הערה: המאמרים שקשורים למשחקיות ולהסקה סיבתית מאוד קשורים לנושא השאלה ומדברים בדיוק על הדברים המעניינים אבל הדאטאסטים שבהם משתמשים לא מתאימים לבעיה שלנו.

1. Cognitive Model Priors for Predicting Human Decisions

<https://proceedings.mlr.press/v97/peterson19a/peterson19a.pdf>

risky choice

מאמנים מודל עם פריו שנקבע על ידי פסיכולוגים, כדי שיוכלו לאמן את המודל עם דאטאסט קטן.

כלומר, מייצרים דאטא סינטטי על סמך ידע קודם של התנהגות אנושית, ומאמנים מודלים על הדאטא הזה. לאחר מכן מאמנים את המודלים עם הדאטא האמיתי בשביל finetuning.

מציעים דאטאסט של החלטות של בני אדם (240000 החלטות מעל 13000 בעיות). Choices13k

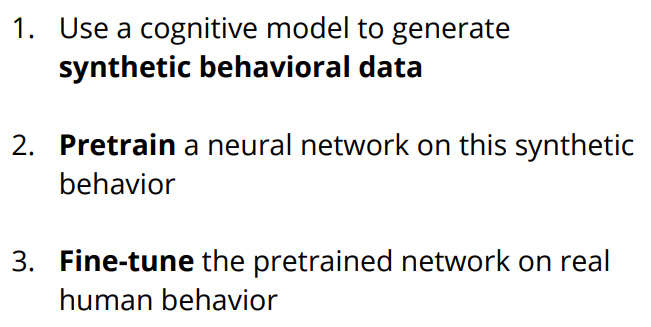
אבל מדובר בהחלטות שלא משפיעות על הפיצ'רים של הבן אדם, וגם לא מסתמכות על מודל פרדיקטיבי כלשהו.

הצעות:

* אפשר לקחת את הדאטאסט ולהתייחס לכל החלטה כאל אחת ש**כן** משנה את הפיצ'רים של הבן אדם. למשל, אדם יימדד בכמות הכסף שלו X (שאותה שואף להגדיל), וכמות הכסף שאותה הרוויח בעקבות ההחלטה ייתן לנו את X'. (**הבעיה היא שלא כתוב אם אספו פרטים על המשתתפים. דבר נוסף שבעייתי זה שתוצאת המודל f לא תלויה בx, אלא רק בהסתברויות. עם זאת, סביר להניח שהחלטות המשתמש כן ישתנו בהתאם למצבו הנוכחי.**).

כלומר ניתן להסתכל על הסתברויות ההימור כעל המודל F והשקיפות הזו היא שמשפיעה על החלטות האנשים.

* אפשר לעשות ניסוי **יחסית קטן** שמתאים בדיוק למיפוי המקורי אותו רצינו לחקור, ולהשתמש בפריו ממדעי ההתנהגות בשביל לתת בסיס למודל. הדאטא יהיה עבור finetuning.



שאלה:

מה זה אומר שהמודל הפרדיקטיבי f שקוף למשתמש? הרי אם הוא פשוט מדי אז כל שיש למשתמש לעשות זה להציב בנוסחה או משהו ולגזור. אם המודל מסובך, אז אי אפשר להבין מה עדיף למשתמש ולכן הדרך לשתף איתו את המידע היא הצגת המון דוגמאות של קלט פלט. (למשל בצורת גרף). ואז המשתמש פשוט "יתקדם בכיוון הגרדיאנט".

1. A Choice Prediction Competition: Choices from Experience and from Description

<https://web.iem.technion.ac.il/images/user-files/erev/Erev_Ert_Roth_Haruvy_et_al.pdf>

עשו 3 ניסויים (ונתנו לחוקרים בעולם להתחרות זה בזה ולנסות לחזות את החלטות האנשים).

כל הניסויים הם בחירה בין אופציה "בטוחה" בעלת סיכוי 100% לבין אופציה "מסוכנת" עם סיכוי מסוים.

1. הצגת ההסתברויות והפרס למשתמשים (שקיפות מלאה).
2. אפשרות לsampling מתוך ההסתברויות אך לא חושפים את ההסתברויות, ורק אז בחירה אמיתית.
3. בחירה עיוורת בין שתי האפשרויות והצגת התוצאה, 100 פעמים (עבור אותה הבעיה).

(**הבעיה היא שהדאטאסט קטן מאוד – 160 סטודנטים מהטכניון על 60 בעיות, וגם אין ידע מוקדם על הסטודנט- למשל כמות הכסף שלו.**)

הצעות:

* הניסוי השלישי נשמע מתאים לבעיה המקורית שלנו- אף על פי שאין לנו ידע מוקדם על הסטודנט.

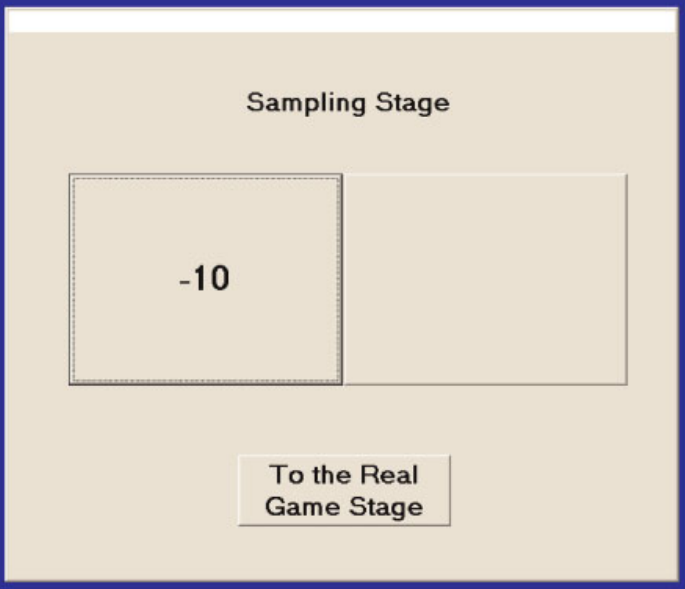
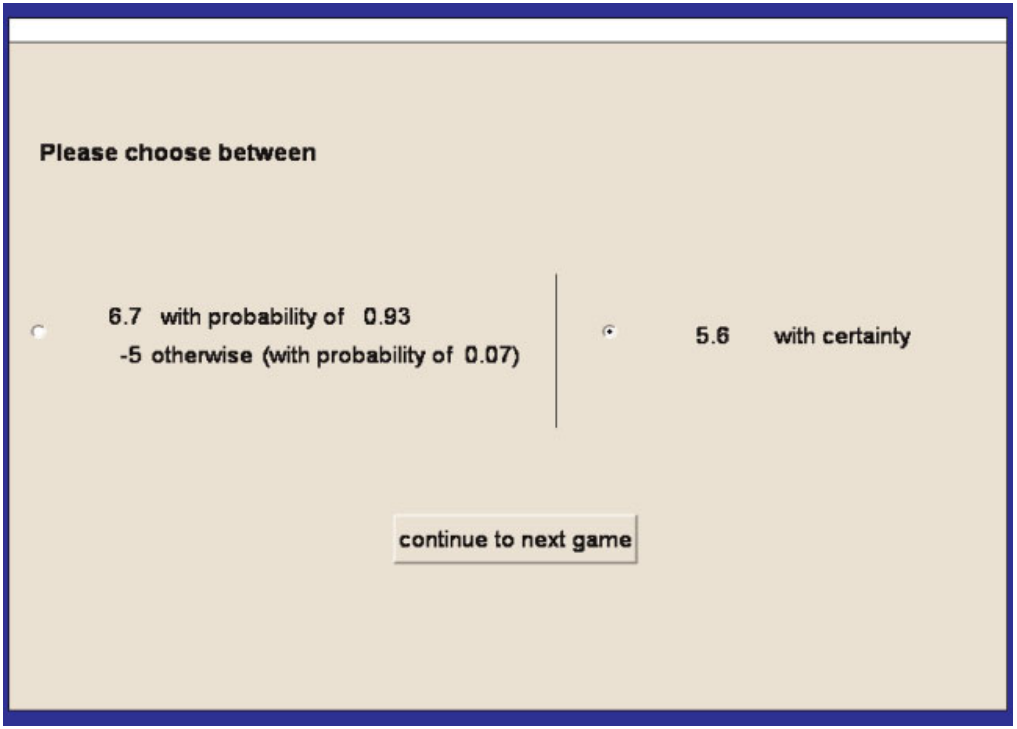
מה שאפשר לעשות זה לקחת את הדאטא מהניסוי הזה, ולהחליט שהx ההתחלתי הוא כמות הכסף ההתחלתית (שילמו לסטודנטים 40 שקלים בהתחלה וכל החלטה מורידה או מוסיפה להם כסף). ואז כל החלטה מזיזה את הx בהתאם. לכן אפשר להסתכל על "סשן של בחירות" עבור בעיה מסויימת כהרבה דגימות של מיפוי x->x’

(זה בעצם reinforcement learning של הבן אדם).

אם הדאטא לא מתאים לכזו אדפטציה אז אולי אפשר לעשות ניסוי מותאם בעצמנו.

* בגלל שבתהליך כזה המשתמש לומד את המודל רק בנקודות ש"קרובות" למצב ההתחלתי שלו,

אפשר לבצע את הניסוי עם קבוצה של אנשים במקביל, כאשר כל משתמש יקבל מצב התחלתי (x) שונה (למשל משתמש א' יקבל תחילה 50 שקלים, משתמש ב' יקבל תחילה 200 שקלים ומשתמש שלישי לא יקבל כסף כלל.



1. Explaining Human Behavior in Dynamic Tasks through Reinforcement Learning

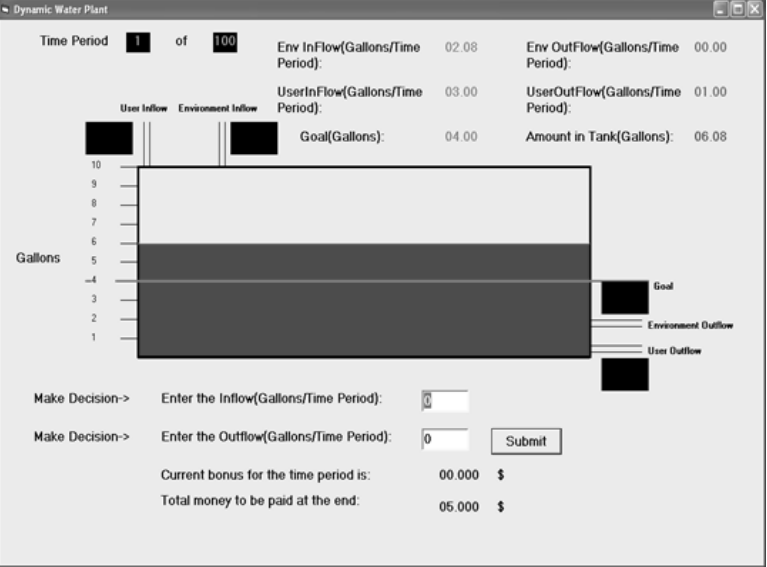
<https://www.cmu.edu/dietrich/sds/ddmlab/papers/Dutt%20inpress.pdf>

גישה של reinforcement learning בדומה לניסוי מהמאמר הקודם (2).

בן אדם מקבל החלטות עבור אותה בעיה שוב ושוב ו"לומד בעצמו את המודל", כלומר, המודל לא מוצג בשקיפות למשתמש והוא מקבל החלטה על סמך זה, אלא המודל נסתר, והמשתמש מקבל החלטות שוב ושוב ומקבל פידבק עליהן וכך הוא גם לומד את המודל וגם מקבל החלטות בו-זמנית.

דוגמה שלהם עם מפלס מים שבו המים יכולים בכל שלב לעלות או לרדת בהתאם לפונקציה נסתרת מהמשתמש, והמשתמש יכול להעלות או להוריד את המים לפני השינוי במטרה להתקרב למפלס מסויים.

הם מאמנים מודל לחזות את החלטות הבן אדם בזמן שהוא מקבל החלטות, ולא אחרי.



לגבי הפרוייקט השני,

<https://5harad.com/papers/wisdom-of-crowds.pdf>

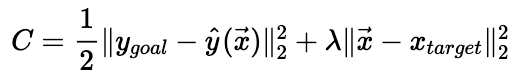
דאטאסט ענק עם כל מה שצריך.

ADVERSARIAL LEARNING

* זיהוי תמונות
* פלטור ספאם
* פלטור פקטות
* Nlp
* זיהוי ביומטרי
* זיהוי וירוסים

כללי:

באופן כללי אנחנו יכולים לייצר דוגמאות אדברסריאליות משלנו



ולפתור עם גרדיאנט דיסנט.

Classifier evaluation and attribute selection against active adversaries

<https://www.stat.purdue.edu/~xbw/research/BoweiXi.AdversarialClassification2010.pdf>

הגדירו את הבעיה כבעיית אופטימיזציה של משחק בין 2 שחקנים. הם פותרים אותה באמצעות היוריסטיקות ומטלב ומוצאים נקודת שוויון בין המסווג למי שנותן את הדוגמאות.

הם משתמשים בדאטאסט של הלוואות ומייצרים דוגמאות של הלוואות שנמצאות בנקודת השוויון הזו. הטענה היא שאפשר להשתמש בשיטה הזאת על כל דאטאסט של מסווג שמפלטר דברים (מחלקה טובה ומחלקה רעה).

NLP:

Black-box Generation of Adversarial Text Sequences to Evade Deep Learning Classifiers

<https://arxiv.org/pdf/1801.04354.pdf>

ייצור של דוגמאות אדברסיאליות של משפטים, ביקורות וספאם. יש דאטאסט שצריך לבקש.

LEARNING THE DIFFERENCE THAT MAKES A DIFFERENCE WITH COUNTERFACTUALLY-AUGMENTED DATA

<https://arxiv.org/pdf/1909.12434.pdf>

זה מה שניר שלח.

לקחו ביקורות של סרטים והפכו אותם תוך שינוי מינימלי לביקורת הפוכה.

זיהוי תמונות:

DAmageNet: A Universal Adversarial Dataset

https://arxiv.org/pdf/1912.07160.pdf

Generating Adversarial Examples with Adversarial Networks

<https://arxiv.org/pdf/1801.02610.pdf>

משתמשים בGANS (generative adversarial networks) כדי לייצר תמונות אדברסריאליות ריאליסטיות. יש דאטאסט.

Adversarial Transformation Networks: Learning to Generate Adversarial Examples

<https://arxiv.org/pdf/1703.09387.pdf>

משתמשים בGANS (generative adversarial networks) כדי לייצר תמונות אדברסריאליות ריאליסטיות. יש דאטאסט.

פרסומות:

Sales Conversion Optimization

<https://www.kaggle.com/loveall/clicks-conversion-tracking>

Criteo Sponsored Search Conversion Log Dataset

<https://ailab.criteo.com/criteo-sponsored-search-conversion-log-dataset/>

שני אלה הם דאטאסטים של פרסומות של מוצרים, האם הקליקו עליהם, האם בסוף קנו את המוצר, כמה עלתה הפרסומת וכו'.

Ads\_CTR\_Optimisation

<https://www.kaggle.com/akram24/ads-ctr-optimisation>

10 פרסומות עבור אותו מוצר ולכל פרסומת האם הקליקו עליה או לא.

תמיד אפשר לעשות סקר.

The main takeaway is that should not be reversible, we don’t need to restrict it to be reversible.

Idea 1:

make sure is scaled to the cost function by adding a regularization term.

Idea 2:

We can “find” by training the non-strategic model:

And then train the strategic model with the learned .

To make sure that the scale of is good (in relation to the cost function) we can re-scale or the cost function (by setting for example).

We can also do this simultaneously (like GANS) and train both the non-strategic and the strategic models together (not optimizing regarding the strategic model calculations).

Though this ‘technique’ is not unique to our differentiable model – every algorithm could use a preprocessed .

Idea 3:

Since our model is differentiable, maybe we can do something with recurrent NN. For instance, if the input is a variable-sized sentence, we can use a recurrent version of our model to work with it! Need to formalize it more but maybe you can help me focus on a well defined model.