותר, ואילו במדד ה- Fluency נרשם שיפור משמעותי.

כמו כן, התוצאות מראות כי בהרבה מהמרקמים פרופטיטים שטוביים עבור משימות downstream הם חסרי קוורנטיות, דוגמא לפרופט נלמד עבור משימת סנטימנט: "Compare (=) either". חוסר קוורנטיות של הפרופטיטים מקשה באספקט של פרשנות והבנה, ומכאן שמודלי שפה עושים שימוש שונה בפרופטיטים מאשר משתמש אונשי>.

Review 25: Improving Self-supervised Learning with Automated Unsupervised Outlier Arbitration

פינט הסוקר:

המלצת קרייה ממוקד וברהמ: שווה קרייה לחובבי למידה ייצוגית (unsupervised learning)

בஹירות כתיבה: ביןונית

ידע מוקדם:

- עקרונות בסיסיים של למידה ייצוגית (representation learning)
- שיטות אימון ניגודיות (contrastive learning)
- importance sampling

ישומים פרקטיים אפשריים: שיפור באיכות הייצוג של דאטה המופק באמצעות מגוון שיטות של למידה ייצוגית

פרטי מאמר:

מאמר: זמן להורדה.

קוד: כאן

פורסם בתאריך: 15.12.21, בארכיב.

הציג בכנס: NeurIPS 2021 Poster

תחומי מאמר:

self-supervised learning •

כליים מתמטיים, מושגים וסימונים:

- Importance sampling
- Radon-Nykodim derivative

מבוא:

אחת הדרכים המקובלות ביותר להגדיל את מ Lager הדאטה לאימון של מודל היא באמצעות אוגמננטציות - לדוגמה מהמארג שיש לנו ומשנים אותו במגוון צורות. למשל, נניח ויש לנו תמונה של חתול, אז גם סיבוב של

התמונה, חיתוך שלה בזרויות שונות, שינוי הגודל ועוד כמה טרנספורמציות (אגמננטציות) נוספות, אין-Amorot לשנות את העובדה שבתמונה יש חתול. על ידי פעולות פשוטות אלו ניתן ליצור מתמונה אחת עוד תמונות רבות השייכות לאוֹתָה קטגוריה. העובדה שאגמננטציות מסוימות של הדוגמה המקורית שייכות לאוֹתָה הקטגוריה כמו הדוגמה המקורית הינה בעלת ערך מוסף, כיון שלא רק הגדלנו את הדאטסהט אלא הוספנו דוגמאות מתייגות. גם כאשר אין לנו כלל דатаה מתייג ואנו רוצים להפיק ייצוג חזק של דטהה שעשו לשמש למשימות downstream, אוגמננטציות יכולות להועיל מאוד לה כדי "לرمוז" למודל לגבי פיצרים סמנטיים חשובים של הדטה.

הנחהה המסתתרת מאחריו השימוש באגמננטציות הינה פשוטה והגיונית, אך כפי שנראה, היא לא תמיד מתקיימת. בעצם אנו מניחים כי הדוגמאות הן אינוריאנטיות לאוגמננטציות, כלומר טרנספורמציות מסוימות אינן משנה את המאפיינים העיקריים של הדוגמה: התמונה לאחר אוגמננטציה עדין שייכת לאוֹתָה קטגוריה, והתוכן הסמנטי שלה נשמר. במאמר הנסקר מעררים על הנחה זו ומראים שהיא עלולה להיות בעייתית. המחברים מראים דוגמאות שעבורן אוגמננטציות מסוימות משנהות את התוכן הסמנטי של התוצאה.

המחברים דנים באימון מודלים על דטהה לא מתייג, הנקראת למידת ייצוג (representation learning), ומראים כי אוגמננטציות עלולות לפגוע ביכולת ההכללה של המודל המאמן, ומציעים פתרון אלגנטי להתחומות עם בעיה זו.

הרעין הבסיסי:

הסבר על הבעיה:

כאמור המאמר מנסה לטפל בבעיות דוגמאות חייבות "שקריות" שועלות במהלך בדיקות למידת ייצוג (representation learning) בפרט אלה ש商量וטות על שיטות ניגודיות (contrastive methods). בשיטות למידה ניגודית זוג דוגמאות חייבות מוגדר בניי משתי אוגמננטציות של אותה דוגמה. ההנחה המרכזית בשיטות אלו אומרת כי דוגמאות אלו הן בעלות אותו תוכן סמנטי. בדוגמא היזואלי (קרי תמונה) זוג של דוגמאות חייבות יכול להיות שני פאצ'ים שונים (או crops) של אותה תמונה או שתי טרנספורמציות של אותה תמונה (למשל שני סיבובים שונים).

אך גישה פשוטנית זו טומנת בחובה מוקש פוטנציאלי: למשל אם בתמונה יש שתי חיות, חתול וכלב, זוג של דוגמאות חייבות עלול להכיל פאץ' בו מוצג כלב ופאץ' שני בו מוצג חתול. פונקציית הלס הניגודי תנסה לקרב את הייצוגים של שני הפאצ'ים, על אף שהתוכן הסמנטי שלהם מאד שונה.

铭记 כי ההנחה המרכזית מאחוריו שיטת למידה ניגודית אומרת כי ייצוגים של דוגמאות "דומות" (= חייבות) צריכים להיות קרובים למרחב הייצוג והייצוגים של דוגמאות לא דומות צריכים להיות רחוקים.

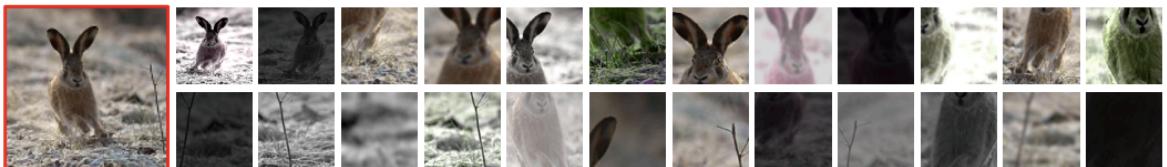


Figure 1: Illustration of OOD samples sampled from distribution \tilde{p} . Figures are ranked according to a descent order of its associated $w_{i,j}$. The biggest image in the red box is the original instance input x_i .

הערה: ניתן להשתמש בשיטה המוצעת במאמר גם עבור שיטות למידת ייצוג שלא משתמשות באופן מפורש בהנחהasis היסוד של הגישה הניגודית (קירוב יציגים של דוגמאות חיוביות והרחקה של אלו עבור דוגמאות שליליות). בין השיטות הללו נמנota בין השאר **SwaV** ו- **ByOL** (אשר משתמש בזוגות חיוביים בלבד). בהמשך נדון עיקרי בשימוש בשיטה המוצעת עבור גישות ניגודיות קלאסיות.

המאמר הנסקר מנסה לתת מענה לבעיית הזוגות החיוביים ה-**"שקרים"** באמצעות משקל אדפטיבי כאשר תרומה של כל זוג חיובי תהיה פרופורציונלית למידת **"אמיות"** שלו. כלומר, עבור זוג דוגמאות חיוביות נשערת את הסבירות שהן אכן מכילים את אותו התוכן הסמנטי. ככל שהסבירות הزادה גבואה יותר, הצוין שהזוג מקבל גבואה יותר והתרומה שלו לפונקציית הלוס גם היא גבואה יותר. גישה זו דומה ל-**Sampling Importance**, טכניקה לדגימה מהתפלגות מורכבת המשקלה באמצעות דגימה והתפלגות פשוטה יותר ומשקל של דגימות אלו.

פרטים נוספים:

כעת נבין את העקרונות המתמטיים של הגישה המוצעת במאמר. קודם כל נזכיר מבנה של פונקציית הלוס של שיטת למידת ייצוג כלשהי. פונקציית L זו היא ממוצע של ערכי הלוס על פני מספר מיני-באזים בינוים מזוגות חיובים (ולפעמים מיני-באז', כולל גם דוגמאות שליליות, הנבחרות בדרך כלל רנדומלית). ערך פונקציית L oso של מיני-באז' הוא סכום ערכי פונקציית L עבור הזוגות המרכיבים מיני-באז'. אבל מה היא L ?

פונקציית L מקבלת יציגים של דוגמאות חיוביות (ולפעמים שליליות) ומודדת "מידת התאמה של יציגים אלו להנחהasis היסוד של השיטה".

דוגמאות של פונקציה עבור כמה שיטות למידת הייצוג:

- **MoCO** - פונקציה L היא יחס מרתקים בין יציגים של זוגות שליליים לבין אלה של הזוגות החיוביים.
- **SWaV** - פונקציה L היא מרחק בין קלאסטרים של דוגמאות חיוביות.
- **ByOL** - פונקציה L היא מרחק $2L$ בין יציגי דוגמאות חיוביות (אין דוגמאות שליליות).

לאחר מכן, מגירים סט דוגמאות חיוביות (ולפעמים גם שליליות) ומחשבים את הערך של L על הסט זהה.

עכשו נשאלת השאלה מאי זו התפלגות אנו דוגמים טרנספורמציות (אגמננטציות) המניבות לנו זוגות חיוביים. קודם כל, רצוי להשתמש בזוגות של טרנספורמציות שייצרו תכונות בעלות תוכן סמנטי זהה, או לפחות דומה, בסבירות גבואה. אולם חוק התפלגות (נסמן אותו P - (P)) של זוגות טרנספורמציות אלו אינו ידוע ובנוסף הטרנספורמציות עשויות להיות תלויות בדגם עצמה. כלומר, שני קורפים זהים יכולים להכיל תוכן סמנטי זהה לתמונה אחת (למשל שני חתולים) ותוכן שונה (למשל חתול חדש) עבור תמונה אחרת.

במטרה להתגבר על המכשול הזה ולדגם מההתפלגות הטרנספורמציות הזו, נשתמש בשיטה הנكرةת (**IS**) **importance sampling**. כאמור IS מאפשרת לדוגם מההתפלגות P , אשר ניסיון לדוגם ממנו באופן ישיר דגימות רבות, באמצעות התפלגות אחרת Q , ממנה ניתן לדוגם יותר בקהלות. המשקל של דגימה x הוא היחס $(x)/Q(x)$. כלומר, דגימות בעלות יחס גבואה מקבילות משקל גדול יותר ולהיפך. במקרה שלנו, ההתפלגות Q תהיה ההתפלגות שמננה אנו דוגמים אוגמננטציות לבנייה של זוגות חיוביים של דוגמאות.

אבל יש לנו בעיה כאן. אנחנו לא יודעים לחשב את $(x)/P$ באופן מפורש, כלומר אין לנו דרך לדעת מהי ההסתברות שזוג אוגמננטציות יוביל לתכונות בעלות אותו תוכן סמנטי. מזלנו אנחנו כן יכולים לחשב בקירוב את היחס של P - Q זהה למשה הרעיון העיקרי של המאמר. הקירוב מתבסס על כך שרוב האוגמננטציות שבדרכן כל משמשים בהם בلمידת יציג כנ שומרות על אותן תוכן סמנטי ויש יחסית מעט ככל שלא מקיימות את התוכנה הזו. התובנה העיקרית היא שניתן להזות אוגמננטציות שלא מקיימות את התוכנה הزادה באמצעות ניתוח של מרחק מהייצוג

הממוצע z_{mean} המתkeletal מתמונה נתונה לאחר הפעלת מספר אוגמנטציות (מוסמן בתור M במאמר). כלומר אם יציג של תמונה לאחר אוגמנטציה A רחוק מ- z_{mean} (גם השונות נלקחת בחשבון כאן) אז ניתן להסיק כי A אינה שומרת על התוכן הסמנטי.

אם כך, המשקל w של אוגמנטציה A מוגדר כמרקח יציג הדוגמה לאחר A מהייצוג הממוצע z_{mean} (במנוח שנות המוחשבת על פני כל הדוגמאות במיני-באץ):

$$w_{i,j} = \exp[-(\mathbf{z}_{i,j} - \boldsymbol{\mu}_i)^T (\tau \boldsymbol{\Sigma})^{-1} (\mathbf{z}_{i,j} - \boldsymbol{\mu}_i)],$$

$$\boldsymbol{\mu}_i = \frac{1}{M} \sum_j^M \mathbf{z}_{i,j}, \quad \boldsymbol{\Sigma} = \frac{1}{NM} \sum_i^N \sum_j^M (\mathbf{z}_{i,j} - \boldsymbol{\mu}_i)(\mathbf{z}_{i,j} - \boldsymbol{\mu}_i)^T.$$

כאשר הפרמטר τ שולט ב"יחס התלות" של משקל w במרקח הנ"ל, וככל שהוא נמוך יותר המשקל יהיה יותר מלא במרקח המקורי.

אוף מעת יותר פורמלי: נסמן את ההתפלגות של האוגמנטציות ה"רצויה" ב-P. התפלגות זו אינה ידועה לנו, ונdagoms ממנה באמצעות היוריסטייקה מההתפלגות Q, המכילה את כל האוגמנטציות "הריגילות" שבדרך כלל שומרות על התוכן הסמנטי כמו קרוב או סיבוב. ההתפלגות Q כן ידועה לנו ונרצה להיעזר בה על מנת לדגום מ- P באמצעות שיטת sampling的重要性 (IS). עבור זוג דוגמאות i ו- j (שהן התמונה המקורית וגרסתה לאחר הפעלת אוגמנטציה A_j), נרצה לחשב את היחס באופן מפורש, כפי שראנו לא יכולם לחשב את היחס באופן מפורש, כפי שראינו יודעים את ההתפלגות הרצiosa של אוגמנטציות P, ונרצה לשער את היחס זהה (נסמן אותו בתור w_{ij}). משקל w_{ij} ייכנס לפונקציית הלוס, וינסה לתת לאוגמנטציה זו את המשקל "ההולם" עבורה ביחס לדוגמה המקורית. ככל שהאגמנטציה שומרת יותר על התוכן הסמנטי של התמונה כך המשקל שלו יהיה גבוה יותר ואילו משקל האוגמנטציות ה"לא טובות" יהיה קרוב ל-0. ניתן לשער את הערך של w_{ij} באמצעות מරחק (מאוד דומה למראק Mahalanobis) של יציג התמונה לאחר אוגמנטציה A_j מהייצוג הממוצע z_{mean} של M אוגמנטציות שונות של התמונה.

הישגי מאמר:

המאמר השווה אספקטים רבים של ביצועי הגישה המוצעת עם שיטות SOTA רבות, אך החשובה העיקריות ביניהם היא ההשוואת ייצוגים המופקים באמצעות הטכניקה המוצעת עם אלו של שיטות supervised обучות שמשימות סיווג ויזיהו אובייקטים. השיטה המוצעת מצליחה להשיג את הביצועים הטובים ביותר, אך השיפור על פני אלגוריתמים אחרים לא גדול.

Table 6: Accuracy of linear classification model on ImageNet1K. Bold numbers are the best performance among models trained for 200 epochs. Numbers (+x%) denotes additional gain compared to the baseline model (i.e., SwAV without the table) without UOTA approach. * denotes results represented from [3, 9]. / means results of our reproduced reproduced based on SwAV official code.

Method	Epochs	Batch size	Top-1 (%)	Top-5 (%)
CPC-v2 [21]	200	12	63.8	85.1
CMC [39]	240	/	64.8	86.1
MoCo [18]	200	256	60.6 [†]	83.1 [†]
MoCo-v2 [8]	200	256	67.6 [†]	88.0 [†]
ICL [3]	200	256	68.7	89.0
SimCLR [7]	1000	4096	69.3	89.0
SimSiam [9]	200	256	70.0	/
InfoNCE [40]	200	256	70.1	89.4
BYOL [15]	200	4096	70.6 [†]	/
Barlow Twin [47]	1000	2048	73.2	91.0
SwAV [5]	200	256	72.7 [‡]	91.5 [‡]
SwAV+UOTA (Ours)	200	256	73.5 (+0.8%)	91.8 (+0.3%)

Table 7: Performance on downstream tasks: object detection [35] (left), instance segmentation [19] (middle) and keypoint detection [19] (right). Accuracy in %. All models pretrained 200 epochs and finetuned on MS COCO with 1× schedule.

Model	Faster R-CNN + R50-FPN			Mask R-CNN + R50-FPN			Keypoint R-CNN + R50-FPN		
	AP _{bbox}	AP _{segm}	AP _{kp}	AP _{bbox}	AP _{segm}	AP _{kp}	AP _{bbox}	AP _{segm}	AP _{kp}
random	30.1	48.6	31.9	28.5	46.8	30.4	63.5	85.3	69.3
unsupervised	38.2	59.1	41.5	35.4	56.5	38.1	65.4	87.0	71.0
MoCo [18]	37.1	57.4	40.3	35.1	55.9	37.6	65.6	87.1	71.3
MoCo-v2 [8]	37.6	57.9	40.8	35.3	55.9	37.9	66.0	87.2	71.4
ICL [3]	38.1	58.3	41.3	35.6	56.2	38.3	66.2	87.2	72.3
InfoNCE [40]	/	/	/	36.7	57.7	39.4	/	/	/
SwAV	38.5	60.5	41.4	36.3	57.7	38.9	65.6	86.9	71.6
SwAV+UOTA	39.0	61.0	42.0	36.7	58.4	39.4	66.3	87.4	72.3

לט'יכם, מדובר במאמר מאד מעניין המציע דרך להתמודד עם אוגומנטציות שלא משמרות את התוכן הסמנטי של תמונה במהלך למידה "צוגית על DATA" ללא מטאסתים לא מתוארים.

שיטת פעולה: הסקירה נכתבת על ידי [מichael erlihson](#), [michael erlihson](#) וברහם רביב.

Review 26: What does a platypus look like? Generating customized prompts for zero-shot image classification

פינית הסוקרי:

המלצת קרייה ממיק וליואר: מומלץ למי שמתעניין במשימות סיווג DATA ויזואלי עם מיליון פתח (של קטגוריות)

בחירה כתיבה: בינונית.

ידע מוקדם:

- הבנה בעקרונות של מודלי שפה
- הבנה בסיסית בפרומופטים
- ידע במודלים cross-domain כמו CLIP ובסיווג עם מיליון פתוח

ישומים פרקטיים אפשריים:

- יצירת מהירה של פרומופטים למשימות סיווג בעלות מיליון קטגוריות פתוח

פרטי מאמר:

[לינק למאמר: זמין להורדה.](#)

[לינק לקוד: כאן](#)

פורסם בתאריך: 2022.09.07, בארכיב.

הציג בכנסו: ---.

תחומי מאמר:

- סיווג תמונות באמצעות מילון פתוח (open-vocabulary classification)

כליים מתמטיים, מושגים וסימונים:

- מודלי שפה גדולים (LM) כמו GPT3
- מודלים cross-domain המאפשרים סיווג zero-shot של תמונות

מבוא:

מטרת משימת סיווג תמונות היא לאמן מודל לזהות הקטגוריה של התמונה נתונה. בעבר משימה זו הינה קיומ של מילון קטגוריות קבוע מראש ולא משתנה במהלך אימון המודל (למשל 1000 קטגוריות של ImageNet). בשנה האחרונהנו רואים יותר ויותר מאקרים שימושים בגישה מבטיחה לסיווג תמונות שהיא מבוססת על מילון קטגוריות פתוח (open vocabulary classification - OVC). בשונה משיטת סיווג ישנות יותר OVC מאפשרת סיווג תמונות עם **קבוצה של קטגוריות ולא סגורה** של קטגוריות המוגדרות באמצעות שפה טבעיות. למשל תמונה של דוב יכולה להיות מסווגת עם מודל OVC בתור "דוב שחור אמריקאי שנפוץ בארצות הברית הצפונית".

מודלי OVC שהיגו ביצועים גבוהים על משימות סיווג על מספר רב של נתונים **בහדר דעתה מתייג** (כלומר zero-shot). איך זה קרה, אתם שואלים? מודלים אלה מננים כמויות אדירות של צמדים **תמונה-טקסט** (= תמונות עם כתורת) זמינים באינטרנט כדי למפות אותם (תמונות והתייאר שלהם) לאוטו מרחב לטנסי. במרחב לטנסי זה השיכונים (embeddings) של תמונה והcotורת שלה נמצאים קרוב אחד לשני כאשר השיכונים של תמונה וtekst לא קשור אליה מוקמים רחוק אחד מהשני. הדוגמא המפורשת ביותר של מודל זה המנצל בצורה אינטנסיבית במספר משימות ML היא [CLIP](#).

מודלים כאלהאפשרים לסיווג תמונות על ידי הדמיון בין ייצוגי התמונה והcotורת. כדי לסיווג תמונה נתונה יש צורך ביצירת **פרומפטים** (prompts) המתאימים לכל קטgorיה בΖורתה המטיבית. לאחר מכן הדמיון בין השיכון של הפרומפט הטוב ביותר לקטgorיה לבין שיכון התמונה יספק את מידת ההתאמה של קטgorיה זו לתמונה. באופן זה נוכל לבצע סיווג ללא אימון נוספת וללא צורך בدادה מתייג (כלומר zero-shot).

תמצית מאמר:

הגישה המתוארת הינה מאוד נוחה לשימוש ועשויה לחסוך לא מעט זמן אך היא טומנת בה מוקש קטן והוא מתחבא במבנה פרומפט המיציג קטגוריה נתונה בדרך הטובה ביותר. הגישה הסטנדרטית היא לייצר כמה תבניות גנריות לפרומפטים כמו "תמונה של {קטgorיה}" ואז ליצר פרומפטים לכל קטגוריות של המשימה. לאחר מכן אנו מחשבים דמיון בין השיכונים של סט הפרומפטים לבין השיכון של התמונה ומסוגים את התמונה לפי הקטגוריה עם סט הפרומפטים הći דומה לה שיכון התמונה.

לשיטת זו יש כמה חסרונות משמעותיים. ראשית, כל פרומפט בנייתו בצורה ידנית וזה מצריך בניה מחדש של פרומפטים עבור כל דאטסהט חדש שהופך פעולה זו ללא סקילבלי. שנית, הפרומפטים חייבים להיות כלליים מספיק כדי לחול על כל קטגוריות התמונות. לדוגמה, פרומפט חייב להיות כללי מספיק: *ImageNet* הקטגוריה של פלטיפוס ([platypus](#)) יכול להיות "תמונה של {פלטיפוס}" ולא יכולה להיות משהו כמו "תמונה של {פלטיפוס}, יונק מימי" כי זה לא יתאים לא קטגוריות אחרות. לבסוף, כתיבת פרומפטים איקוטיים עם דרישת ידע על הדאטסהט עצמו שלא ניתן להקלילו על דאטסהטים אחרים וזה מאריך את הזמן הנדרש לבניית מודל.

המאמר מציע גישה חדשה לבניית פרומפטים שנוננת מענה לאתגרים המתוארים בפסקה הקודמת. במקום לבנות פרומפטים בצורה ידנית החוקרים מוצאים מודל שפה גדול לבנייתם. ההתערבות האונושית נדרש רק בשלב הראשון לבנייה של כמה פרומפטים כלליים בוודאים כמו "איך נראה פלטיפוס?" וכדומה. למרות שהוא דרוש קצר "הנדסה ידנית", זה מתגמד מול כמה פרומפטים שצריך לייצר בשיטה הסטנדרטית (הנדסה לעיל). פרומפטים אלו נקראים פרומפטி *MLL* במאמר. כדי ליצר פרומפטים שנייתן לנצל אותם למשימת *OVC*, מזינים פרומפטים אלו למודל שפה מאומן (המאמר משתמש ב-[GPT-3](#) למשימה זו). פרומפטים אלו נקראים פרומפטי התמונה (.image prompts).

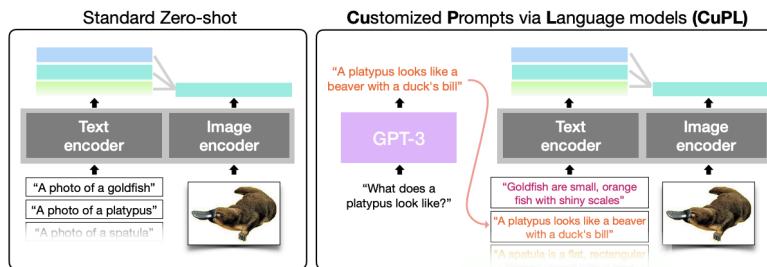


Figure 1: **Schematic of the method.** (Left) The standard method of a zero-shot open vocabulary image classification model (e.g., CLIP [29]). (Right) Our method of CuPL. First, an LLM generates descriptive captions for given class categories. Next, an open vocabulary model uses these captions as prompts for performing classification.

פרטים נוספים של הגישה המוצעת:

המחברים ניסו את שני הוריאנטים הבאים של גישה זו:

CuPL Single Prompt: כתיבה של פרומפט אחד לכל הדאטסהטים לפי הטמפליט הבא: 1.

"Describe what a(n) {category}, a type of __, looks like"

החלק המודגש מכיל סוג כללי שהקטגוריה שיכת אליו (כמו חיית בית או מטווס לדאטסהטים כמו *Oxford* או *FGVC Aircraft Pets*). לדאטסהטים כלליים יותר כמו *ImageNet* חלק זה נמחק מהפרומפט.

.2 CuPL Full Prompts - שימוש בפרומפטி LLM שונים לכל דאטהסט (בסק הכל 5 לכל דאטהסט).

למשל ל-ImageNet הפרומפטים הבאים נוצרו:

- a. "Describe what a(n) {} looks like",
- b. "How can you identify a(n) {}?"
- c. "What does a(n) {} look like?"
- d. "A caption of an image of a(n) {}:"
- e. "Describe an image from the internet of a(n) {}"

המחברים מצינו שהווריאנט השני דורש יותר מאמץ לייצירה של פרומפטים אלו אך עדין בכמות נמוכה מאשרו מלה שנדרש בשיטות הקודמות.

לאחר הייצירה של פרומפטי LLM לכל קטgorיה, הם מזונים למודל שפה גדול (GPT3) והפלט שלו משמש לייצירה של פרומפטי תמונה כאשר עברו כל פרומפט LLM נוצרם 10 פרומפטי תמונה. לאחר מכן מחשבים את השיכון (embedding) של פרומפטי התמונה שנוצרו לכל קטgorיה ומוצאים אותו (לכל קטgorיה בנפרד) כדי לבנות "ցוג" של כל קטgorיה. בשלב האחרון מחשבים את הדמיון בין השיכונים של הקטגוריות עם שיכון התמונה ומסווים את התמונה עם הקטgorיה בעלת דמיון הגבוה ביותר.

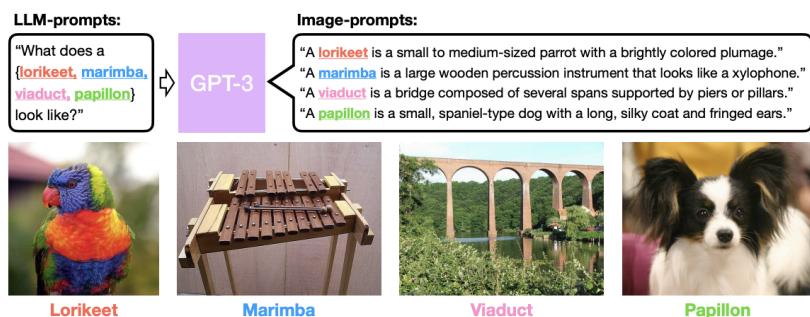


Figure 2: Example CuPL LLM-prompts and Image-prompts. LLM-prompts are filled in with a class name and then used as input to GPT-3, which then outputs image-prompts. Example LLM generated image-prompts and associated images from ImageNet are shown. Only image-prompts are used for the downstream image classification.

הישגי המאמר:

החוקרים ערכו ניסוי לבדיקת ביצועי הסיווג של שני הווריאנטים לגישה המוצעת לייצרת פרומפטים, ביחס לשיטה הסטנדרטית אשר משמשת כ-baseline. השיטות נבדקו על שמונה benchmarks מוכרים של סיווג תמונות בשיטת Zero Shot.

מעבר לתוצאות הסיווג נבדקו גם ההשפעות של גודל המודול, כמות הפרומפטים והמגוון שלהם על הביצועים.

על מנת למש OVC נדרש שכל קטgorיות תמונות תיוצג בשפה טבעית בצורה חד משמעית. לא בכל הדאטאסטים הדבר זמין. כך למשל, ב-ImageNet הקטgorיות מיוצגות כ-ID אשר יכול להיות ממוקה במספר מילים נרדפות ב-WordNet. לכן, בבדיקה זו הם השתמשו בתוויות כפי שהוגדרו [בעבודה קודמת בנושא](#).

תוצאות הניסוי:

	ImageNet [6]	DTD [5]	Stanford Cars [18]	SUN397 [39]	Food101 [2]	FGVC Aircraft [22]	Oxford Pets [25]	Caltech101 [9]	Total hand-written	Unique hand-written
standard [29] # hand-written	75.54 80	55.20 8	77.53 8	69.31 2	93.08 1	32.88 2	93.33 1	93.24 34	136	97
CuPL (single) Δ standard # hand-written	75.71 1	59.06 1	75.45 1	71.42 1	93.24 1	33.89 1	93.38 1	93.37 1	8	1
CuPL (full) Δ standard # hand-written	76.60 5	61.70 6	77.63 9	73.31 3	93.36 3	36.11 2	93.81 2	93.43 3	33	25

עבור כל דאטסהט מוצגים top 1 accuracy של הסיווג, הדلتא (ההפרש) ביחס לשיטה הסטנדרטית (ירוק = שיפור), ומספר הפרומפטים הידניים שנוצרו.

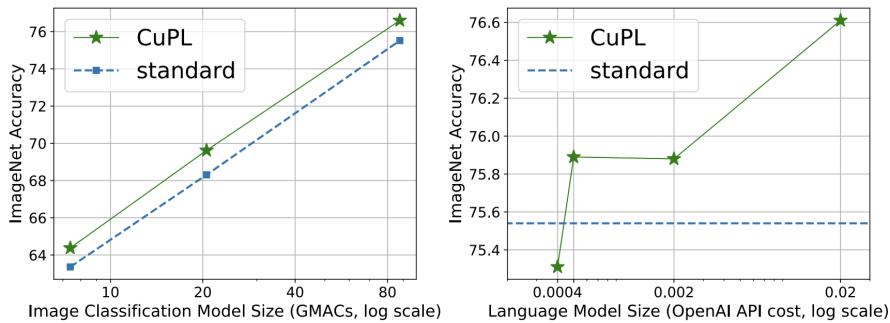
יש לשים לב שבקירה של השיטה הסטנדרטית מסpter הפרומפטים הידניים מתיחס לפרומפט התמונה, ובשיטות CuPL המספר מתיחס לפרומפט ה-LLM.

כאמור בשיטת CuPL Single, נדרש פרומפט ייחד לכל הדאטסהט, לעומת 97 סה"כ, בשיטה הסטנדרטית. מעבר לכך, הפרומפטים בשיטה הסטנדרטית נדרשו להיות מאוד ספציפיים לדאטסהט, למשל "תמונה בוחר לבן של {}" בעוד CuPL Single נדרשה רק מילה אחת נוספת - סוג הקטגוריה, כפי שצוין קודם.

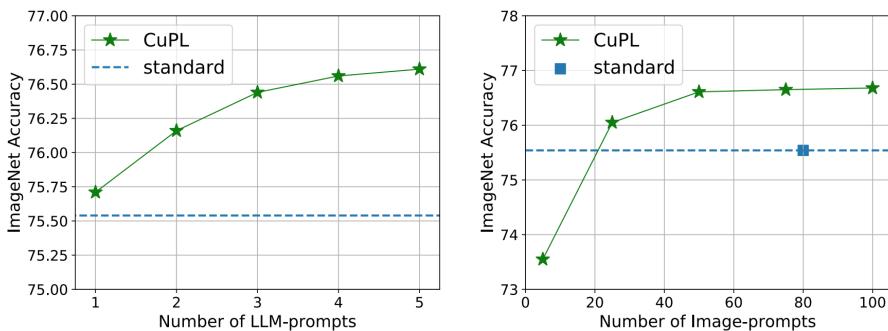
בשיטת CuPL full אמם נדרש מספר גדול יותר של פרומפטים ידניים מאשר CuPL-single אבל עדין הרבה פחות מאשר השיטה הסטנדרטית (דוגמה - 5 לעומת 80 ב-ImageNet). בנוסף מוצע שיפור משמעותית של מעל לאחוז בחלק מהדאטסהטים.

מעבר לתוצאות הסיווג הכלליות נבחנו גם השפעות של נושאים נוספים על הביצועים:

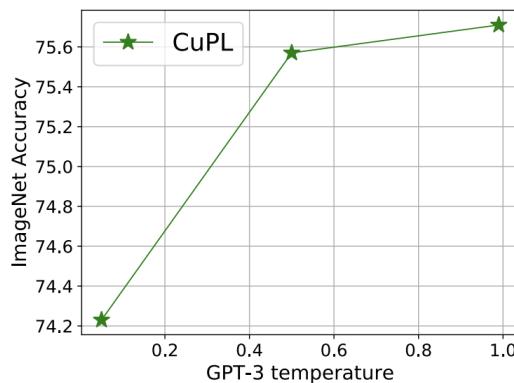
1. גודל המודל - לשם בוחינת נושא scaling, בוצעה השוואה בין השיטה הסטנדרטית לשיטת CuPL full עם ImageNet עבור גודלי מודל שונים - גם של מודל השפה (ימין) וגם של מודל הסיווג (שמאל). במקורה של מודל השפה הגרף של השיטה הסטנדרטית קבוע אחר והוא לא עושה בו שימוש. המסקנה היא שמודלים גדולים יותר יובילו לאחוזי דיקון גבוהים יותר.



2. כמות הפורומפטים - בוצעה השוואת ביצועים על גדלים שונים של כמות הפורומפטים (נבדקו בנפרד גם פורומפטי ה-LLM וגם פורומפטי התמונה). במקרה של פורומפטי ה-LLM ניתן לראות שיש שיפור כבר החל מפורומפט יחיד. במקרה של פורומפטי התמונה, עבור מספר קבוע של חמישה פורומפטי LLM נisos גודלים שונים. נמצא כי החל מסהפר של 25 פורומפטי תמונה, הגישה החדשה מתעללה על הביצועים של ה-LLM (אשר כאמור, משתמש בכ-80 פורומפטים ידניים ל-ImageNet baseline).



3. מגוון פורומפטים - על ידי עדכון ה-temperature של GPT-3 אשר מאפשר שילוב של מידת רנדומליות ביצירת הפורומפטים, נבחנה ההשפעה של המגוון. גם כאן הוכח שיפור כל שהפורומפטים היו מגוונים עבור ImageNet.



4. השוואת בין שימוש בפורומפטים לשימוש בהגדרות קטגוריתית תמונה - הגישה המוצעת נבחנה גם ביחס לשימוש בטקסט תיאורי שמקורו בהגדרת הקטגוריה. לאחר מכן נבוצע WordNet על ImageNet מבוסס על חלץ לכל קטגוריה את ההגדרה שלה ועליה לבצע עיבוד לפורמט מתאים. הביצועים שנרשמו פחותו טוביים מהגישה המוצעת:

Standard	CuPL	WordNet
75.54	76.60	73.44

המאמר מציג שיטה אלגנטית וטבעית לייצירה של פרומפטים למשימת סיווג VOC. השיטה מנצלת מודל שפה מאומן לייצירה של מגוון פרומפטים מסווג מועט של פרומפטים כלליים שהונדרו באופן ידני.

שיתוף פעולה: הפוסט נכתב על ידי מיכאל (מייק) ארליךסון, Michael Erlhson, PhD וליאור כהן, Lior Cohen

Review 27: Meta-AAD: Active Anomaly Detection with Deep Reinforcement Learning

פינת הסוקר:

המלצת קריאה מדע ומיון: מומלץ לאנשים שאוהבים Reinforcement Learning ו-Anomaly Detection.

בahirotכתיבת:

ידע מוקדם: Reinforcement Learning, Online Algorithms

ישומים פרקטיים אפשריים: SOC - Security Operation Center System

פרטי מאמר:

lienק למאמר: [זמן להזדהם](#).

lienק לקוד: [깃](#)

פורסם בתאריך: 16.9.20, בארכיב.

הוזג בכנס: ICDM 2020.

תחומי מאמר:

- **זיהוי אномליות**
- **למידה באמצעות חיזוקים** (RL - Reinforcement Learning)

כלים מתמטיים, מושגים וסימונים:

- למידה באמצעות חיזוקים (Reinforcement Learning)
- תהליכי החלטה מרקוביים (Markov decision process)
- PPO - Proximal Policy Optimization
- למידה عمוקה באמצעות חיזוקים (DRL - Deep Reinforcement Learning)

מבוא:

תחומים רבים נעזרים בטכניקות לזיהוי אונומליות כדי לפתור בעיות שונות, למשל בתחום הסיבר - לזיהוי התקפות סיבר, בתחום הרפואה - לזיהוי גידולים סרטניים וכדומה. לזיהוי אונומליות הינו משימה שבה המודל מתבקש לזהות דפוסים חריגים במידע, אליו השוניים באופן מובהק מרוב המידע. גישה זו לרוב מיושמת על ידי אלגוריתמים לא מפוקחים (Unsupervised). לעיתים קיימן דטה מתויג ונינע למfn' אותו לזיהוי אונומליות ספציפיות. אלגוריתמים לזיהוי אונומליות מניחים הנחות על דפוסי ההתנהגות של אותו מידע חריג.

כל שיטה לזיהוי אונומליות מtabסת על סט הנחות המגדירות מהי אונומליה. למשל EOF מינחה כי מידע תקין יהיה מרוכז באשכול, ככלומר כל נקודה תהיה קרובה לנקודות אחרות. לעומת זאת, אונומליה שונה משאר המידע ולכן תהיה באחור פחות מרוכז, שהאלגוריתם יוכל לזהות. הנחות אלו עלולות להביא לחוסר התאמה בין מה שהאלגוריתם מגדר לבין מה שהיא משתמש באלגוריתם מגדר אונומליה.

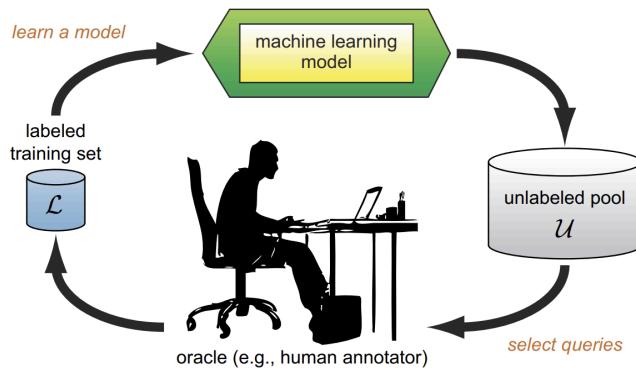
מערכת העשויה שימוש באלגוריתמים כאלו עלולה לסבול מחוז גבוה של FP - False Positive. לכן, לעיתים קרובות שיטות לזיהוי אונומליות משתמשות בגורם אנושי הבוחן את הדוגמאות שהוגדרו כאונומליות, ומחליט האם מה שהוגדר כאונומליה, אכן הוא אונומליה. לצורך כך, נשאף למקסם את אחוז האונומליות שהאלגוריתם ישלח לתויג במסגרת תקציב שנקבע מראש. זאת בשונה מסתם שליחה של דוגמאות אקרראיות לבניין לשפר את זיהוי האונומליות. ההבדל הוא שבגישה זו, חשוב לחושף את האלגוריתם גם לדגימות תקינות נוספת לאונומליות, כדי שיוכל להפריד בין שני הסוגים.

עם זאת, שימוש בגורם אנושי הינו יקר ולכן נרצה לנצל את זמנו בצורה אופטימלית, ככלומר לא לבודבב אותו על דוגמאות אשר יתבררו כ-FP. כאן באהה כדי ביטוי הבעיה שכותבי המאמר מנסים לפתור: מזעור אחוז ה- ϵ -FP, או לחלופין מקסום אחוז ה- ϵ -TP, בקשר האונומליות שהועברו לבוחן. ההנחה כאן כי תהליכי זיהוי אונומליות מערב בוחן אנושי אשר יסוג את האונומליות מתוך רשימה של אונומליות המופקת על ידי המערכת באופן אוטומטי, והמערכת תחשב ציון אונומלי (anomaly score) לכל דגימה בהתבסס על המשוב מהבוחן. בתורו, הבוחן ינסה לחקור כמה שיטות אונומליות במסגרת ציון קצובה ("התקציב") ולזהות אלו מהן הן אכן אונומליות, ואילו לא. סיטואציה זו פותחת דלת לתרחיש מעניין שבו המערכת עשויה לנfn' את הבדיקה מהגורם האנושי באופן הבא:

1. אונומליות הדומות לאלו שהבוחן סימן אמיתיות, יקבלו ציון גובה יותר באיתרציה הבאה ורק יגדל הסיכון שלහן להיות מזוהות אונומליות.
2. דוגמאות שסומנו כתקינות על ידי הבוחן, יקבלו ציון נמוך יותר שיוריד את הסיכון של דוגמאות דומות להישלח לתויג להבא.

קיימות שיטות שבוחרות את הדוגמאות בעלות הפוטנציאל הגדול ביותר להיות אונומיות. האנאליסט מתייג דוגמאות אלו, האלגוריתם מפיק מהן ידע, שוב מריצים אותו על הדאטה ובוחרים דגימות נראות אונומיות, וחוזר חלילה עד תום תקציב התקציב.

דוגמה ויזואלית ניתן לראות כאן בציור הבא:



שיטות אלו אכן מסוגלות להביא לביצועים טובים בטוווח הקצר, אך עלולות לסבול מביצעים לא אופטימליים בטוווח הארוך. הסיבה לכך היא קיום דוגמאות עם ציון אונומליה נמוך, אך שmagמלות בתוכן אונומיות מסווג שוניה שעדיין לא נחקר (דוגמה לכך ניתן לראות [כאן בפרק 3.1](#)). בטוווח הקצר השיטות הקיימות פועלות באופן חמדני, ככל מרב בוחרות מבין האונומיות את אלו עם הציון הגבוה ביותר, ולכן אונומיות בעלות ציוןBINONI עשויה לא להישלח לתקציב כלל. כתבי המאמר טוענים שגם כן ניתן לחשב בדוגמאות אלו, הן עלולות לגרום לתוצאות פחות טובות בטוווח הקצר, אך בטוווח הארוך הן יגרמו לאונומיות חדשות ומעניינות להיבחר גם כן. כך הגורם האנושי יכול לחקור אונומיות שאחרת לא היה רואה, שכן השיטות החמדניות היו מראות לו את אותן אונומיות שוב ושוב. תרחיש זה הוא שהביא את החוקרים לחקור שיטות שמתיחסות לטוווח הארוך.

מידול הטוווח הארוך טומן בו מספר אתגרים:

- בדרך כלל מרחיב החיפוש (= סט כל הדוגמאות) הינו עצום, ונצרך לעבור על כלו כדי לבחור את הדוגמה שתשתקוף את הביצועים בטוווח הארוך.
- כל דאטasset הינו שונה וייה קשה למצאו אסטרטגיית בחירת דוגמאות גנרטיב עבר כולם.

ניסוח הבעיה:

כדי לנסוט לפטור את האתגרים הנ"ל, כותבי המאמר מציעים את שיטת MetaAAD. הבעיה שנותנו מנסים לפתור הינה בחירת הדוגמאות עם ההסתברות הגבוהה ביותר להיות אונומיות תחת תקציב מסוים T , מספר הדוגמאות שהובחנו מתייג. במאמר המסורק, הבעיה מנוסחת באופן הבא: עבור דאטasset X המכיל n דוגמאות x_1, \dots, x_n , ו- y_i המסמן את מצב התקציב של דוגמא x_i . מצב התקציב $\{y_1, 0, 1, \dots, 1\}$ – i – מיצג דוגמא שנשלחה לתקציב וסומנה כאונומליה, 1 מסמן דוגמא לא אונומלית ו-0 מסמן דוגמא לא מתזגות. בהתחלה, כל הדוגמאות מאותחלות עם $y_i = 0$, כלומר אף דוגמא לא מתזגת. בכל שלב, דוגמא אחת תבחר לתקציב, קלומר מצבה ישנה מ-0 ל-1, $y_i = 1$ בהתאם לתשובה הבוחן. בהינתן תקציב T שאלות שניות לשולח לבוחן,

מטרתנו הינה ללמידה מדיניות π לבחירת דוגמא שתישלח לתיאוג בכל איטרציה, במטרה למקסם את מספר הדוגמאות שתויגו כאנומליה במסגרת התקציב T .

הסבר על מושגים רלוונטיים:

כותבי המאמר מגדלים את הבעה בתור MDP (ראה נספח בסוף הסקירה). המטרה של MDP הינה ללמידה את האסטרטגיה הממקסמת את התגמול הכללי, אך איך נמדדת המדיניות הטובה ביותר? במאמר זה התעולת נוסחה כתגמול המצטבר המוזל הצפוי:

$$E_{\pi} [\sum_{t=0}^{\infty} \gamma^t * r_t] = \gamma * r_1 + \gamma^2 * r_2 + \dots + \gamma^t * r_t$$

כאשר $1 < \gamma < 0$ הינו פקטור ההזנחה (discount factor), המבטא ירידת ערךו של התגמול t צעדים אחריו פועלה פי פקטור של γ^t . פקטור זה הינו קבוע שmagder מראש.

הרעילון הכללי מאחורי השיטה:

כאשר מאמנים שיטה על דאטasset מסוים, לא ניתן להבטיח כי היא תעבור על דאטasset בעל מאפיינים שונים ממנו. כותזאה מכך יש צורך לבנות מטא-מאפיינים מספיק גנרים ורוביוטיים כדי לאפיין אנומליות בדאטassets רבים. נזכיר כי מטרתנו הינה למצוא את מספר האנומליות הגדול ביותר במסגרת תקציב תיוג T ונרצה להשתמש בmeta-מאפיינים שייתרמו לנו למטרה זו. החוקרים השתמשו במאפיינים הבאים:

- **מאפייני גלאים** (Detectors): ציוני האנומליה שהושבו על ידי גלאי אנומליה מבוססי למידה לא מפקחת. כל אלגוריתם גלי אנומליות בסיסי יכול ליפק לנו מאפיין שכזה.
- **מאפייני אנומליות**: מאפיינים אלו מתארים עד כמה דוגמא "דומה" לאנומליות המתואגות בדאטasset (כל שהשיטה תróż יותר זמן ונקל יותר תיוגים מהבחן, מאגר האנומליות המתואגות יגדל). תחת קטgorיה זו נכללו 3 מאפיינים:
 - המרחק האוקלידי המינימלי וה ממוצע מהדוגמא לדוגמא אנומלית (2 מאפיינים)
 - מאפיין ביןארי (1 או 0) המציין האם לדוגמא קיים שכן שהיא אנומליה מתואגת כאחד מtar K השכנים הקרובים.
- **מאפייני נורמליות**: מאפיינים אלו זים למאפייני האנומליה (מינימום, ממוצע ושכנים), רק שבמקומות להסתכל על האנומליות המתואגות, ניקח את הדוגמאות שתויגו כתקינות.

הערות:

- החוקרים מצינים שהשיטה מספיק גמישה כך שהיא אפשר להוסיף/להחסיר מטא-מאפיינים למודל בצורה פשוטה ולבדק כיצד זה משפיע על הביצועים.
- יש צורך בחישוב המרחקים בין כל זוג דוגמאות בדאטasset לפני תחילת האימון כדי שניתן יהיה לחשב את מאפייני האנומליות והנורמליות.

שימוש בזרם מידע:

וקטור המכיל את ששת המאפיינים האלה יציין לנו את המצב s של דוגמא. מפה עולה נקודה חשובה - כאשר מדובר באלגוריתם RL קלאסי (למשל Iteration, Value Iteration, Q-Learning), יש צורך להחזיק טבלה בגודל מרחב המצבים כפול מרחב הפעולות. כל תא בטבלה יציג פעולה ו מצב. האלגוריתם שומר בכל תא עד כמה כדאי לו לבצע את אותה פעולה כאשר הוא נמצא במצב מסוים. נשים לב לכך דברים: קודם כל, כל מצב מיוצג על ידי וקטור בגודל 6 ולא על ידי מספר בודד. שנית, מספר המצבים תלוי בגודל הדאטסהט שכן כל דוגמא מהווה מצב. כתוצאה לכך יש לשמר בכל רגע בזיכרון טבלה שיכולה להיות גדולה מדי לזכרון החומרה. כדי להתמודד עם הבעיה, החוקרים משתמשים בזרם (stream) של מידע, כך שבכל איטרציה האלגוריתם יפגש רק דוגמא אחת מכל המרחב ולא את המרחב כולו. בעת נתאר את הדרך שבה זה נעשה:

יצור דאטסהט שבו כל דוגמא הינה המטא-פיצ'רים והתיאוג של דוגמא מהדאטסהט המקורי, ככלmor נהורן את הבעיה לבעת למדיה מפוקחת על ידי יצירת צמדים הבאים:

$$Dataset = \langle (X_1, y_1), (X_2, y_2), \dots, (X_n, y_n) \rangle$$

כאשר X הינו מצב הכלול את המטא-פיצ'רים ו- y הינו התיאוג של אותו מצב (אנומליה או לא). בכל איטרציה נבחר בצורה רנדומלית את הדוגמא הבאה מהדאטסהט ונזין אותה למודל.

כמו שיטות למידת חיזוקים عمוקה רבות, MetaAAD משתמשת בראשת נוירונים כדי למדל את $(S)A$ על מנת להימנע משמירת הטבלה המלאה המכילה את כל המצבים. ככל שהראשת "תראה" יותר פעולות ותקבל פידבק מהסבביה בדמות תגמולים, יכולת שערוך $(S)A$ תשפר וכך תוכל לתת מידע מדויק יותר עבור הסוכן שתוביל לשיפור המיחול של המדיניות שלו.

MetaAAD מנסה למקסם את פונקציית המטרה הבאה:

$$L_t(\theta) = \hat{\mathbb{E}}_t[L_t^{CLIP}(\theta) - c_1 L_t^{VF}(\theta) + c_2 \cdot entropy(\pi_\theta(\cdot | s_t))].$$

הלו ס מרכיב מהחלקים הבאים:

L_t^{CLIP} - פונקציית הלו ס של שיטת PPO (לפרטים, ראה נספח), כאשר רשות ה-"שחקן" של PPO מקבלת כקלט מאפייני דוגמא, ומוציאה כפלט אומדן להסתברות שליחתה של הדוגמא לתיאוג. בעזרה אוטו אומדן דוגמים את הפעולה.

- L_t^{VF} - מודדת את דיק השערוך של רשות המבקר.
- $entropy$ - מעודד למידת מדיניות פחות דטרמיניסטית, כלומר בעלת אנטרופיה גבוהה יותר. זה מעודד את הסוכן לחזור יותר את מרחב הפעולות (exploration), תוך כדי בחירה של פעולות שכרגע תגמולן הצפוי אולי נמוך. כך לסוכן יש פחות סיכוי להיתקע במקומות ליקאלי של "מרחב התגמולים". מנגנון רגולרייזציה דומים נמצאים בשימוש נרחב באלגוריתמי מדיניות (policy) של RL.
- c_1, c_2 שניהם היפר פרמטרים שנitin לכון

אימון מול מצב אמת:

במהלך פרק של אימון הסוכן יכול לבצע T פעולות, שכל אחת מהן היא שליחה או אי שליחה של דוגמא לתיאוג. בזמן תהליכי האימון יש צורך בדעתהסט מתיוג. הסיבה לכך היא שזמן תהליכי הלמידה של הסוכן, הפידבק שיוחזר לו מהתשכחה, זה שאמור להיות הפידבק מהגורם האנושי, יחולף בתיאוג האמתי של אותה דוגמא שנבחרה להישלח לחקירה.

במצב אמת בו משתמשים בדעתהסט לא מתיאוג, מתבצעים השלבים הבאים:

1. עברו כל דוגמא בדעתהסט מחשבים את המטא-פיצרים ומתחילה את מצבה $c=0$ (הDOGMA לא נבחרה לתיאוג), קלומר הצמד $\hat{y} > X$
2. הסתברות שליחה לתיאוג מחושבת לפי פונקציית המדיניות עברו כל דוגמא בדעתהסט לבדיקה (קלומר פעולה מס' 1).
3. הדוגמא בעלת הסתברות הגבוה ביותר נשלחת לבדיקה. לאחר הפידבק של הבוחן, הסוכן מעדכן את המדיניות שלו ואת המצב \hat{y} להיות תוצאה התיאוג.
4. התהליך חוזר על עצמו עד שהתקציב T נצל במלואו.

شرطוט ויזואלי של התהליכי:

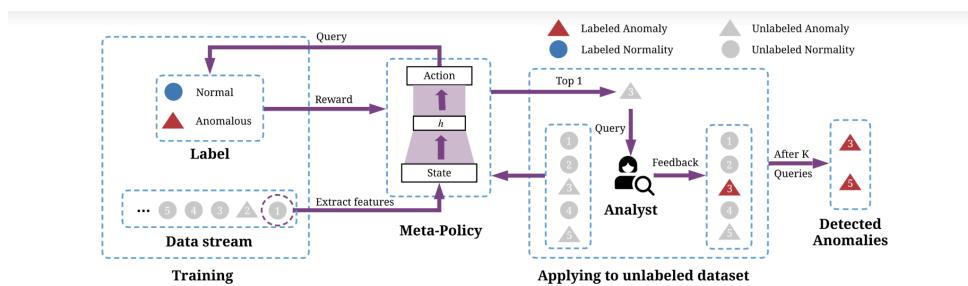


Fig. 2: An overview of Meta-AAD. In training, we shuffle the data and feed them to the meta-policy in a streaming manner. The meta-policy is rewarded based on the labels. The trained meta-policy can then be directly applied to a new unlabeled dataset. In each iteration, the meta-policy chooses one of the instances and queries an analyst (human).

הישגי מאמר:

כדי לבדוק את השיטה שלהם, החוקרים השתמשו ב-24 דatasets בגודלים שונים. תקציר של הדatasets ניתן להלן:

TABLE II: Statistics of the datasets.

Dataset	Points	Dim.	Anomalies	Anomaly%
Annthyroid	7200	6	534	7.4
Arrhythmia	452	274	66	15.0
Breastw	683	9	239	35.0
Cardio	1831	21	176	9.6
Glass	214	9	9	4.2
Ionosphere	351	33	126	36.0
Letter	1600	32	100	6.3
Lympho	148	18	6	4.1
Mammography	11183	6	260	2.3
Mnist	7603	100	700	9.2
Musk	3062	166	97	3.2
Optdigits	5216	64	150	3.0
Pendigits	6870	16	156	2.3
Pima	768	8	268	35
Satellite	6435	36	2036	32.0
Satimage-2	5803	36	71	1.2
Shuttle	49097	9	3511	7.0
Speech	3686	400	61	1.7
Thyroid	3772	6	93	2.5
Vertebral	240	6	30	12.5
Vowels	1456	12	50	3.4
Wbc	278	30	21	5.6
Wine	129	13	10	7.7
Yeast	1364	8	64	4.7

החוקרים השוו מול כמה שיטות שונות:

- **AAD**: אלגוריתם שבאותה תקופה היה נחassoc לטוב ביותר ביגלי אונומליות. האלגוריתם משתמש במספר גלאים (detectors) וידע למשקל כל גלאי בהתאם "ליקולתו לזרחות אונומליות". AAD מערב את הגורם האנושי ומستخدم בפידבק שלו לעדכן המשקלים ש הгалאים בהתאם לפידבק.
- **FIE**: שיטה שמשתמשת בפידבק האנליטי כדי לעדכן את אלגוריתם Isolation Forest - IsF.
- **SSDO**: משלבת גלאים שונים בסביבה מפוקחת חלקית (semi-supervised).
- שיטות לא מפוקחות קלאסיות לגלי אונומליות כגון FIs. שיטות אלו לא משתמשות בפידבק מהගורם האנושי ולא מתעדכנות בזמן ריצה בהתאם לפידבק. שיטות אלו הן בעצם הבסיס המינימלי שצרכי להיות מעליו.

הgalai בו השתמשו חוקרי המאמר בשבייל לחוץ את מאפייני הgalais הינו FIs.

ניתוח תוצאות:

1. 12 הדאטסטים הראשונים בראשימה המוצגת לעיל נבחרו להיות סט האימון והשאר נבחרו להיות סיבת האמת שעלייהם לבדוק השיטה. המטריקה שנבחרה כדי לבצע בדיקה לטיב השיטה הינה **(ADC)** *Anomaly Discovery Curve* שמצירת על גרף את כמות האונומליות שהתגלו מול מספר השאלות שהשתמשו כדי לגלוות אותן. גרף עם שיפוע 1 מראה שככל השאלות הביאו לגלי אונומליות בעודן גראף עם שיפוע 0 מראה שבו כל השאלות הביאו לדוגמאות רגילות ולא אונומליות. נרצה שהשיטה תביא לגרף עם שיפוע קרוב ל-1. התקציב 2 של שאלות בכל פרק בו השתמשו להרצת הניסויים הינו 100:

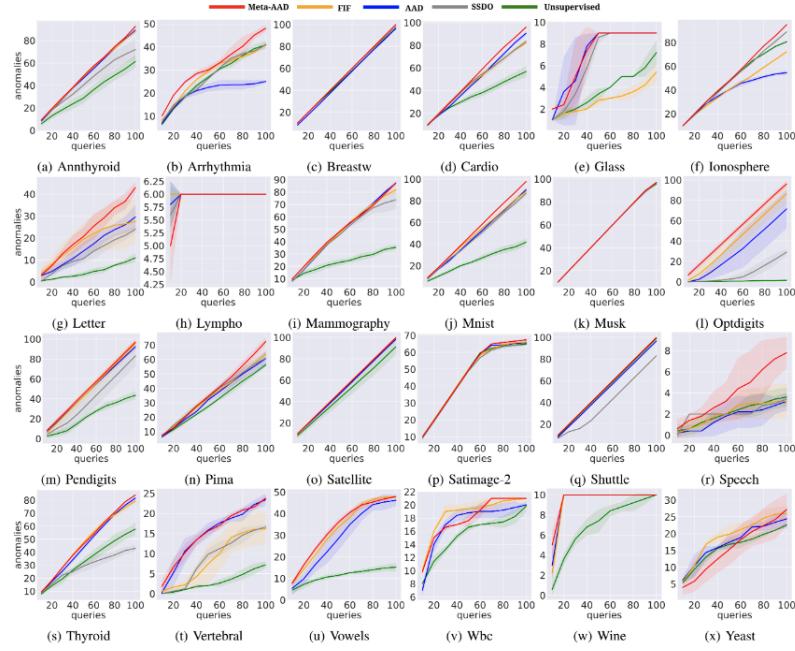


Fig. 3: Performance comparison of Meta-AAD against the state-of-the-art alternatives and unsupervised baseline.

2. עברו כל שיטה נבדק הדרוג הממוצע של האנומליות שנמצאו לאורך מספרسائلות שונה:

Method	20	40	60	80	100
unsupervised [2]	4.188▲	4.146▲	4.167▲	4.333▲	4.375▲
SSDO [18]	3.312▲	3.396▲	3.500▲	3.625▲	3.438▲
AAD [5]	3.229▲	3.208▲	3.271▲	3.167▲	3.104▲
FIF [6]	2.208	2.333	2.312	2.396▲	2.708▲
Meta-AAD	2.062	1.917	1.750	1.479	1.375
Improvement	0.146	0.416	0.562	0.917	1.333

מהתוצאות ניתן להסיק כמה מסקנות:

1. ניתן לראות שכל האלגוריתמים, המשמשים בפידבק מהמשתמש, מראים תוצאות טובות מהאלגוריתם הלא מפוקח הבסיסי לכל הדאטסהטים. מכך ניתן להבין את החשיבות שיש לשימוש בפידבק כדי להמשיר ולأمان את האלגוריתם באופן מכוון ובכך לאפשר לו להשתפר לאורך זמן.
2. SSDO שהוא אלגוריתם חיצי מפוקח מראה תוצאות פחות טובות מאשר האלגוריתמים המשמשים בפידבק בכל הדאטסהטים. הסיבה לכך לפי המאמר הנינה פונקציית המטרה. SSDO מנסה להגיע לאופטימום פונקציית מטרה שונה מאשר האלגוריתמים המשמשים בلمידה אקטיבית. זה יכול לגרום ל-SSDO להגיע לאופטימום מקומי אשר פחות טוב מאלגוריתמי הפידבק.
3. MetaAAD מראה תוצאות שונות לפחות טובות כמו שאר אלגוריתמי הפידבק הטובים ביותר. סיבה אפשרית לכך היא שב-MetaAAD המידול של הטווח הארוך נעשה באמצעות טכניקות RL. בנוסף, טבלת הדירוג מראה שה-MetaAAD מגיע לביצועים טובים יותר ככל שמספר השאלות עולה הינו הוכחה לכך.

הערה: לא ברור מהמאמר כיצד בוצע הדרוג.

במאמר הוצגה שיטת MetaAAD לזיהוי אנומליות, שיטה אשר משתמשת ב-DRL כדי למקסם את מספר האנומליות שניתן למצוא בדאטה. השיטה יודעת להשתמש בגלאי אנומליות אשר כבר קיימים בארגון/מערכת ובהבנה שלהם מהי אנומליה. בנוסף, על ידי שימוש הגורם האנושי בתהיליך, השיטה מנצלת את הפידבק שלו כדי להשתפר לאורך זמן לצורך מקוונת. השיטה הוכחה כתובה לפחות וחומר משיטות הנחשבות לטובות ביותר בתחום גילוי האנומליות.

נספחים:

תהליך קבלת החלטות מركובי:

(MDP - Markov Decision Process) הינה מסגרת מתמטית המשמשת לمدל בעיות קבלת החלטות שבהן התוצאות הן בחלוקת אקראיות ובחלוקת ניתנות לשיליטה. מקבל החלטות, או סוקן, "ח'י" בסביבה, אשר משתנה באופן אקראי בתגובה לפעולות הפעולה (action) שנעשו על ידי הסוקן. ב-MDP, הסתברות המעבר והתגמול תלויים רק במצב הנוכחי וב פעולה שנבחרה על ידי הסוקן, ולא תליה במצב הтурם ופעולות העבר. מצב הסביבה משפיע על התגמול המיידי שמקבל הסוקן, כמו גם על הסתברויות מעברים עתידיים בין המצבים. מטרת הסוקן היא לבחור אסטרטגייה ד'
(סדרת פעולות) כדי למקם את התגמול הכללי שהוא מקבל. האסטרטגייה ד' מגדירה את פעולה הסוקן בהינתן המצב שהוא נמצא בו.

MDP מופיעין על ידי הפרמטרים הבאים:

- S - סט כל המצבים האפשריים שניתן להגעה אליהם או בשם אחר מרחב המצבים.
- A - סט כל הפעולות האפשריות שניתן לבצע.
- $P_a(s, s')$ - ההסתברות לעבור מצב s במצב s' כתוצאה ביצוע פעולה a .
- $R_a(s, s')$ - התגמול המיידי על ביצוע פעולה a ממצב s ומעבר לו- s'

למידה عمוקה באמצעות חיזוקים:

שם כולל לאלגוריתמי למידה عمוקה בהם הרשת היא זו שקובעת את האסטרטגייה של הסוקן. בדרך כלל, משתמשים בסוקן מבודס למידה عمוקה כדי ללמידה מדיניות עבור MDP.

:Proximal Policy Optimization

אלגוריתם RL המורכב משתי רשותות: רשות המבקר (critic) ורשות השחקן (actor):

- השחקן - רשות זו אחראית להחליט איזו פעולה hei כדי לבצע במצב מסוים ולמעשה היא מושערת את המדיניות הסטטוסטית π עבור דוגמא נתונה מהדאה-5ט.
- המבקר - רשות זו אחראית לבצע קירוב של כדיות המצב וברק מידעת את השחקן על טיב הפעולה אותה בחר לבצע. רשות מקבלת קלט מצב וmozhia כפלט מספר שמייצג בקירוב את פונקציית ערך המצב $(S)V$. פונקציית ערך המצב מושערת את התגמול הממוצע שניתן לקבל החל מצב S .

הסברים יותר עמוקים - [כאן](#), [כאן](#), [כאן](#).

נזכיר Sh-MDP מודל על ידי הפרמטרים הבאים: $.S, A, P_a(s, s'), R_a(s, s')$ מגדירה אותם באופן הבא:

- S - המטא-מאפיינים של הדוגמא הנוכחיות בזרם, דוגמא ?
- A - מרחב הפעולות הינו 1 או 0 כאשר 1 אומר לשילוח את הדוגמא לתויג ו-0 מmdl או שליחת של דוגמא לתויג .

- $P_a(s, s')$ - לא הוגדר במאמר. קיימים מודלים אשר מודיע זה לא נתון בהם והם לומדים אותו תוך כדי אינטראקציה עם הסביבה. החוקרים לא הגדירו שזה המצב, אך לעניות דעתנו זה מה שקרה כאן.
- $R_a(s, s')$ - פונקציית תגמול
 - כאשר הסוכן החליט לא לשלו דוגמא לתיאוג, ניתן לו אוטומטית תגמול של 0
 - כאשר הסוכן החליט לשלו הדוגמא תיאוג: אם תיאוג אונומלית הסוכן מקבל תגמול של 1. אם הדוגמא תיאוג כתקינה (כלומר היה עדיף לדלג עליה) התגמול הוא 0.1.

Review 28: Kitsune: An Ensemble of AutoEncoders for Online Network Intrusion Detection

פינת הסוקר:

המלצת קריאה מעדן ומיק: מומלץ לאנשים העוסקים בתחום ה-NIDS או לאנשים שאוהבים Autoencoders ו-Detection

בahirot כתיבה: בימנית

ידע מוקדם: Autoencoders, Online Algorithms

ישומים פרקטיים אפשריים: Network Intrusion Detection System

פרטי מאמר:

lienek למאמר: [זמן להורדה](#).

lienek לקוד: [קוב](#)

פורסם בתאריך: 25.02.18, בארכיון.

הציג בכנס: Network and Distributed Systems Security Symposium (NDSS) 2018

תחומי מאמר:

- דיהוי אונומליות
- שימוש ואיימון של אלגוריתמים בזמן אמת (Online)
- למידת אנסמבל

מבוא:

התקפות הסיביר רק הולכות ונעשהות מתחכחות יותר בשנים האחרונות. אחד מכל' ההגנה הנפוצים הינו - NIDS Network Intrusion Detection System. כל' זה הוא שם למערכת תוכנה או חומרה אשר שורקת את הרשת בחיפוש אחר תעבורת רשות זדונית שיכולה להיעיד על התקפה. כאשר תעבורת מסווג זה מזוהה, המערכת מעלה התרעעה לאחראי המערכת כדי לידע אותו על המתרחש. כדי שתוקפים לא יעקפו את המערכת היא לרוב מחולקת באופן מבוזר ברשות הארגון במיקומים שונים (למשל בתוך הרשת, בחיבור של הרשת עם האינטרנט וכדומה).

כבר שנים רבות נעשה שימוש באlgorigthmi למידת מכונה עבור NIDS. רשות ניורונים הפגינו ביצועים חזקים ביותר NIDS בשל יכולת למדוד דפוסים מורכבים. הגישה הנאיבית אומרת שאם ניתן לרשות למדוד רגיל של הרשות הארגונית ומידע שנוצר מהתקפת סיביר, הרשות תלמוד להפריד בין שני סוגי תעבורת הנ"ל. בנוסף כדי לאפשר את הגישה המבוזרת בצורה קלה וдолה, הדבר הגיוני לעשות הוא לשלב את המודל בתוך החומרה עצמה בתבאים היישבים ברשות. אולם לגישה זו יש כמה חולשות:

1. **צורך לשמור מידע רב על הנתבים:** באימון מודל לא מקוון(רגיל) יש צורך לפחות כמות מידע מסויימת לאורך הזמן ולאחר שנאספה כמות מספקת, המודל מאומן על הדadata שנאסף. שיטה זו צורכת משאבי רבים יותר (כגון זיכרון וזמן CPU), מאשר המקבילה שלה - אימון מקוון. צריכת המשאבי הגדולה עלולה לפגוע בביטחוני הנתבים וכתוצאה לכך לפגוע ברשות הארגונית אם מאמנים את המודל בצורה לא מוכנות.
2. **דפוסי התקפות משתנים מקשא על ביצוע למידה מפוקחת "סטטיטית"** - אימון מודל עם הגישות המפוקחות מצריך מידע מתיוג. השגת מידע מתיוג איכוטי במקורה זה היא משימה לא טרייניאלית, שכן כיוון שהתקפות כל הזמן משתנות; המודל שמאומן על מידע היסטורי עלול להתקשות לזראות דפוסי תקיפות חדשים. בנוסף ההתקפה יכולה להיות כבר לא רלוונטיות זמן קצר לאחר השגת המידע המתויג שכן התקופים משכליים את ההתקפות שלהם כל הזמן.
3. **סיבוכיות חישוב** - סיבוכיות החישוב גבוהה של רשות ניורונים עלולה להכבד על נתב לבצע את ההסקה (inference) בזמן אמיתי.

הערה: באימון מקוון המודל מתעדכן בצורה שוטפת כלומר כל דגימה (או סט של דגימות) משמשת לעדכון של פרמטרי הרשת.

בעבר הוצעו כמה שיטות לזיהוי anomalיות בתעborת הרשת. שיטה מקוונת בשם IDS PAYL המבוססת על חישוב היסטוגרמות של מאפיינים שונים של חבילת (packet) המידע. גישה זו הינה חסכנית מבחינות המשאבי הנדרשים ויכולת לזרוך על נתבים חלשים, אך יחד עם זאת סובלת מביצועים חלשים. גישה נוספת נספפת משתמש במספר רשותות ניורונים שונות, שככל אחת מהן מאומנת לזראות התקפה ספציפית. גישה אלו מניחה למידה מפוקחת(supervised) ובנוסף דורשת שמירה של סט האימון על המכשיר המקומי, הנחה שהיא לא תמיד מתקינה כשהזה מגיע לצד רשות כמו נתבים.

כדי להתגבר על קשיים אלו, המאמר מציג את שיטת *Kitsune*, שהיא שיטת זיהוי אונומליות המשלבת אנסמבל של Autoencoders (AE) השיטה מסוגלת ללמידה בזמן אמיתי, בדומה לא מפוקחת וצורכת מעט מושבים תוך כדי הציג תוצאות גבוחות לא פחות מושיות לא מקוונות קודמות (Offline).

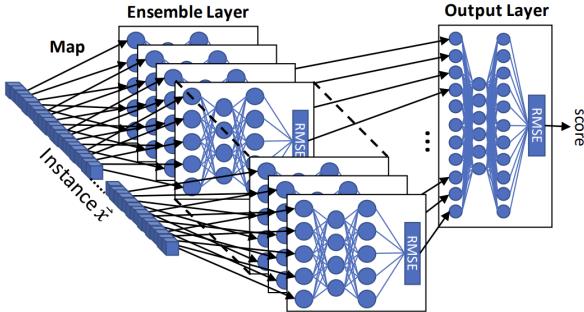


Fig. 1: An illustration of **Kitsune**'s anomaly detection algorithm *KitNET*.

הreview הכללי מאחורי המאמר:

לפי השיטה כל מאפיין (feature) ממופע לאחד ה-AE בשכבה האנסמבל. כל AE מבצע את משימת שחזור הקלט ומהשבר את שגיאת השחזור, כולם את-h-RMSE. אותו RMSE הוא הפלט של כל אנסמבל. ה-h-RMSE של כל רשת מועבר קלט למודל נוסף של AE שמקבל את-h-RMSE-ים של כל האנסמבלים כקלט ומנסה ללמידה את ההתנהגותם הרגילה בזמן האימון. בכך AE לומד את הקשר בין האנסמבלים השונים. הפלט של ה-h-AE האחרון הינו ציון בוודד שמצוין עד כמה הדגימה נחשבת כאנומלית.

הכותבים מגדירים שבמהלך האימון רק דגימה אחת נשמרת בזיכרון לכלי אוור תהיליך האימון. זאת על ידי שימוש ב-B-SGD, כאשר backpropagation מופעל על דגימה בזווית במקום על אוסף של דוגימות (batch). לאחר עדכון של משקליו הרשת הדגימה נזרקת ובכך שומרים על האלגוריתם כמיוקן. כדי להתמודד עם סיבוכיות החישוב הגדולה של AE, כותבי המאמר הגבילו את גודל הרשת המקסימלית ל-3 שכבות עם מקסימום 7 נוירונים בשכבה הקלט והפלט. בכך ניסו הכותבים לאפשר לרשת לזרוץ ללא מאץ על נתונים.

cut נרחב על המבנה של השיטה המוצעת:

(1) מחלץ המאפיינים (FE):

כותבי המאמר הגיעו כי הגישה הנאייבית הינה שימוש בחולון עליון מחושבים המאפיינים הסטטיסטיים כגון מקסימום, ממוצע וכדומה. למשל בחולון של 5 שניות מחשבים את ממוצע ה-PAYLOAD של כל חיבור. הבעייה עם גישה נאייבית זו היא שקצב הגעת המידע יכול להיות גבוה שהחולון יכול מספר גדול מאוד של דוגימות ויעמיס על הנתב מאחר וכמויות גדולות של>Data צריכה להיות מאוחסנת עליון (הנתב). לכן הם הציעו להשתמש בסטטיסטיקה מצטברת דועכת (Damped Incremental Statistics) שבה בכל עת נשמר בזיכרון סט של המאפיינים הבאים: $IS = (N, LS, SS)$ כאשר שלושת הממדים הינם: כמות הדגימות, הסכום של ערכי הדגימות וסכום הריבועים של ערכיה. בכך לדגימה חדשה יהיה ניתן לבצע את העדכון הבא: $(N + 1, LS + x_i^2, SS + x_i^2) \leftarrow IS$ ולאחר מכן לחשב את כל המאפיינים החדשניים:

$$\mu_S = \frac{LS}{N}, \sigma_S^2 = \left| \frac{SS}{N} - \left(\frac{LS}{N} \right)^2 \right|, \sigma_S = \sqrt{\sigma_S^2}$$

בתחילת זה יש גם חשיבות בזמן שכן התנהלות הרשות הארגונית משתנה לאורך זמן כך המודלים צריכים לשנות את התנהלותם בהתאם לשינויים של הקלט. כדי לבצע זאת משתמשים כתובבי המאמר בפונקציית דעיכה:

$$d_\lambda(t) = 2^{-\lambda t}$$

האחרונה. כאמור השפעה של דגימה על הפרמטרים של המודל תדוער עם הזמן. ט המאפיינים החדש מוגדר באופן הבא: $IS_{i,\lambda} := (w, LS, SS, SR_{ij}, T_{last})$ כאשר w הינו משקל הנוכחי, LS הזמן של העדכן האחרון, SS הינו סכום השגיאות (Residual sum of squares) בין שני ערכיו תקשורת x_i . במהלך האימון וההערכתה של המערכת מתעדכן סט המאפיינים הנ"ל באמצעות מקדם הדעיכה:

Algorithm 3: The algorithm for inserting a new value into a damped incremental statistic.

```

procedure: update( $IS_{i,\lambda}, x_{cur}, t_{cur}, r_j$ )
1  $\gamma \leftarrow d_\lambda(t_{cur} - t_{last})$             $\triangleright$  Compute decay factor
2  $IS_{i,\lambda} \leftarrow (\gamma w, \gamma LS, \gamma SS, \gamma SR, T_{cur})$   $\triangleright$  Process decay
3  $IS_{i,\lambda} \leftarrow (w+1, LS+x_{cur}, SS+x_i^2, SR_{ij}+r_i r_j, T_{cur})$ 
    $\triangleright$  Insert value
4 return  $IS_{i,\lambda}$ 
```

על ידי שימוש בממוצע וסטיית התקן חושבו מאפיינים נוספים בין ערכי תקשורת שונים כגן השונות בין הערכים, גודל הערכים ובדומה. כלל מאפיינים אלו (יחד עם הממוצע וסטיית התקן של כל ערך) הם המאפיינים שנכנסו למודלים השונים בתור הקלט:

TABLE II: The statistics (features) extracted from each time window λ when a packet arrives.

The packet's...	Statistics	Aggregated by	# Features	Description of the Statistics
...size	μ_i, σ_i	SrcMAC-IP, SrcIP, Channel, Socket	8	Bandwidth of the outbound traffic
...size	$\ S_i, S_j\ , R_{S_i, S_j}, Cov_{S_i, S_j}, P_{S_i, S_j}$	Channel, Socket	8	Bandwidth of the outbound and inbound traffic together
...count	w_i	SrcMAC-IP, SrcIP, Channel, Socket	4	Packet rate of the outbound traffic
...jitter	w_i, μ_i, σ_i	Channel	3	Inter-packet delays of the outbound traffic

תפקיד רכיב זה הינו למפות תת-קבוצת מאפיינים מהקלט לאחד ממודלי AD. כדי לדעת כיצד לחלק את מרחב המאפיינים של הקלט בצורה טוביה, נעשה שימוש באלגוריתם אשכולות היררכי (clustering). הקלייסוטור מבוסס על הקורלציה בין מאפיינים (המפרק בין מאפיינים הינו ביחס הפוך לקורלציה ביניהם). המטריה היא לבנות k אשכולות כך שבכל אשכול לא יהיו יותר מ- m מאפיינים כאשר m הוא מספר הנוירונים בשכבה הקלט של כל AD. כיוון שמרחב המאפיינים הינו קטן ניתן לבצע את החישוב זהה בזמן ריצה.

(3) מזהה אונומליות (Anomaly Detector):

רכיב זה נקרא KitNET והוא מורכב משתי שכבות צפוי שניות לראות בציור 3: שכבת האנסמבל ושכבת הפלט, כל אחת מורכבת מאותו-אנקודרים.

שכבות האנסמבל: השכבה היראשונה ב-KitNET נקראת שכבת האנסמבל. שכבת האנסמבל מורכבת ממספר אוטו-אנקודרים כאשר כל אחד מהם מחשב את ה-RMSE עבור הקלט אותו קיבל ממפה המאפיינים. הפלט של כל אנסמבל עובר קלט לשכבה הבאה.

שכבות הפלט: שכבה זו כוללת אוטו-אנקודר ייחיד שמקבל את כל ה-RMSE מכל האנסמבלים. שכבה זו פולטה לבסוף RMSE בודד שהוא ציון האנומליה של אותה דגימה.

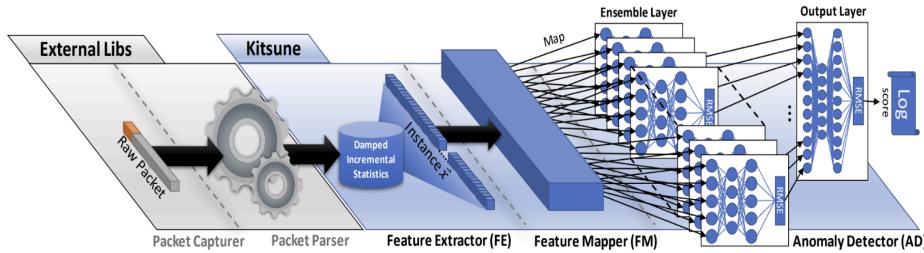


Fig. 3: An illustration of Kitsune's Architecture.

הערה: הספריות החיצונית בציור הין ספירות שכותבי המאמר השתמשו בהן ללא שינוי וכך לא הזכרו.

הסבר של רעיונות בסיסיים:

הינו מודל שמטרתו היא לדחוס את הקלט כך שייהי ניתן לשחזרו מוצրתו הדחוסה (הנקראת לפעמים ייצוג לטני או הקוד של הקלט) בדיקוק מקסימלי. במלים אחרות אוטו-אנקודר מנסה להחלץ את המאפיינים המהותיים שלו תוך כדי ניפוי מאפיינים פחות חשובים (redundant). אוטו-אנקודר מורכב שתי רשתות המופעלות אחת אחרי השניה. הרשת הראשונה, הנקראת אנקודר או מקודד, דוחסת את הקלט (מקטינה את מימדו) ומפיקה ממנו את הייצוג הלטני. החלק השני נקרא *decoder* או מפענה שטמרת לשחזר את הקלט מהייצוג הלטני המופק על ידי האנקודר. אוטו-אנקודר מאמן למצוור את שגיאת שחזר הקלט.

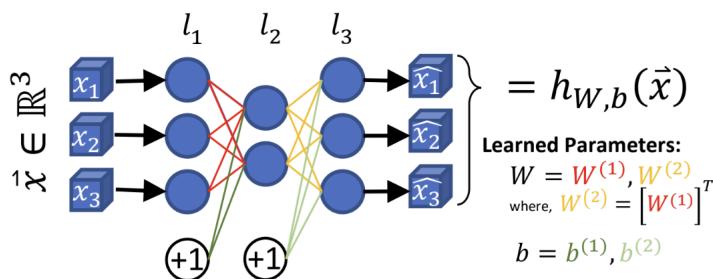


Fig. 2: An example autoencoder with one compression layer, which reconstructs instances with three features.

במקרה שלנו אוטו-אנקודר מנסה לאמן רשת h_θ לשחזר את מאפייני הקלט. הכותבים השתמשו בפונקציית Root Mean Square Error (או RMSE) בתור פונקציית לוס (מრחק בין הוקטור המשוחזר לקלט).

הישגי מאמר:

$$\text{RMSE} (\vec{x}, \vec{y}) = \sqrt{\frac{\sum_{i=1}^n (x_i - y_i)^2}{n}}$$

לצורך בוחנת ביצועי Kitsune כותבי המאמר ניסו לבדוק האם המערכת תזהה התקפות המבוצעות על [טאלמות IP](#) ולשם כך הקימו רשת המכילה כמה מצלמות מסווג זה המחווראות לאתר מרוחק דרך VPN. דרך אותו VPN המשתמש יוכל לגשת למצלמות. מערכת Kitsune נפרשה בנקודת הגישה למצלמות. דרך נקודה עולן התקוף לגשת למצלמות. בנוסף כדי לבחון את Kitsune על רשת רוועת יותר המדמה יותר את העולם האמיתי, הוקמה רשת המכילה מכשירי IoT שונים יחד עם שלושה מחשבים רגילים. ברשת זאת אחת המצלמות הודבקה מראש בנוזקה כדי לבדוק את ביצועי המערכת מולה.

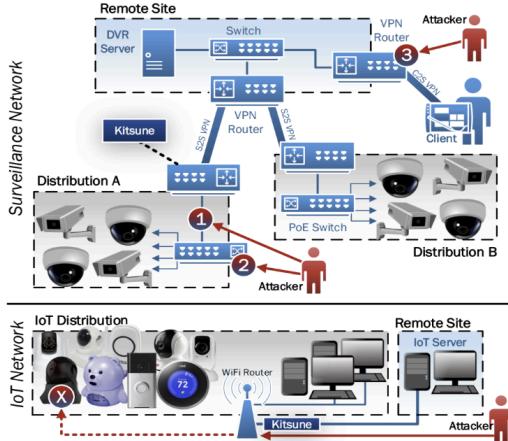
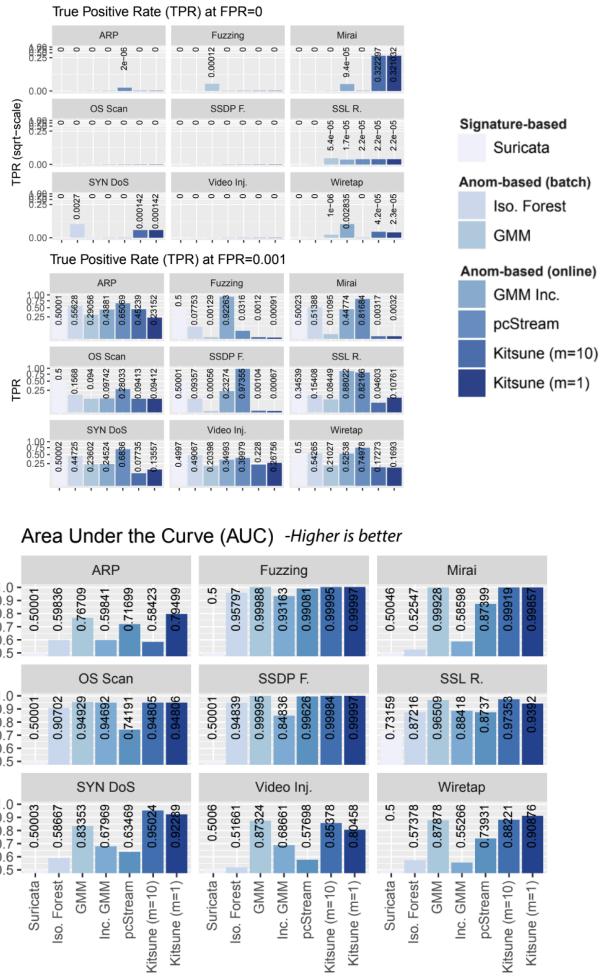


Fig. 7: The network topologies used in the experiments: the surveillance network (top) and the IoT network (bottom).

השוואה:

ביצועי המערכת הושוו מול ביצועים של מודלים מסווג לא מקוון כגון: Isolation Forest, Gaussian Mixture Models (כלומר ככלו שיש להם גישה לכל סט האימון) ומול מודלים מקוונים (עם גישה לדגימה אחת בכל פעם): Suricata NIDS Open source [Incremental GMM](#), [pcStream2](#). בנוסף נעשה שימוש במערכת [Kitsune](#) בשם Suricata Amity. מערכת שנעשה בה שימוש בתעשייה, זאת כדי לבדוק את ביצועי המערכת במאמר מול מערכת אמיתית.

כותבי המאמר השתמשו בגדים שונים של שכבות הקלט של כל AE על ידי שינוי פרמטר α של המערכת מ-1 עד 10. כמה מהמדדים החשובים בהם השתמשו הינם True Positive Rate (TPR), False Positive Rate (FPR), AUC :Rate(FPR), AUC



ניתן לראות של מרבית המודלים לא מצליחו גישה לכל סט האימון, ביצועי Kitsune לא נפלה מהם ואף חלק מהתפקידים גבירה עליהם. בנוסף ניתן לראות בבירור שה-GMM מנצח את כל המתחרים המוקונים כמעט בכל התקפה, כפי שניתן לראות מהתוצאות ה-AUC בהם Kitsune (ימין קיזון) תמיד מעיל pcStream ו-GMM (מספר שלוש וארבעה מימין).

מדד נוסף אותו הראו כתבי המאמר הוא קצב עיבוד החבילות של הנטב שלא נפגע מהרצת המודול. המערכת (כולל הנטב) ריצה על PI Raspberry Sheia חומרה יחסית חלשה, ולמרות זאת ביצועי הנטב לא נפגעו.

מהגרף ניתן לראות שקצב עיבוד החבילות עולה כאשר משתמשים ביוטר אוטו-אנקודרים בשכבה האנSEMBL. הסיבה לכך היא ירידה במספר המאפיינים שימושו לכל אוטו-אנקודר. כפי שתואר לעיל, מalfa המאפיינים מנסה לקבץ מאפיינים לאשכולות לפי מספר האוטו-אנקודרים (אליז' שעליו לעמוד בו), וככל שמספר זה גדול יותר, פחות מאפיינים ימושו לכל אחד (כדי לעמוד באיליז') וכתוכזהה מכך גודלו של כל אוטו-אנקודר יקטן. הקטנה של כל אוטו-אנקודר תביא לירידה בכוח העיבוד שכל אחד צורך. לדוגמה, עם $m=35$ קצב עיבוד החבילות בשלב האימון עומד על 5400 חבילות בשניה ובזמן הריצה עומד על 37300 החבילות בשניה. ביצועים טובים כשלוקחים בחשבון את החומרה עליה המערכת ריצה.

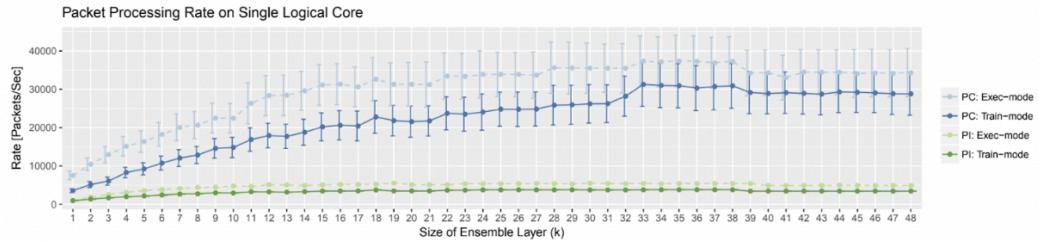


Fig. 10: The affect *KitNET*'s ensemble size (k) has on the average packet processing rate, while running on a single core of a Raspberry PI and an Ubuntu VM (PC), using $n = 198$ features.

סיכום:

המאמר מציג את מערכת Kitsune מערכת ראשונה מסוגה ל Z^{high} אונטולוגיות. המערכת הייתה הראשונה לשלב Autoencoders בקרה מקוונת כדי להזמין התקפות סייבר ברשות הארגונית. המערכת הינה play-and-play-back בכך שהיא אינה צריכה תיוגים כדי ללמידה ומסוגלת לróżע על נתבים בעלי חומרה חלשה בלי לפגוע בביטויים שלהם דבר שיכל להוביל לפגיעה ברשות כולה.

שיטת פעולה: הסקירה נכתבת יחד עם עדן יבין.

Review 29: Language Modeling via Stochastic Processes

פינית הסוקרי:

המלצת קרייה מכותבי הסקירה: שווה קרייה למי שעוסק בגנרטוט טקסטים באמצעות מודלי שפה

בahirot ctiyha: בימנית

ידע מוקדם:

- הבנת העקרונות הבסיסיים של מודלי שפה (במיוחד בשימוש גנרטוט טקסטים)
- רקו בתהליכי סטוכסטיים (כמו גשר בראוני – brownian bridge)

"ישומים פרקטיים אפשריים":

- גנרטוט טקסטים ארוכים בהינתן הקשר

פרטי מאמר:

לינק למאמר: [כאן](#).

תחומי מאמר:

- מודלי שפה לגנרטוט טקסטים
- תהליכיים אקראיים

כליים מתמטיים, מושגים וסימוניים:

- גשר בראוני (brownian bridge)

מבוא:

מודלי שפה מודרניים מפגינים ביצועים מצוינים בתחום גנרטוט טקסטים קצרים (גמ תלויי הקשר). לעומת זאת מודלים אלו מתקשים בגנרטוט טקסטים ארוכים שבמקרים רבים מתקשים לשומר על קוורנטיות וגם עלולים "לסתות" מהונושא (ההקשר). אחת הסיבות לכך היא הינה האופן האוטורוגרסיבי שבו מודלי שפה מגנרטיטים טקסט. עם זאת זו כל טוון (מילה או רצף מילים סמכות) נוצר בהינתן הטוקנים שכבר נוצרו על ידי המודל. מכיוון שה- "זיכרון" האפקטיבי של המודל מוגבל ומוסוגל "לזכור" רק כמות מוגבלת של מידע, המודל מתקשה להתחשב במקרים הנמצאים רחוק מהמשפט שכרגע מג'ונרט. תופעה זו עשויה להיות הסיבה העיקרית לא-קוורנטיות של טקסטים ארוכים הנוצרים באמצעות מודלי שפה.

תמצית מאמר:

אחד הדרכים להתמודד עם הבעיה זו היא ללמידה את התפלגות של הייצוג הלטנטי של מקטעי טקסט ארוכים (כגון משפט). לאחר מכן, ניתן לנצל התפלגות זאת כדי להתנו את הפלט במידע נוסף, ולהנחות את יצרת הטוקנים במהלך גנרטוט הפלט. כאמור, קודם כל אנו מגדירים את השיכון של כל משפט בטקסט ולאחר כך מתנים את יצרת הטוקנים ביצוגים אלו.

ניתן להסתכל על התהליך זהה כתכנון מסלול של טילול ארוך: קודם מחליטים על אבני דרך חשובות ואז בונים את המסלול ביניהם. גישה זו מחזקת את קוורנטיות של הטקסט המגנרט מאחר ותכנון זהה מאפשר לשומר על הקשרים הסמנטיים בין חלקים רחוקים בטקסט וכך הסבירות של גנרטוט טקסט לא קוורנטי יורדת.

הסבר על הרעיון העיקרי:

אבל איך נוכל לבנות "מסלול" כזה לטקסטים ארוכים? עבדות קודמות הציעו גישות המבוססות על הלמידה הניגודית ([contrastive learning](#)) אך לטענת המאמר גישה זו מחייבת רק אחרי קשרים בין משפטים סמוכים ומתקשה להתמודד עם מידול יחסים בין משפטים רחוקים בטקסט. במטרה לתת מענה לסוגיה זו, המחברים מציעים גישה "גLOBלייט" המנסה למדל את ההתפלגות של כל המשפטים בטקסט יחד **במרחב הלטנטי**. התפלגות המשפטים מודלים באמצעות גשר בראוני ([brownian bridge](#)). גשר בראוני זה הוא מקרה פרטי של תנואה בראונית ([standard Wiener process](#) או [brownian motion](#)) מוגדר בקטע $[T, 0]$ כאשר ערכי התהילר ב- $t=0$ וב- $T=t$ הם דטרמיניסטיים (המסומנים z_0 ו- z_T בהתאם).

הдинמיקה של גשר בראוני כזו מוגדרת באופן הבא:

$$p(z_t | z_0, z_T) = \mathcal{N}\left(\left(1 - \frac{t}{T}\right)z_0 + \frac{t}{T}z_T, \frac{t(T-t)}{T}\right)$$

כאשר N היא ההתפלגות הגaussית. המשווה הזה היא די אינטואיטיבית – היא למעשה מבצעת סוג של אינטראולציה לינארית רועשת בין z_0 ו- z_T . למשל ככל ש- t יתקרב ל- T , התוחלת של z תתקרב ל- z_T והשונות תקטן. נעיר כי השונות המקסימלית מתאפשרת בנקודה $z=T/2$ שבה באופן טבעי יש מקסימום אי-ודאות. השיטה המוצעת נקראת **TC** – Time Control.

המטרה כאן למצוא פונקציה

המפה משפט למרחב הלטנטי כך שההתפלגות למרחב הלטנטי תקיים את הדינמיקה של הגשר הבראוני. כמובן, f_θ מודדת באמצעות רשת ניורונים. כדי לאמן את הרשות הזה משתמשים בלמידה הניגודית באופן הבא:

1. דוגמים מיני-באצ'ים המורכבים משלשות של משפטיים (x_0, x_t, x_T) כאשר המשפט x_t חייב להיות בין x_0 ו- x_T בטקסט. משפטיים אלו יהיו הדוגמאות החיוויות.
2. דוגמים שלשות של משפטיים באקראי כדי ליצור דוגמאות שליליות.
3. מביצים אופטימיזציה עם פונקציית המבחן הניגודית הבאה:

$$\begin{aligned} \mathcal{L}_N &= \mathbb{E}_X \left[-\log \frac{\exp(d(x_0, x_t, x_T; f_\theta))}{\sum_{(x_0, x_{t'}, x_T) \in \mathcal{B}} \exp(d(x_0, x_{t'}, x_T; f_\theta))} \right] \\ d(x_0, x_t, x_T; f_\theta) &= -\frac{1}{2\sigma^2} \left\| \underbrace{f_\theta(x_t)}_{z_t} - \underbrace{\left(1 - \frac{t}{T}\right) f_\theta(x_0) - \frac{t}{T} f_\theta(x_T)}_{\text{mean in Equation 1}} \right\|_2^2 \end{aligned}$$

האיבר השני במשווה התחולתו הוא התוחלת מהביטוי עבור הגשר הבראוני.

המטרה בפורמלציה הזאת היא לכפות על ייצוגים של משפטיים מסוימים הטקסט לקיים את הדינמיקה של הגשר הבראוני. לומר ייצוגים אלו צריכים להיות מסלול חלק בין התחילה לסיוף של הטקסט למרחב הלטנטי. אלו למעשה אבני הדרך שלנו שעליים נבסס את גנרטו הטוקנים הסופי.

אימון מודל לגנרט טקסט עם TC

אחרי שהבנו איך בונים את מסלול המשפטים באמצעות TC, נתאר כיצד איר מגנרטים בהתבסס על מסלול זה. לטקסט בעל T משפטיים (x_0, \dots, x_T) ו-W טוקנים, קודם כל בונים את המסלול (z_0, \dots, z_T) באמצעות אנקודר מאומן $f_\theta(x)$. המחברים בחרו לנצל את המסלול שנבנה כדי לכיל את GPT-2 (כלומר את הדקודר של GPT) שהוא מודל אוטורגרטיבי שאומן על כמות DATA עצומה. כדי לגנרט טוקן t השיר למשפט (t, s) , משתמשים ביצוג הלטנטי של המשפט z_s ובטוקנים שוגנרטו לפני כן x_t . תהליך גנרט הטקסט מתואר בציור למטה.

הערה לגבי כיוול של GPT-2: כדי לכיל שפה גדול כמו GPT-2 למשימה נתונה עם DATAhost D לוקחים GPT-2 מאומן ומאמנים אותו על D כאשר רק חלק מהמשקלים של GPT מעודכנים והשאר מוקפאים.

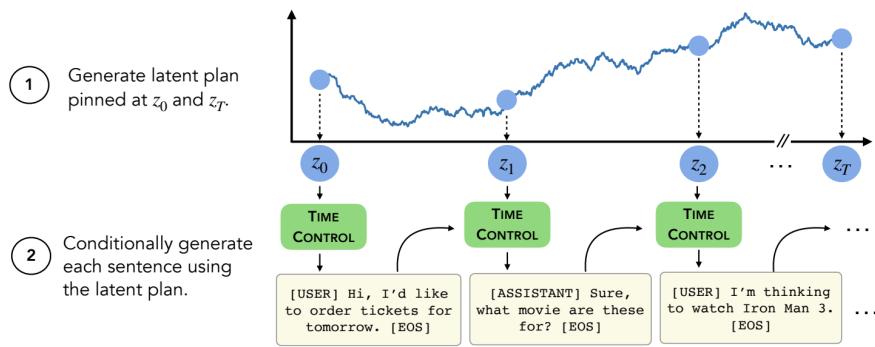


Figure 2: Time Control generates text conditioned on a latent plan. A latent plan is first generated by running Brownian bridge dynamics pinned between a sampled start z_0 and goal latent variable z_T forward. A decoder then conditionally generates from this latent plan on a sentence-level.

גנרט טקסט עם TC

גנרט טקסט עם TC הוא מתרחש באופן טבעי. אם נתונים לנו משפט התחלה x_0 והמשפט האחרון x_T אז:

1. מחשבים את השיכונים של (x_0, \dots, x_T) של המשפט הראשון והאחרון.
2. דוגמים את מסלול המשפטים (z_0, \dots, z_T) לפי התפלגות של הגשר הבריאני.
3. מייצרים טקסט בהינתן מסלול זה באמצעות הדקודר המכיל של GPT-2.

אם המשפט הראשון והאחרון לא ידועים, דוגמים את ייצוגיהם הלטנטיים מההתפלגות שלהם המשוערכות על סט האימון. במלחינים אחרות, הפרמטרים של שיכון המשפט הראשון משוערכים על בסיס השיכונים של כל המשפטים הראשונים של הטקסטים מהדאטהסט.

הישgi המאמר וניתוח תוצאות:

aicoot הטקסט שוגנרט נבחנה על ידי בחינת הדינמיקה והריהוט של הטקסט המגונרט, עבר מקטעי טקסט לokaלים וגלובליים.

דינמיות טקסט מקומי

דינמיקת טקסט מקומי נבדקה על ידי בחינת היכולת של מסוויג לבנות מסגרת קו-הרטניט לשיח, כאשר קו-הרטניטות של שיח יכולת של ידי יכולת של זוג משפטים מופיעים בסדר תקני או לא.

בוחינת היכולת של המודול להזות האם זוג משפטיים מופיעים בסדר תקין נועשתה על ידי ליקוח של שני משפטיים x ו- y כאשר $\{x, y\} \in K$ וחישוב השיכונים שלהם z_T ו- z_{T+K} . אילו הוכנסו בסדר אקריאי למסווג לינאריארי.

תוצאות הדיוק (accuracy) של המטוגן הליניארי הושוו לנתוצאות סיווג ליניארי מחמישה מודלים שונים (GPT2, BERT, ALBERT, S-BERT, Sim-CSE) בשלושה נתונים שונים (Wikisection, TM-2, TicketTalk). בכלל הניסויים מודל TC הראה יכולת טובה לזהות את הסדר התקין של המשפטים, כאשר כמעט בכל המקרים דיוק המודל היה גבוה מהמודלים האחרים הוא הושווה.

	Wikisection		TM-2		TicketTalk	
Method	$k = 5$	$k = 10$	$k = 5$	$k = 10$	$k = 5$	$k = 10$
GPT2	50.3 ± 5.8	50.2 ± 6.3	55.7 ± 5.3	63.6 ± 7.3	54.7 ± 6.1	65.0 ± 8.1
BERT	50.9 ± 4.9	47.8 ± 9.0	68.8 ± 3.5	80.7 ± 3.8	68.4 ± 5.1	80.4 ± 6.3
ALBERT	49.9 ± 12.1	49.6 ± 18.0	$\textbf{81.6} \pm \textbf{4.0}$	$\textbf{86.1} \pm \textbf{7.3}$	$\textbf{78.4} \pm \textbf{6.7}$	$\textbf{89.4} \pm \textbf{3.1}$
S-BERT	50.8 ± 6.0	48.0 ± 9.1	73.4 ± 3.5	$\textbf{83.3} \pm \textbf{4.3}$	72.1 ± 5.3	84.2 ± 5.2
Sim-CSE	49.1 ± 6.4	48.1 ± 8.5	75.4 ± 3.8	$\textbf{86.2} \pm \textbf{3.9}$	$\textbf{75.1} \pm \textbf{5.9}$	85.2 ± 3.1
VAE (8)	49.5 ± 5.5	50.5 ± 5.1	50.5 ± 4.4	51.5 ± 6.0	49.9 ± 1.0	51.2 ± 1.0
VAE (16)	50.1 ± 5.8	51.3 ± 4.7	48.8 ± 4.8	50.8 ± 4.9	50.1 ± 1.0	49.5 ± 1.0
VAE (32)	50.5 ± 5.1	50.0 ± 6.0	48.0 ± 5.1	47.3 ± 5.9	50.0 ± 1.0	49.3 ± 1.0
ID (8)	49.8 ± 5.9	50.1 ± 5.0	60.3 ± 5.2	65.2 ± 6.8	59.2 ± 1.9	66.5 ± 1.1
ID (16)	$\textbf{53.3} \pm \textbf{5.4}$	55.8 ± 6.2	60.5 ± 5.0	67.7 ± 6.8	60.3 ± 1.0	68.4 ± 6.4
ID (32)	50.0 ± 5.0	50.1 ± 5.0	60.4 ± 5.3	67.6 ± 7.1	61.0 ± 1.0	67.9 ± 6.5
BM (8)	49.8 ± 5.4	50.0 ± 5.4	49.8 ± 5.4	49.9 ± 5.2	49.7 ± 5.0	50.6 ± 5.8
BM (16)	50.3 ± 5.5	50.5 ± 5.2	49.9 ± 4.3	51.1 ± 6.0	50.3 ± 4.6	50.8 ± 5.5
BM (32)	49.3 ± 5.6	48.8 ± 5.8	49.5 ± 4.7	49.6 ± 5.2	49.5 ± 5.6	49.1 ± 6.1
TC (8)	49.23 ± 5.72	48.3 ± 6.8	$\textbf{77.6} \pm \textbf{7.8}$	$\textbf{87.7} \pm \textbf{6.9}$	71.6 ± 2.9	82.9 ± 4.1
TC (16)	$\textbf{57.25} \pm \textbf{5.30}$	$\textbf{65.8} \pm \textbf{5.4}$	$\textbf{78.2} \pm \textbf{8.1}$	$\textbf{88.0} \pm \textbf{7.1}$	71.3 ± 3.3	82.9 ± 4.1
TC (32)	50.1 ± 4.8	49.8 ± 5.8	$\textbf{77.9} \pm \textbf{7.9}$	$\textbf{87.9} \pm \textbf{7.4}$	$\textbf{72.0} \pm \textbf{3.9}$	84.4 ± 3.9

Table 1: Discourse coherence accuracy measured by the test accuracy of the trained linear classifier, reporting $\mu \pm$ standard error over 3 runs. Random accuracy is 50%. Values are bolded if they are within range of the highest mean score and its corresponding standard error. The highest mean score are marked in gray cells. When applicable, the methods are run with varying latent dimensions marked in parentheses (dim).

רְהִיטוֹת שֶׁל טַקְסָט מִקּוֹמִי

קוווהרטניות של טקסט מוקמי נבחנה על ידי בחינה של ביצועי המודול במשימת השלמת טקסט חסר (infilling).

הדאטהסט שנבחר לשיממה זאת, ROCStories, מורכב מסיפורי קצרים בני חמישה משפטים. מודל TC יצר את הגשר הבראוני על ידי חישוב השיכונים של המשפט הראשון והאחרון של כל סיפור, ובהתאם למסלול המשפטים שחושב המודל, ייצר טקסט. קוהרנטיות הטקסט שנוצר נבדקה באربע שיטות שונות (BLEU, ROUGE, BLUERT, BERTScore) והשוואה לשני מודלים שונים (LM, ILM). מודל TC קיבל ציון BLEU גבוה יותר בהשוואה למודלים אחרים, וציון דומה או מעט יותר גבוה בשאר המבחנים. בנוסף ל מבחנים האילו קוהרנטיות הטקסט נבדקה גם על ידי הערכה אנושית, שם המודל קיבל ציון מעט יותר נמוך מ ILM.

Method	Human
LM	2.4 ± 0.06
ILM	3.77 ± 0.07
TC (8)	3.64 ± 0.07

Table 6: Human evaluations on text infilling. Scores were ranked between 1 and 5. Higher is better.

динаміка розширення тексту глобально

Динаміка розширення тексту глобально перевірена на 100 випадків, що відповідають за використанням моделі для заповнення тексту. Для цього було використано датасет Wikisection, який містить короткі описи артикулів з високим рівнем точності. Використанням цих даних можна перевірити, чи може модель заповнювати текст з урахуванням контексту, який відсутній у нейтральному тексті.

Модель TC згенерувала текст, який відрізняється від інших моделей, які використовують тільки один підхід до заповнення. Це може бути зуміснено, якщо звернутися до таблиці 3, де показано, що модель TC має найменший відсоток помилок у порівнянні з іншими моделями. Це свідчить про те, що модель TC використовує більше контексту, щоб заповнювати текст, ніж інші моделі.

Method	MM % (↓)
GPT2	17.5 ± 0.1
SD	10.0 ± 0.1
SS	10.6 ± 0.1
VAE (8)	10.8 ± 0.1
VAE (16)	9.6 ± 0.1
VAE (32)	8.7 ± 0.1
ID (8)	10.8 ± 0.1
ID (16)	154.8 ± 0.1
ID (32)	138.6 ± 0.1
BM (8)	9.2 ± 0.1
BM (16)	17.8 ± 0.1
BM (32)	10.8 ± 0.1
TC (8)	16.8 ± 0.2
TC (16)	7.9 ± 0.1
TC (32)	9.3 ± 0.1

Table 3: Percentage of length mismatch (MM) during generation.

реалізація розширення тексту глобально

Оцінка реалізації розширення тексту глобально була зроблена на 100 випадків, що відповідають за використанням моделі для заповнення тексту. Для цього було використано датасет Wikisection, який містить короткі описи артикулів з високим рівнем точності. Використанням цих даних можна перевірити, чи може модель модель зберігати контекст, який відсутній у нейтральному тексті.

בנוסף לזה נעשתה גם הערכה אנושית לאיכות הטקסט המוגנרט, כשמודל TC קיבל ציון גובה יותר ממודל GPT-2 אליו הוא הושווה.

Method	Human
GPT2	2.8 ± 0.06
TC (8)	3.6 ± 0.07
TC (16)	3.4 ± 0.07
TC (32)	3.3 ± 0.07

Table 7: Human evaluations on tail end quality in forced long text generation. Scores were ranked between 1 and 5. Higher is better.

סיכום של כל המבחןים שבדקו את הטקסט המוגנרט, ראה שבעזרת מודל TC ניתן לגנרט טקסט אורך שהוא גם קוהרנטי וגם ישמור על מסגרת של השיח לאורך כל הטקסט המוגנרט.

סיכום

מאמר זה מציע דרך חדשה לגינרט שפה. בשונה מהגישות הקיימות כיום המתחשבות רק במצב ההתחלתי של השיחה ובאופן אוטורגטיבי מגנרטות טקסט, מודל TC מתחשב גם במטרה הסופית של השיחה ובעזרת גשר בראוני הוא יוצר מסגרת לתוך השיחה, בתוך מסגרת זאת הוא מגנרט את הטקסט.

תוצאות הניסויים שבוצעו לבחינת הטקסט המוגנרט ממודל זה מראות שמודל TC יכול לגנרט טקסטים ארוכים תוך שמירה על קוהרנטיות ומבנהו לאורך זמן.

שיטוף פעולה: הபוסט נכתב על ידי מיכאל (מייק) ארליךsson, PhD, Michael Erlhson ומשה משען.

שנקרא:

Review 30: Diffusion-LM Improves Controllable Text Generation

פינת הסוקר:

המלצת קרייה מכותבי הסקריה: מאמר מומלץ למתעניינים במודלי שפה, במיוחד שמתחמקדים בגינרט טקסט מוכoon משימה (controllable text generation)

בahirot_citiba: בינוית

ידע מוקדם:

- יסודות מתמטיים של מודלי דיפוזיה הסתברותיים לגינרט נתונים (Denoising Diffusion Probabilistic Models -DDPM)
- הבנה טוביה במודלי שפה לייצור טקסט מוכoon משימה

ישומים פרקטיים אפשריים:

- ייצור טקסט מוכoon משימה אינטלי יוטר
-

פרטי מאמר:

לינק למאמר: [כאן](#).

לינק לקוד: [כאן](#)

פורסם בתאריך: 22.05.22, בארכיב.

הציג בכנס: טרם ידוע

תחומי מאמר:

- מודלים גנרטיביים לייצור טקסט מוכoon משימה
- מודלי דיפוזיה לגנטוט פיסות DATA חדשה

כליים מתמטיים, מושגים וסימונים:

- [Denoising Diffusion Probabilistic Models -DDPM](#)
 - [מודלי שפה מבוססי רשתות ניירונים](#)
-

תמצית מאמר:

מבוא:

מודל דיפוזיה הסתברותי (DDPM - Denoising Diffusion Probabilistic Model) שייר למשפחת המודלים הגנרטיביים המאפשרים ייצור פיסות DATA חדשות. משפחה זו כוללת גם (VAE) Variational AutoEncoders,GANs (Generative Adversarial Networks) – מודלים של זרימה מנורמלת (Normalized Flows) וכן מודלים גנרטיביים "פופולריים" קצת פחות. בשנה האחרונות הצליחו מודלי דיפוזיה להשווות ואפילו לשפר את ביצועי מודלי SOTA בתחום הראיה הממוחשבת (בעיקרGANs ו-VAE-ים). מודלים אלה שימשו לייצור של תמנונות באיכות מרתקה (ראה למשל [Diffusion Models Beat GANs on Image Synthesis](#) שנשוך במדור זה). בנוסף לפני כמה חודשים עלה לאoir מאמר שהציג שיטה בשם [GLIDE](#) שהצליח ליצור תמנונות מדיימות מהירות באמצעות מודל דיפוזיה. לאחר מכן יצא כמה עבודות שהשתמשו במודלי דיפוזיה בנסיבות שונות של הראייה הממוחשבת למשל עבור [super-resolution](#) (שיפור הרזולוציה של תמנונה).

עכשו נשאלת השאלה האם ניתן לנצל פרדיגמה זו למשימות של עיבוד שפה המערבות גנרטוט טקסט למשל לצירת טקסט מכוון משימה? המאמר הנסקר מספק תשובה חיובית לשאלת זו ומצביע שיטה לגנרטוט טקסט מכוון משימה באמצעות מודל פיקציה של מודל דיפוזיה.

עתה נתאר בקצרה את יסודות מודלי הדיפוזיה ההסתברותיים לגנרטוט DATA (ראה [פרק זה](#) ולדין יותר מעמיק). מודל דיפוזיה מורכב משני "תהליכי": התהליך הקדמי וההתהליך האחורי. **התהליך הקדמי** מורכב מכמה איטרציות של הוספת רעש גאוסי לדאטה כאשר מטרת כל איטרציה היא לטשטש את הדאטה. למשל אם הדאטה היא תמונה אז כל פיקסל עבור תהליך דעיכה: התוחלת של שער הפיקסל x_i לאחר איטרציה t הופכת להיות $x_i \sim \mathcal{N}(0, \alpha)$ כאשר $\alpha < 0$ והשונות שלו גדלה. מטרת התהליך הקדמי היא "להפוך" פיסות DATA לרעש גaussiano איזוטרופי כלומר מפולג ($\mathcal{N}(0, \alpha)$). המטרה של **התהליך האחורי** היא לשחזר את הדאטה מהרעש - וזה גם נעשה באיטרציות. מודל המסוגל לבנות פיסות DATA מריעש (בתהליך איטרטיבי) הוא למעשה מודל גנרטיבי לכל דבר.

אבל איך זה נעשה? קודם כל בדומה למה שמקובל באימון מודלים גנרטיביים נרצה "להתאים" מודל פרמטרי הממוקם את פונקציית הנראות המירבית (likelihood) של הדאטס. ניתן להשתמש ב- [ELBO](#) בשביל לבנות את החסם התיכון לנראות המירבית:

$$\begin{aligned} L_{\text{vib}} &:= L_0 + L_1 + \dots + L_{T-1} + L_T \\ L_0 &:= -\log p_{\theta}(x_0 | x_1) \\ L_{t-1} &:= D_{KL}(q(x_{t-1} | x_t, x_0) || p_{\theta}(x_{t-1} | x_t)) \\ L_T &:= D_{KL}(q(x_T | x_0) || p(x_T)) \end{aligned}$$

כאשר (x_0, x_1, \dots, x_T) היא התפלגות המשוררת באמצעות התהליך הקדמי (והיא גאוסית!!), $(x_{t-1} | x_t)$ היא המודל הפרמטרי שמאומן לשערור x_{t-1} מ- x_t ו- x_0 היא הדוגמא המקורית. כלומר מטרת האיטרציה t של התהליך האחורי היא לחזות את שער הדאטה באיטרציה הקודמת, x_{t-1} , כלומר אנו רוצים לשער את $(x_{t-1} | x_t)$. כאן x_t מסמן פלט של האיטרציה t של התהליך הקדמי.

הערה חשובה: חשוב לציין כי למרות שהתפלגות $(x_{t-1} | x_t)$ היא גאוסית לפי הגדרת התהליך הקדמי $(x_t | x_{t-1})$ היא איננו גaussiano. $(x_t | x_{t-1})$ תלויה גם בהתפלגות של הדאטה עצמו - ניתן לראות את זה בקלות אם פותחים $(x_t | x_{t-1})$ באמצעות נוסחת ביס. אולם עבור בחירה מושכלת של קבוע α ניתן לקרב $(x_t | x_{t-1})$ באמצעות התפלגות גaussית וזה בדיק מה שנעשה במודלי דיפוזיה.

מודלי דיפוזיה גנרטיביים הראשונים השתמשו בפונקציית הלואן הניל' אך לא הצליחו להציג ביצועים בריא השווא עם שיטות SOTA. ועקב כך במאמרם מאוחרים יותר במקומות למזער KL-divergence מאמנים מודל לחזות את התוחלת המותנית של הדאטה באיטרציה $t-1$. תוחלת זו מסומנת ב- $(x_{t-1} | x_0)$, כלומר המודל מאומן למזער את הביטוי הבא:

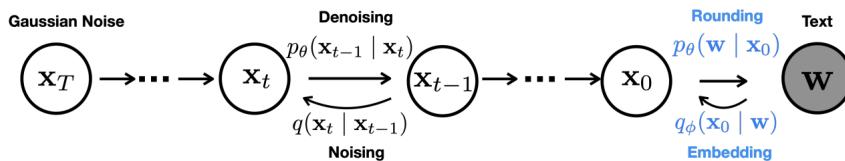
$$\mathcal{L}_{\text{simple}}(x_0) = \sum_{t=1}^T \mathbb{E}_{q(x_t | x_0)} \|\mu_{\theta}(x_t, t) - \hat{\mu}(x_t, x_0)\|^2.$$

הערה: יש כמה עבודות שבמוקם לחזות את התוחלת של הדטה בשלב הקודם ($x_{t-1} | x_t$) מ, בנו מודל לחיזוי של הרעש שהתווסף בשלב t (פרמטריזציה עצמה). גישה זו הוכחה כיציבה יותר מחיזוי ישיר של התוחלת (ראיתי) כמו הסברים לגבי הסיבה לתופעה זו אך לא השתקנה עת.

הסבר של רעיונות בסיסיים:

מודל דיפוזיה מותאם למודל שפה (לא מכוון לשימוש):

از איך נוכל לבנות מודל שפה מבוסס על עקרון הדיפוזיה? הרי הקלט למודל זה הוא דיסקרטי (המורכב ממילים או טוקנים) והוספת רעש במרחב זה לא ניתנת להגדירה פשוטה וגם משמעו זה לא גמרני ברורה. במקרים זאת המחברים מציעים להשתמש בשיכונים (embeddings) ולמרות שמרחב השיכונים הוא גם דיסקרטי בטבעו, הוספה רעש למרחוב שיכון היא יותר טבעית ו-tractable. למעשה בשבייל להתאים את מודל הדיפוזיה לשימוש זה, המחברים הוסיפו שלב ראשון של חישוב שיכון טוקנים.



כאמור, בתהיליך קדמי קודם כל ממפים את המילים w לקטורי השיכון \mathbf{x}_0 כך שהתפלגות של \mathbf{x}_0 מוגדרת בתור ($\mathbf{x}_0 | \sigma^2(w)$). לתהיליך האחורי (denoising) מושגים שלב נוסף בסוף הנקרא עיגול (rounding). מטרתו של שלב העיגול היא למפות את קטורי השיכון \mathbf{x}_0 מהשלב האחרון של התהיליך האחורי לטוקנים מהmillion (למעשה לטקסט). פועלה זו נעשתה באמצעות שערור של ($\mathbf{x}_0 | w$).

המאמר מראה כי פונקציית הלוס של מודל הדיפוזיה (החזזה תוחלת של האיטרציה הקודמת) עם השלבים שנוספו תיראה באופן הבא:

$$\mathcal{L}_{\text{simple}}^{\text{e2e}}(\mathbf{w}) = \mathbb{E}_{q_\phi(\mathbf{x}_{0:T} | \mathbf{w})} [\mathcal{L}_{\text{simple}}(\mathbf{x}_0) + ||\text{EMB}(\mathbf{w}) - \mu_\theta(\mathbf{x}_1, 1)||^2 - \log p_\theta(\mathbf{w} | \mathbf{x}_0)]$$

למעשה האיבר השני בנוסחה הזה ממציע את הפרש בין השערור ($1, \mu_\theta(\mathbf{x}_1, 1)$) של השיכון של הדטה המקורי \mathbf{x}_0 מהדטה של האיטרציה הראשונה \mathbf{x}_1 לבין השיכון של \mathbf{x}_0 , המסופם $\text{EMB}(\mathbf{w})$. האיבר האחרון ממקסם את ההסתברות של הטוקן w בהינתן השיכון שלו \mathbf{x}_0 .

מהלך אימון של מודל שפה דיפוזיוני:

אימון מודל השפה הדיפוזיוני עם פונקציית הלוס הזה, טומן בחובו כמה מוקשים (aicots הטקסט שנוצר לא גבוהה מספיק) שדורשים שימוש במספר טרייקים:

טריק 1: במקום לחזות את התוחלת של האיטרציה הקודמת, המחברים הציעו לחזות את הדטה עצמה (השיכון שלו) \mathbf{x}_0

טריק 2 (Clamping): במקום להשתמש באומדן של x_t באיטרציה t (המסומן ב- (t, x_t)) כדי לדגום את x_{t-1} ממנה, המחברים דוגמים את x_t מהשיכון של סדרת המילימט הקרובה ביותר ל- (t, x_t) .

הערה: ניתן לקבל ביטוי סגור עבור x_t מ- x_0 ורשות גאוסי סטנדרטי ($N(0, 1)$) דרך שימוש בהגדרת התהילה הקדמי.

מהלך אימון של מודל שפה דיפוזיוני מכון לשימה:

از יש לנו כרגע מודל דיפוזיה מאומן שידוע לגנרט טקסט מרעיש. השאלה עכשו איך נוכל למנף אותו לייצרת טקסט מכון לשימה, כלומר בהינתן משתנה בקרה (control variable), המסומן c . c יכול להיות עץ סינטקטי או סנטימנט שהtekst הנוצר צריך לקיים. קודם אנו צריכים לגנרט פלטים של מודל הדיפוזיה באופן מכון לשימה, המוגדרת על ידי c :

$$p(\mathbf{x}_{0:T} | \mathbf{c}) = \prod_{t=1}^T p(\mathbf{x}_t | \mathbf{x}_{t-1}, \mathbf{c})$$

از לפי חוק ביאו ($\mathbf{x}_t | \mathbf{x}_{t-1}, \mathbf{c} \propto p(\mathbf{c} | \mathbf{x}_{t-1}) p(\mathbf{x}_t | \mathbf{x}_{t-1})$). כדי ליצור פלט של שלב-1- t של מודל הדיפוזיה מבצעים $\text{log gradient descent}$ עבור $\text{log}(p(\mathbf{x}_{t-1} | \mathbf{x}_t, \mathbf{c}))$ כאשר הפרמטר המאופטם הוא \mathbf{x}_{t-1} :

$$\nabla_{\mathbf{x}_{t-1}} \log p(\mathbf{x}_{t-1} | \mathbf{x}_t, \mathbf{c}) = \nabla_{\mathbf{x}_{t-1}} \log p(\mathbf{x}_{t-1} | \mathbf{x}_t) + \nabla_{\mathbf{x}_{t-1}} \log p(\mathbf{c} | \mathbf{x}_{t-1})$$

המאמר מציע שני חידושים קלים לתהיליך אופטימייזציה זה. הראשון הוא fluency regularization המכenis משקל בין שני איברי הנוסחה: $(\mathbf{x}_{t-1} | \mathbf{c}) \log + (\mathbf{x}_t | \mathbf{x}_{t-1}) \log$. מקדם זה תורם לוויסות האיזון בין "שיטף של הטקסט" להתקאה לשימה. החידוש השני הוא שימוש ב-3 איטרציות של GD לכל שלב של דיפוזיה.

מכיוון שתהיליך הגנרט המתואר די איטי, המחברים השתמשו ב-200 איטרציות של מודל דיפוזיה במקום 2000 המקבילות. גישה זו עדין איטית באופן משמעותי משיטות פשוטות יותר, כמו אימון טרנספורמר במבנה encoder-decoder.

ניסויים ותוצאות

בחינת ביצועי המודל נעשתה עבור מס' שימושות שכלי אחת מהן בchnerה היבט אחר של גנרט טקסט, כאשר המددים להשוואה היו רהיטות (fluency) הטקסט ועמידה במשימות אליון הוא הוכן:

- גנרט טקסט מכון לשימה - ייצור טקסט בהתאם לפרמטרים נתוניים. למשל, טקסט עם סנטימנט חיובי.
- גנרט טקסט מכון משימות מרובות - ייצור טקסט בהתאם למספר פרמטרים רצויים. לדוגמה, טקסט חיובי בעל מבנה סנטנטי מוגדר.
- השלמה של טקסט חסר (infilling) - משימת השלמה של מקטעי טקסט חסרים אשר תואימים טקסט נתון.

גנרט טקסט מכון לשימה

על מנת לבדוק את פלט המודל, המחברים השווו את הטקסט שגונרט לפלאטם של מודלי שפה אחרים בחמש משימות שונות. בכל המשימות בהן מודל הדיפוזיה נבחן, הוא הציג תוצאות טובות יותר ממודלי שפה גדולים אחרים (E-FUDGE ו-PPLM). גם בהשוואה למודל (GPT-2) שאותם במיוחד למשימות אלו, להפתעת החוקרים, על ביצועי המודל הדיפוזי על מודל (GPT) שאותם במיוחד למשימות אלו בשתי משימות שדרשו הסתכלות על כל הטקסט במקביל (גנרט טקסט בהינתן עז תחבירי וגנרט טקסט בהינתן טווח תחבירי נתון), כאשר יתר המשימות המודל הדיפוזי השתווו למודל המאומן.

גנרט טקסט עבור משימות מרובות

אוסף נוסף של גנרט שפה מוכoon משימה הוא האפשרות ליצור את הטקסט המגונרט 'למס' משימות במקביל. החוקרים בחנו זאת ע"י השוואה לשני מודלי שפה אחרים (FUDGE ומודל EoP) בשני ניסויים שבכל אחד מהם הטקסט כוון לשתי משימות שונות. בשני הניסויים מודל הדיפוזיה הראה יכולת טוביה יותר בגנרט טקסט שעומד בקריטריונים של המשימות אליהן הוא הכוון, אך זה בא על חשבון רהיטות הטקסט שנוצר, שם ביצועי מודל הדיפוזיה נפגעו ממשמעותית.

השלמת טקסט חסר

במשימת השלמת טקסט, מודל הדיפוזיה הראה ביצועים טובים יותר מכל אחד מארבעת המודלים אליהן הוא הושווה, כולל מודל שאומן במיוחד זאת. העליונות של מודל הדיפוזיה הייתה עיקבית עבור כל אחת מחמשת שיטות המדידה בהן המודל נבחן.

סיכום:

המאמר מציע גישה חדשה לגנרט טקסט מוכoon משימה באמצעות מודל דיפוזיה. גישה זו מצליחה להשיג ביצועים טובים במגוון משימות, כאשר היא מראה עליונות על גישות קיימות בגנרט טקסט למשימות מרובות ובמשימות שדורשות הסתכלות על כל הטקסט במקביל. עם זאת, אני חשש שההירות הגדולה אינה גבוהה מספיק כדי להתחזרת בגישות הקיימות כרגע.

שיתוף פעולה: הפוסט נכתב על ידי מיכאל (מייק) ארליךソン, PhD, Michael Erlhison, משה משען Moshe Mishan