Masterarbeit

Climate Informatics TU Berlin / Causal Inference Group DLR Jena

Are We Explaining the Data or the Model?

Concept-Based Methods and Their Fidelity in Presence of Spurious Features Under a Causal Lense.

Lilli Joppien

Betreuer*innen: Oana-Iuliana Popescu, Simon Bing

Erstgutachter: Prof. Dr. Jakob Runge

Zweitgutachter: Prof. Dr. Tim Landgraf (oder Prof. Dr. Grégoire Montavon ?)

Berlin, November 28, 2023

b

Abstract

- The abstract must not contain references, as it may be used without the main article. It is acceptable, although not common, to identify work by author, abbreviation or RFC number. (For example, "Our algorithm is based upon the work by Smith and Wesson.")
- Avoid use of "in this paper" in the abstract. What other paper would you be talking about here?
- Avoid general motivation in the abstract. You do not have to justify the importance of the Internet or explain what QoS is.
- Highlight not just the problem, but also the principal results. Many people read abstracts and then decide whether to bother with the rest of the paper.
- Since the abstract will be used by search engines, be sure that terms that identify your work are found there. In particular, the name of any protocol or system developed and the general area ("quality of service", "protocol verification", "service creation environment") should be contained in the abstract.
- Avoid equations and math. Exceptions: Your paper proposes E = m c 2.

Motivation

- explainable AI shows great progress in visualizing how neural networks see/decide
- however there have been many criticisms and some argue that the XAI methods don't show what is actually seen by the NN and rely more on hyperparameters or the data itself.
- For example, it is known that some attribution methods do not react well to constant vector shifts in the data which do not affect prediction.
- it is especially unclear how the network deals with causal constructs: is there a difference between how it displays cause and effect, can it find important interactions between 2 variables or find spurious correlations?
- we want to identify how the ground truth biasedness of a dataset interacts with the biasedness of the model and the biasedness of the explanation
- for general attribution methods it has been shown that heatmaps can be misleading. If the spurious feature has any correlation with the core feature, it will have importance assigned. Often, the spurious feature comes as a watermark which is easy to identify. Consequently its importance can be overestimated when looking at a general heatmap of an image.
- Looking at individual concepts with their relevances and specific heatmaps has the potential to identify which of the features (core or spurious) is actually most relevant.

d

Problem Statement

- investigate the example of CRP, a recent method which takes the popular Layer-Wise Relevance Propagation to the next level, by producing conditional attributions for neurons or sets of neurons coined "concepts"
- find out, whether the heatmaps or relevances produced by this algorithm have a connection either to the causal ground truth of data or the "causal pathways" in the NN

Approach

- for validation purposes very simple disentangling dataset DSPRITES
- introduce "causal" biases into dataset, by adding small watermark not uniformly to certain images
- use a very small neural network, which seems to learn the bias strongly (check for accuracy)
- as preliminary experiment check, if the bias is strongly visible in the data: if the heatmaps/crp hierarchies produced on average for the watermarked/un-watermarked subsets differ strongly
- *do causality lol*

Results

- does CRP succeed in identifying the true biasedness of the model
- what do we want to explain
- does this result generalize for other attribution methods, data, SCMs?

Conclusions

- found a new benchmark measure to combat the critique about the robustness and fidelity of especially concept-based methods.
- from that new method a way to enrich or improve those methods arises
- it is important to look at explanations in a more causal light because that is what they are ought do be doing
- what else needs to be done especially

Zusammenfassung

Hier ist eine Deutsche Zusammenfassung die so noch nicht existiert, um zu testen ob ich auch sachen zu overleaf schicken kann.

Contents

List of Figures

List of Tables

1. Introduction

- (1-2 pages)
- Context: make sure to link where your work fits in Problem: gap in knowledge, too expensive, too slow, a deficiency, superseded technology. Strategy: the way you will address the problem
- Outline of the rest of the paper: "The remainder of the paper is organized as follows. In Section 2, we introduce ..Section 3 describes ... Finally, we describe future work in Section 5." (Note that Section is capitalized. Also, vary your expression between "section" being the subject of the sentence, as in "Section 2 discusses ..." and "In Section, we discuss ...".)
- Avoid stock and cliche phrases such as "recent advances in XYZ" or anything alluding to the growth of the Internet.
- Be sure that the introduction lets the reader know what this paper is about, not just how important your general area of research is. Readers won't stick with you for three pages to find out what you are talking about.
- The introduction must motivate your work by pinpointing the problem you are addressing and then give an overview of your approach and/or contributions (and perhaps even a general description of your results). In this way, the intro sets up my expectations for the rest of your paper – it provides the context, and a preview.
- Repeating the abstract in the introduction is a waste of space.

REFER MOR TO *Are We Explaining Th Data Or The Model?*

1.1. Motivation and Context

The recent method of Concept-Relevance-Propagation (CRP) introduced in [1] has been developed for a more fine-grained explanation of a neural networks decisions. Instead of producing one saliency map explaining the overall prediction output such as LRP [5] does, each *concept* in some hidden layer of the network gets assigned a conditional relevance and its own saliency map. In addition to the saliency maps, the relevance scores also act as a metric to maximize when searching representative samples for each of the concepts. According to the authors, through this more detailed explanation one can not only understand *where* a model sees the most relevant features, but also *what* features are relevant in this area. Their claim is, that the deeper layers of models represent concepts which are human-understandable and therefore aid in the explanation of what the model predicts.

Some works have criticized local attribution methods, to which LRP counts, for their class-insensitivity due to the lack of negative explanations as well as overall

subpar performance in the *limit of simplicity* i.e. for very small linear datasets. In the following we will investigate whether the extension through the concept conditional saliency maps and relevance scores can alleviate some of the criticisms.

Others call for more user-guided evaluation of explanation methods as the ultimate goal is to help humans understand and evaluate machine learning models. One example of a user study and accompanying benchmark dataset is [30]. Similar to our work they investigate how well users can quantify biases of a model, one of the most important applications of XAI methods.

There is still no consensus on the appropriate evaluation of back-propagation methods specifically and saliency methods in general. Most authors introducing new methods show explanations on examples from typical benchmark datasets and models. Usually ablation tests, in which singular neurons/channels are deactivated in descending order of attributed relevance, give some confidence that the features identified as important indeed have some relationship with the prediction. However it is unclear whether the explanation methods sensitivity to e.g. biases in the dataset is in accordance with the actual models sensitivity.

ivation
mple of why
ing biases is
of the most
ortant tasks
XAI

- it is super important the explanation method has high fidelity when identifying and quantifying biases a model has learned
- data is always biased, we want to find the bias
- but often the model can learn the *true* features of a distribution although it has strong *spurious* features
- [1] has shown this with watermark example and also somewhat with dog snout example
- need a good example though
- thesis: data is always biased, it is basically impossible to get completely unbiased data in such quantities. especially because sometimes we are not even able to identify the biases as we humans are prone to them too
- so in accoradance to *fair AI* it seems impossible to aim for *completely unbiased* models, as they would need to have all knowable and unknowable knowledge of the universe to not predict 'out-of-distribution'
- instead we should identify a measure of biasedness which tells us how strongly a spurious feature is used and then depending on the use case a threshold for this can be defined.

Therefore we will extend previous work on evaluating the explanation methods fidelity in the presence of data biases and Clever-Hans features. Due to limited resources a user study like [30] is not possible in our case. Instead we intend to develop a metric to quantify the coupling between the models prediction performance to the concept relevances as an artificially introduced bias gets stronger. To test this metric we propose a simple artificial benchmarking dataset based on the existing disentangling dataset *dsprites* [19]. To some of the images

we add a watermark based on a structural causal model (SCM) similar to how we expect the causal relationships in real-world watermark examples to be. Neither does the watermark itself cause the label, nor the label the watermark. Instead, a third, unknown confounder has an effect on both the presence of the watermark and the shape shown in the image. The confounding variable termed the *generator* is mixed with other random variables as described in [10]. Here, the generator is the signal and the other *causal factors* of the two variables the noise, so a better term than 'signal-to-noise' ratio might be 'spurious-to-core' ratio. (The terms 'spurious' and 'core' features are taken from [28].)

Knowing the generating factors of these benchmark images, showing either rectangles or ellipses in different sizes, rotations and positions helps to quantify the ground-truth feature importance of not only the feature to be predicted but expectedly irrelevant features (as a baseline) as well as the Clever-Hans feature.

With the aim of evaluating fidelity in the presence of a spuriously correlated feature, a zoo of models is trained with varying signal-to-noise ratios of the watermark feature. Ground-truth biasedness is calculated for each model and each feature as shown in appendix A.1. The models coupling with the core feature shape suffers and with the watermark feature increases as the spurious-to-core ratio rises. For a preliminary test the total relevance of the pixels within a small bounding box around the watermark are compared to the total relevance of the rest of the image, using the saliency map produced as a global summary and equivalent to what LRP would produce.

If CRP indeed produces an accurate explanation, more concepts should assign higher relevance to the bias feature the stronger the bias impacts the prediction of the model. It is important to note, that the model might accurately predict based on the real feature even though the bias is strong, when there are enough counterexamples. Appendix A.1 shows the non-linear interaction between prediction accuracy and spurious-to-core ratio. Now the question is, whether CRP can correctly identify this non-linear relationship or whether CRPs attribution to the spurious feature will more closely follow its actual presence in the data. In other words: Does CRP learn the causal effect of the spurious feature on the model or just the causal effect within the data? Our goal is to quantify the effect that CRP actually has on human understanding. So even if the overall importance of the watermark can be either denied or affirmed, the numeric importance might not be the same as what a user can see and find through heatmaps, relevance hierarchies and relevance maximization image sets. Therefore it is necessary to develop methods which quantify human understanding of biasedness?

1.2. Strategy

refine strategy based on what actually did

- use very simple artificial disentangling benchmarking dataset DSPRITES
- add artificial watermark to artificial benchmark... because we need ground truth
- create dataset with biased and with unbiased watermark distribution

- train very small convolutional neural network on recognizing shapes
- evaluate CRP on neural network trained on biased and unbiased dataset

1.3. Outline

To further motivate this approach I will in the following summarize previous work on causal XAI, evaluation of XAI and local attribution methods in chapter 2. Then I will lay down the theoretical framework of structural causal models and the used XAI method and evaluation in chapter 3. Chapter 4 introduces the benchmark inspired by causal models and the convolutional neural network model. It also describes the methods used to establish ground-truth *biasedness* of the models as well as of their explanations. Finally the performances are compared in chapter 5 and discussed in chapter 6.

2. Related Work

about 4-6 pages
make a distinction between methods/papers that discuss similar approaches and methods/concepts used in this thesis

1. Back-Propagation/Saliency/Attribution/Local methods name them all
2. LRP and CRP in more detail, showing Reduans results
3. Current XAI evaluation methods - Feature Ablation, Visual Inspection, TCAV
4. Current Criticism of BP methods and lack of methodical evaluation
5. [29], [33], [15] select criticism to look at
6. XAI Methods, Criticism and Evaluation methods using Causality
7. Use of causal methods in XAI and unused potential for evaluation
8. Other benchmark datasets that have been used for evaluation, why need a new one?
9. dsprites dataset? or in method
10. why do we want to look at models reaction to bias-to-core-ratio?

2.1. The Field of Explainable Artificial Intelligence

General Map of the field, embedding CI

1. XAI is needed for AI because of black box other approach is making AI not black box
2. generally divided into local and global methods
3. name a few popular global methods
4. local methods that rely on attribution/ saliency maps (gradientXinput, integrated gradients, LRP, ???)
5. what are backpropagation methods, saliency methods, local attribution methods
6. CRP is based on LRP, so in principle it is a loal attribution method. However the authors argue that it could be a *glocal* method because it can be used to summarize the workings of the model over many samples

General Overview papers to cite

- focus on post-hoc explanations + theoretical foundations, test algorithms [26]
- need some more

overview pape and map of X papers

2.2. Layerwise Relevance Propagation (LRP)

what has LRP been used for already, in which context to set CRP

- LRP first paper [5]
- general XAI [26]
- mention that it has been getting a mathematical background with Deep Taylor Decomposition [21]
- LRP in practice [16]
- disentangle representations, similar to PCA: Principal Relevant Component Analysis - uses LRP [9]
- LRP is also good at pruning... idea/intuition: if you can "prune" certain neurons, their causal effect must be none or extremely small [34]
- recent criticism of Sixt here? (deep taylor decomposition fails, when only positive relevance taken into account, matrix falls to rank 1 [30])

2.3. Concept Relevance Propagation (CRP)

which papers have been published on this

- from where to what... CRP main paper [1]
- reveal to revise: whole framework for XAI using CRP as one of the methods for concept/bias discovery [24]
- using CRP to identify and unlearn bias 'Right Reason Class Artifact Compensation (RR-ClArC)' [11]
- newest summary paper [2]

2.4. Evaluation of XAI Methods

e general
t evaluation
nods exist,
ch apply to
P etc.

2.4.1. Evaluating Back-Propagation Methods

The research on quantification and evaluation of XAI methods has increased with their rising popularity. Recently, a plethora of benchmarks and theoretical analyses have examined the fidelity, especially of feature importance methods, to the model they are trying to explain. Evaluations commonly used by authors of new XAI methods include feature ablation and data randomization (e.g. pixel flipping) . . Additionally, more complex benchmarks [14, 4, 6, 28] which are often human-supervised aim at comparing XAI outputs to human-understandable concepts.

- differentiate between numerical evaluation and evaluation through user studies
- examples of often used evaluations for local attribution methods and concept-based methods:
  - feature ablation and related methods
  - TCAVs [14] with benchmark feature set (hard and often not applicable)
  - clevr-xai? [4]
- clever XAI artificial benchmark dataset [4]
- NetDissect dataset with concept-segmented images [6]
- also other concept/neuron dissection by same authors, similar idea to CRP [7]
- creates new dataset (human-supervised) to detect core vs spurious features [28]

outline which problems CRP solves well, draw connections between unsolved criticism and causal perspective

Recent Critique of Saliency Maps

Although a general lack of dependence between explanations and their model [3, 13] has so far only been studied for less complex attribution methods, current research still draws a less than ideal picture of XAI's fidelity. Kindermans et. al. [15] show that a constant vector shift on the input data, which is not affecting the performance of the model, can lead to misleading explanations. [29] finds the class insensitivity of some back-propagation methods to be due to their improper use of negative relevance. While authors of new methods often underline their results with user studies , Sixt et. al. [31] among others show that XAI methods do not necessarily increase humans skill at identifying relevant features.

cite

cite

Constructing a test which is neither too simple and therefore too far away from realistic application scenarios nor not quantifiable empirically due to its *human* component or unidentifiable ground truth, poses a challenge which [10] tries to tackle. This benchmark is based on recent analysis [33] of suppressor variables, which can be for example the background color of an image, that are used by the model without having an association to the core features to normalize the image and improve the prediction. They introduce a generation process for mixing the suppressor and real features which serves as inspiraiton for the structural causal model applied here.

- explanations are independent of later layers (no negative relevance) [29]
- suppressor variable "in practice, XAI methods do not distinguish whether a feature is a confounder or a suppressor, which can lead to misunderstandings about a model's performance and interpretation"

- kinda stupid, because nueral network also does not make a difference between suppressors and confounders [33]
- the (un-)reliability of saliency methods: should fulfill 'input invariance'
- saliency method mirrors sensitivity of model with respect to transformations of the input
- normal LRP root point (zero) not working
- pattern attribution reference point works (direction of variation in data, determined by covariances) [15]

1. [31]: evaluation of heatmaps/saliency methods not enough based on actual user studies and human performance / explanation quality
   task: look at explanation and rate, weather each feature is relevant or irrelevant
2. [33]: explanation of suppressor variables (that have no statistical association with target) gives false impression that of dependency if their inclusion into the model improves it
   task: linear model with 1 real and 1 suppressor variable, saliency methods mark both suppressor variable and core variable as important
3. [29]: because matrix is converging to rank 1 in BP methods that dont use negative relevance scores appropriatly, heatmaps are not class sensitive
   task: randomize more and more network parameters, look at heatmap for and against class
4. [15]: heatmap methods are sensitive to constant shift in input data, but should fulfill input invariance
   task: add "watermark style" input shift, test if model still predicts accurately and then if heatmap does same as model
5. [13]: explanation depends more on hyperparameters than on model weights and prediction itself
   task: quantify treatment effect when changing hyperparameters in comparison to changing model weights
6. [3]: some saliency methods are independent to both the model and the data generating factors (not testing LRP)
   task: compare explanation trained on true model with explanation trained with random labels, also compare to simple edge detector which is very similar often
7. [25]: use generative model to identify (causal) latent factors and estimate effect they have on prediction outcome
   task: use data with known latent generating factors to test effect estimation on a constructed causal graph

8. [23]: build SCM over input-model-output -> has potential to be more accurate than saliency purely observational

9. [8]: build SCM over last linear layer before output and attribute because of sensitivity to constant shifts as shown by Kindermans
   task: treat Model as SCM and calculate interventional expectations and average causal effect

Causality Research on Evaluation and Benchmarking of XAI

The link an explanation and its model should have, has come under the causal lense both for developing new XAI methods and their evaluation . Counterfactual explanations cite

which other methods/approaches/papers are there that broadly connect explainable AI and causality

- general map of causality and XAI mixups
- counterfactual stuff
- seeing model as scm stuff [8]
- representation learning
- overview of [27]
- generally, mostly about counterfactuals: [22]
- causal attribution, similar to LRP but more "causally" neural networks as SCMs [8]
- causal concept effects (edges in mnist) [12]
- causal in most general sense:independent/disjoint mechanism analysis [17] [18]
- causal binary concepts [32]
- basic framework/idea of interpreting NN as skeleton of SCM and using some transformation to quantify effect:[23]

3. Theoretical Background

about 20-30 pages (rather less I guess?)

1. Introduction to XAI in general
2. Evaluation of XAI methods in general
3. Structural Causal Models and causal framework

write backgro

3.1. Neural Networks

- Explain all general concepts that are needed for understanding CRP etc
- layers
- neurons
- convolutional blocks/ layers
- activation functions (especially ReLU)
- other types of layers?
- backpropagation / forward

3.2. Layerwise Relevance Propagation

Layer-wise relevance propagation [5] is the basis for concept relevance propagation and is next to SHAP, LIME, Integrated Gradients among the most highly cited local attribution methods in XAI. As other saliency methods, LRP is commonly used in computer vision to attribute importance to each pixel in an image, which can then be visualized as a heatmap, but is also applicable to other data formats. In the following I will summarize the basic functioning of LRP for neural networks as described in [5]:

cite

LRP assumes that the model has multiple layers of computation it can be decomposed into, starting from the input layer, for example the pixels of an image, to all latent layers l and finally to the output layer. Further each of those layers has $V(l)$ dimensions for which a Relevance Score $R_d^{(l)}$ could be determined so that the following equation holds:

$$f(x) = ... = \sum_{d \in l+1} R_d^{(l+1)} = \sum_{d \in l} R_d^{(l)} = ... = \sum_{d} R_d^{(1)} \tag{3.1}$$

In neural networks, the general forward step for one layer most often includes weighing the previous layers outputs x_i with the current layers weights $z_{ij} = x_i w_{ij}$, summing the results for all connected neurons and their bias $z_j = \sum_i z_{ij} + b_j$ and running this through a non-linear activation function $x_j = \sigma(z_j)$. The idea then is to follow the flow of relevance from the output, where usually the prediction value is taken to initialize the relevance $R^(1)_d$, back to the input layer by decomposition. In the simplest case relevance is proportionally propagated back to the previous layer where the relevance of all connected neurons is aggregated in the following:

$$R_i = \sum_j R_{i_j} = \sum_j \frac{z_{ij}}{z_j} R_j \tag{3.2}$$

To apply LRP, best practices and rules have emerged [16, 20, 26]. However in this thesis we stick to the propagation rule that the authors of CRP use, namely the composite $LRP_{\epsilon-z+-\flat}$-rule (or "epsilon-plus-flat"), which is recommended by [16] and uses different rules for different parts of the model, further described in the appendix section A.1.

3.3. Concept Relevance Propagation

LRP aggregates the significance of all latent layers and their neurons into one importance map, where the intermediate layers outputs are merely a side-product of the computation. Achtibat et. al. propose in their recent work [1] to use those intermediate results to further disentangle the attributions. While in LRP the initialization at the output layer usually takes the value of one class output y w.r.t input $\mathbf{x}$, all other output neurons set to zero, and thereby produces a class-conditional attribution ($R(\mathbf{x}|y)$), a similar thing can be done in latent layers too. Allthough it is yet unclear how to interpret the attribution to these hidden features, the authors of CRP propose to obtain importance scores for them by computing "(multi-)concept-conditional" relevances $R(\mathbf{x}|\theta)$. The variable θ here describes a set of conditions c_l which in essence *filters* for certain *concepts* i.e. features in potentially mutliple layers by masking out all other features' contributions:

$$R_{i_j}^{(l-1,l)}(\mathbf{x}|\theta \cup \theta_l) = \frac{z_{ij}}{z_j} \cdot \sum_{c_l \in \theta_l} \delta_{jc_l} \cdot R_j^l(\mathbf{x}|\theta) \tag{3.3}$$

δ_{jc_l} is the Kronecker-Delta selecting the relevance R_j^l of feature j in layer l if that index is in the condition c_l, masking out all other features in that layer. If no condition is set for a particular layer, the relevance from that layer is not masked. The authors note that conditions within the same layer compare to logical OR operations and across layers to AND operations. In the following a small example illustrates the process (Figure 3.1):

- some examples of usage:
  - relevance scores for *concepts* (=neurons)
  - relevance maximization images
  - conditioning on single concepts/ neurons ...?

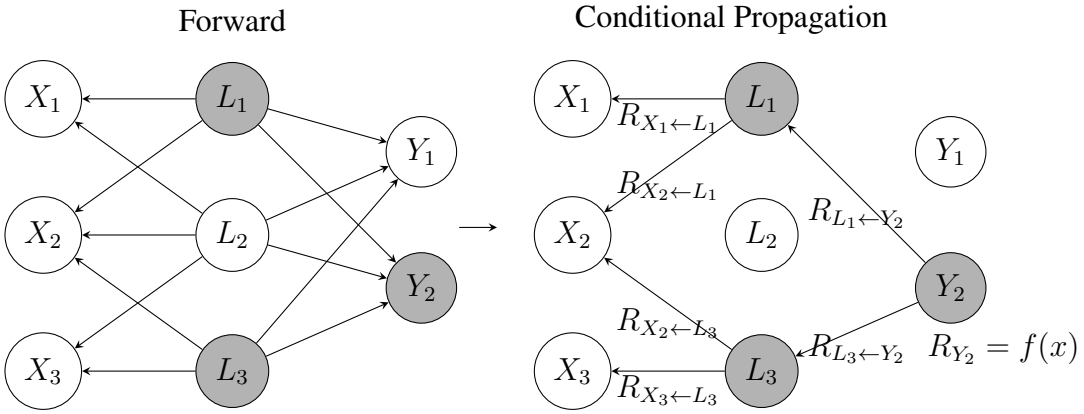

Figure 3.1.: Left side: simple neural network forward pass with input layer X, one hidden layer L and output layer Y. Conditioning set $\theta = \{L_1, L_3, Y_2\}$
Right side: only the relevance of the neurons matching the conditioning set is propagated back
Result at input pixel $R_{X_2} = \sum_j R_{X_2 \leftarrow L_j} = \sum_i \sum_j \cdot \frac{a_i w_{ij}}{\sum_h a_h w_{hj}} R_j \ldots$

- attribution graph

3.4. Causal Framework

3.4.1. Structural Causal Models

- Explain and define in detail Structural Causal Models
- neural networks could be seen as SCMs [8]
- but AI / neural networks in general do not care about causation and work through finding useful correlations
- and that is good this way, otherwise they would never find anything useful, statistics and correlations are great
- none-the-less the better we get at identifying spurious features the more causal methods might apply?
- it doesn't matter whether the network has found the actual causal reasons for its prediction, but explanations are a distinctively causal concept.
- and explanation asks how and why, so we want to know the cause of model predicting Y from X
- causal methods have started to be used for evaluation of xai

3.4.2. Interpretation as Interventions

???

3.4.3. Data Generation Process

Other?

- Short introduction to causal effects
- counterfactuals
-

3.5. Evaluation of Explanations

3.5.1. Ground Truth Importance

- What are currently used ground truth importance measures for concepts or latent factors
- introduce Prediction Flip with formula or application to our use case
- R2 score with formula [29]
- mean logit change with formula
- make clear: human understanding is the ultimate goal, so user studies are the gold standard (but often not well done) but not feasible here
- relate to constant vector shift problem and how this might be measured

3.5.2. CRP Concept Importance Measures

1 proper
sure

- explain the measures i use to score how well the concepts are separated
- show theoretical basis

3.5.3. Causally somehow?

4. Methods

about 10-30 pages (rather more I guess)

- (1/3 of thesis)
- start with a theoretical approach, describe the developed system/algorithm/method from a high-level point of view,
- go ahead in presenting your developments in more detail

1. Benchmark dataset dsprites
2. adaptation with watermark and spurious-to-core feature ratio as an SCM
3. training X models with different ratio, cutoff and learning rate on cluster
4. computing *ground-truth feature importance* of core, spurious and unbiased features: mean logit change for output, R2-score, prediction flip
5. baseline(?) score how much importance is generally assigned to spurious feature (bounding box?)
6. special score for how much importance CRP assigns to concepts encoding spurious feature
7. causal effect estimation? or something like that

4.1. Causal Benchmark DSPRITES-WM

find good nam for adapted benchmark dataset

4.1.1. DSPRITES

- why do we need another dataset for benchmarking watermark bias??
- (we don't but its nice to have)
- some other benchmarks that deal with similar questions are...
- existing benchmark dataset dsprites [19]
- explain latent factors and why we need them

4.1.2. Causal Model

- how I add watermark?
- adaptation with watermark and spurious-to-core feature ratio as an SCM
- causal effect stuff: see fig. 4.1
  - have latent factors - can intervene on each factor extensively
  - for model we can also assume SCM??? all connected neurons are causally connected
  - in given example prediction has shape AND watermark as causal ancestors
  - but in real world example spurious feature is only selection bias?
  - need to find good causal covering for what i am doing here
- why the hell does this make any sense whatsoever???

the hell
ites-wm

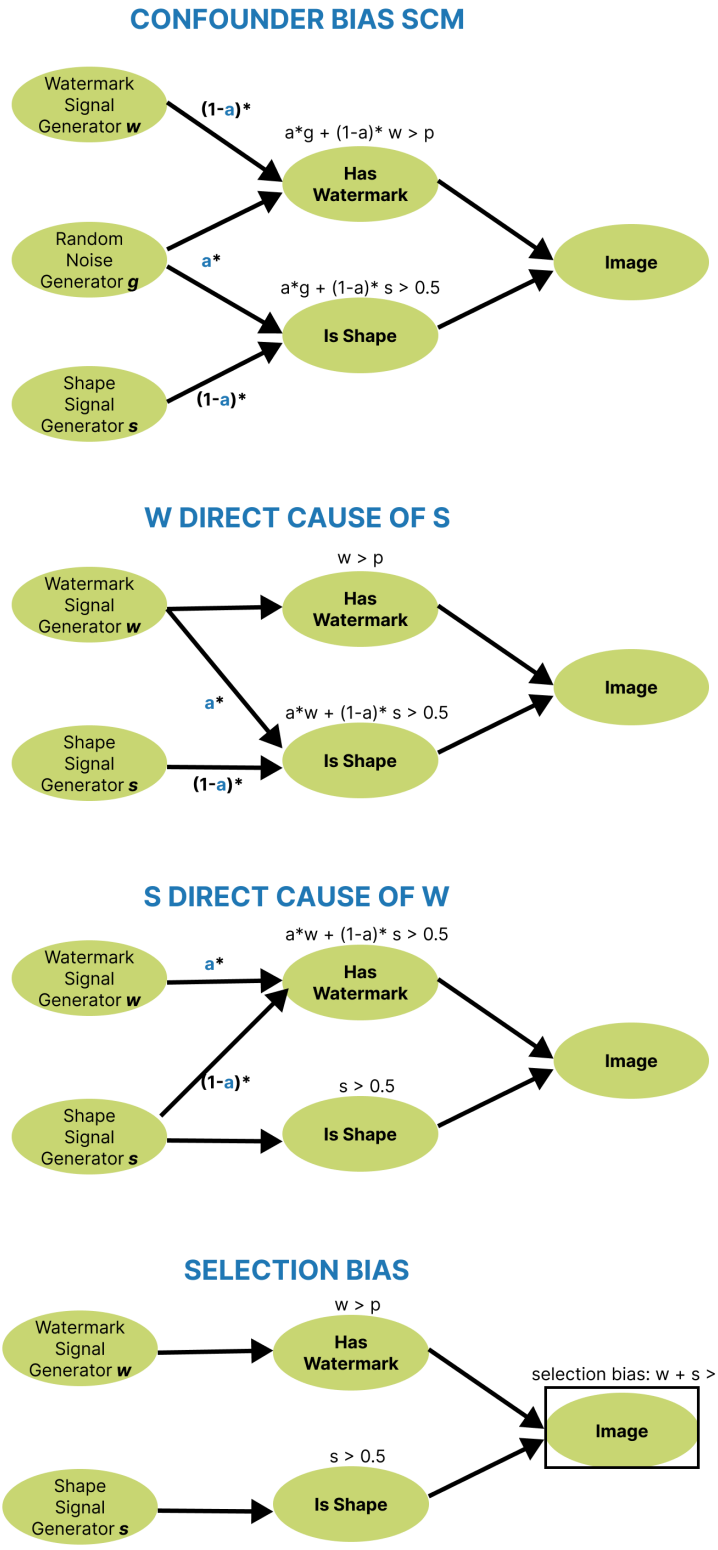

Figure 4.1.: go more into detail about why and which SCM and what to expect from 'real' data

4.2. CNN Model Zoo

4.2.1. Model Architecture

- architecture of the model with reasoning
- size and dimensionality of model has been chosen with eye-ball / trial-and-error method (4 conv was too bad, more than 8 was too redundant or often empty)
- maybe show little example of what purely linear model can achieve?

4.2.2. Hyperparameter Choice

- optimize hyperparameters over all possible biases
- interesting observation: learning rate has different optimal values depending on bias strength
- important to note that it has been shown that often explanation depends on hyperparameters causally [13].
- therefore do not change hyperparameters

4.2.3. Training and Accuracy

- training split?
- how many models with which different features are trained
- showing some examples of heatmaps and maxrel images for different bias strength
- accuracies for all models plot

4.2.4. Computational Setup

- computed on personal dell xps 13 with cpu
- and on cluster

ter specs

- how long did training all models take?

4.3. Preliminary (Causal) Experiments

uld i include
el scm stuff
attribution
hs etc?

- explain and show idea of a causal model for the whole network
- explain why it didnt work (too high, because linear correlation)
- attribution graph as a causal model???

- ideas and experiments with relevance maximization
- something more along the lines of intervening on hyperparameters? [13]

4.4. Establishing a Ground-Truth of Biasedness

- non-linearity: This can also be explained information-theoretically

explanation for non-linear biasedness - information-theoretically

4.4.1. Accuracy for Subgroups

- is the most 'ground' ground-truth measure of biasedness
- is also somehow related to the others???
- not as exact as mean logit change etc. ?

how is accura related to prediction flip etc.

4.4.2. Prediction Flip, R2 Score and Mean Logit Change

- prediction flip and r2 score are different sides of same coin
- mean logit change is more exact, as sometimes prediction stays the same but gets less confident (logits change a bit in that direction)
- mean logit change shall be used as ground truth of *biasedness*

4.4.3. Interpreting Mean Logit Change as Causal Intervention

- it is basically the causal effect of intervening on a latent factor on the models output
- theoretically the interventio must have exactly the same causal effect on the explanation as on the mean logit change???

4.5. Measuring Biasedness for Heatmaps

- this is a more general approach of measuring the biasedness of a saliency methods explanation
- good about it: humans look at the heatmaps and only see whether the watermark is colored or not to identify its importance.
- problem: humans have a hard time estimating the overall importance of concepts/features if they have varying spatial extend, see [1] about noses and fur of dog
- so if watermark is even just a little bit red, it will be important to humans
- even bigger problem: NN do not disentangle concepts strictly. therefore the concepts found could always encode watermark and shape feature at the same time. this effect is strongly visible in our benchmark

- question: how much is the result explained by the spurious feature?
- will be taken as the baseline. all other saliency based / local attribution methods can be benchmarked with this too
- does not take into account the splitting up into an relevance of single neurons
- but can in principle also be applied to each neuron/concept individually
- Find a way to measure how well a single heatmap can show the bias
- e.g.: watermark mask importance bilder mit wm general heatmap, total relevance inside mask for:
- A: attribution mit wm, wenn ellipse und conditioned on y:[1]
- B: attribution mit wm, wenn rect und conditioned on y:[0]
- C: attribution ohne wm, wenn ellipse und conditioned on y:[1]
- D: attribution ohne wm, wenn rect und conditioned on y:[0]
- (A - B) + (D - C)
- **LRP biasedness score sanity check:** This sanity test shows that while LRP assigns strong relevance to the watermark, it fails in correctly identifying the lack of a watermark as the main reason to predict for the negative class (rectangle). Superficially this confirms the criticism of missing negative relevance [29]. It is however not clear if the advantage of not cancelling out importances outweighs this factor for more complex data and applications.

irm class-
riance for
maps

4.6. Concepts Biasedness Measures

- should take into account that there are multiple concepts
- one could be important and not assign strong relevance to watermark
- the other could be unimportant and assign strong relevance to watermark
- *ground truth* idea is to again take the mean logit change for each single neuron or summed together somehow
- we want to be able to identify *spurious* concept and *core* concept automatically, so it is not a good idea to have the latent factors given
- one idea: take masked/bounding box approach again for neurons individual heatmaps
- nmf idea: somehow try to reduce the latent space to Watermark/Shape axis and measure variance in either direction

- centroids idea: use random DR algorithm and calculate ratio of centroid distances (needs latent factors again)
- causal idea??? somehow measure causal effect? - the other things are kind of causal or?

make sure to refer to results section too mu rather leave in out if it cannc explained wel without lookin at the results

5. Experimental Results

10-20 pages

- (1/3 of thesis)
- whatever you have done, you must comment it, compare it to other systems, evaluate it
- usually, adequate graphs help to show the benefits of your approach
- caution: each result/graph must be discussed! what's the reason for this peak or why have you observed this effect

5.1. Experiments

- what have I tried out with the different methods?
- list in concise order the possible measures
- ground-truth feature importance: mean logit change for output, R2-score, prediction flip
- baseline explanation feature importance - thats what we compare to e.g. watermark bounding-box importance for summary heatmap
- special concept explanations feature importance
- how are the experiments set up, how do i make sure they are all well comparable
- to which other baseline could my measures be compared to?

5.2. Results

lots of plots!

- what have I tried out with the different methods?
- what works and what doesn't
- plot for each experiment/possible method?
  - watermark bounding box average relevance for different subgroups, somehow get difference

  - variance of latent factors in relevance maximization image set - low variance means it encodes the concept
  - naive: total relevance for watermark image region
  - total activation + relevance of neuron given just watermark image
  - one idea: take masked/bounding box approach again for neurons individual heatmaps
  - nmf idea: somehow try to reduce the latent space to Watermark/Shape axis and measure variance in either direction
  - centroids idea: use random DR algorithm and calculate ratio of centroid distances (needs latent factors again)
  - causal idea??? somehow measure causal effect? - the other things are kind of causal or?

5.3. Evaluation

- evaluation of evaluation criteria:
  - takes into consideration the whole latent space spanned by the concepts
  - orients itself on known human cognition, user studies in this field would suggest this???
  - performs similar to baseline watermark bounding box importance?
  - ...?

ne success
eria of finding
od measure

- which measure is the best according to those criteria
- which measure is the closest to ground truth
- which is the furthest from ground truth
- does measure find *more information* than CRP itself and could possibly be used as a method on top of CRP for disentanglement/ spurious-core relation explanation?
-

5.4. Verification on Other Well-Known Benchmarks

uld i do
? which
chmarks, how
etup causal
del for them

1. Test method on more complex dataset e.g. CLEVR-XAI
2. compare CRP to other XAI methods?

5.5. Discussion

- do measures work
- what does causality help us with
- is CRP better for constant vector shift stuff or does it still suffer from it?
- can the application of those measures further explain/inform the explanation?
- what failed miserably

6. Conclusion

- (1 page)
- summarize again what your paper did, but now emphasize more the results, and comparisons.
- write conclusions that can be drawn from the results found and the discussion presented in the paper.
- future work (be very brief, explain what, but not much how)

1. which ground-truth feature importance measure is best
2. interesting points looking at model performances and explanation perforc-mance?
3. baseline vs. concept metric, which one is better for CRP
4. performance on other cases
5. how has causality helped in this?
6. Answer Question: *ARE WE EXPLAINING THE DATA OR THE MODEL*

answer questi

Limitations and Future Work

- max 1-2 pages, could also be included into the conclusion section

6. Conclusion

References

[1] ACHTIBAT, R., DREYER, M., EISENBRAUN, I., BOSSE, S., WIEGAND, T., SAMEK, W., AND LAPUSCHKIN, S. From "where" to "what": Towards human-understandable explanations through concept relevance propagation, 2022.

[2] ACHTIBAT, R., DREYER, M., EISENBRAUN, I., BOSSE, S., WIEGAND, T., SAMEK, W., AND LAPUSCHKIN, S. From attribution maps to human-understandable explanations through concept relevance propagation. *Nature Machine Intelligence 5*, 9 (jul 2023), 1006 – 1019.

[3] ADEBAYO, J., GILMER, J., MUELLY, M., GOODFELLOW, I., HARDT, M., AND KIM, B. Sanity checks for saliency maps. In *Advances in Neural Information Processing Systems* (2018), S. Bengio, H. Wallach, H. Larochelle, K. Grauman, N. Cesa-Bianchi, and R. Garnett, Eds., vol. 31, Curran Associates, Inc.

[4] ARRAS, L., OSMAN, A., AND SAMEK, W. Clevr-xai: A benchmark dataset for the ground truth evaluation of neural network explanations. *Information Fusion 81* (2022), 14–40.

[5] BACH, S., BINDER, A., MONTAVON, G., KLAUSCHEN, F., MÜLLER, K.-R., AND SAMEK, W. On pixel-wise explanations for non-linear classifier decisions by layer-wise relevance propagation. *PLOS ONE 10*, 7 (07 2015), 1–46.

[6] BAU, D., ZHOU, B., KHOSLA, A., OLIVA, A., AND TORRALBA, A. Network dissection: Quantifying interpretability of deep visual representations. In *Computer Vision and Pattern Recognition* (2017).

[7] BAU, D., ZHU, J.-Y., STROBELT, H., LAPEDRIZA, A., ZHOU, B., AND TORRALBA, A. Understanding the role of individual units in a deep neural network. *Proceedings of the National Academy of Sciences* (2020).

[8] CHATTOPADHYAY, A., MANUPRIYA, P., SARKAR, A., AND BALASUBRAMANIAN, V. N. Neural network attributions: A causal perspective. *ArXiv abs/1902.02302* (2019).

[9] CHORMAI, P., HERRMANN, J., MÜLLER, K.-R., AND MONTAVON, G. Disentangled explanations of neural network predictions by finding relevant subspaces.

[10] CLARK, B., WILMING, R., AND HAUFE, S. Xai-tris: Non-linear benchmarks to quantify ml explanation performance. *ArXiv* (2023).

[11] DREYER, M., PAHDE, F., ANDERS, C. J., SAMEK, W., AND LAPUSCHKIN, S. From hope to safety: Unlearning biases of deep models by enforcing the right reasons in latent space, 2023.

[12] GOYAL, Y., FEDER, A., SHALIT, U., AND KIM, B. Explaining Classifiers with Causal Concept Effect (CaCE). *ArXiv* (July 2019), arXiv:1907.07165.

[13] KARIMI, A.-H., MUANDET, K., KORNBLITH, S., SCHÖLKOPF, B., AND KIM, B. On the relationship between explanation and prediction: A causal view. In *Proceedings of the 40th International Conference on Machine Learning* (23–29 Jul 2023), A. Krause, E. Brunskill, K. Cho, B. Engelhardt, S. Sabato, and J. Scarlett, Eds., vol. 202 of *Proceedings of Machine Learning Research*, PMLR, pp. 15861–15883.

[14] KIM, B., WATTENBERG, M., GILMER, J., CAI, C., WEXLER, J., VIEGAS, F., AND SAYRES, R. Interpretability beyond feature attribution: Quantitative testing with concept activation vectors (TCAV). In *Proceedings of the 35th International Conference on Machine Learning* (10–15 Jul 2018), J. Dy and A. Krause, Eds., vol. 80 of *Proceedings of Machine Learning Research*, PMLR, pp. 2668–2677.

[15] KINDERMANS, P.-J., HOOKER, S., ADEBAYO, J., ALBER, M., SCHÜTT, K. T., DÄHNE, S., ERHAN, D., AND KIM, B. *The (Un)reliability of Saliency Methods*. Springer International Publishing, Cham, 2019, pp. 267–280.

[16] KOHLBRENNER, M., BAUER, A., NAKAJIMA, S., BINDER, A., SAMEK, W., AND LAPUSCHKIN, S. Towards best practice in explaining neural network decisions with lrp. In *2020 International Joint Conference on Neural Networks (IJCNN)* (2020), pp. 1–7.

[17] LEEMANN, T., KIRCHHOF, M., RONG, Y., KASNECI, E., AND KASNECI, G. When are post-hoc conceptual explanations identifiable? In *Proceedings of the Thirty-Ninth Conference on Uncertainty in Artificial Intelligence* (31 Jul–04 Aug 2023), R. J. Evans and I. Shpitser, Eds., vol. 216 of *Proceedings of Machine Learning Research*, PMLR, pp. 1207–1218.

[18] LEEMANN, T., RONG, Y., KRAFT, S., KASNECI, E., AND KASNECI, G. Coherence evaluation of visual concepts with objects and language. In *ICLR2022 Workshop on the Elements of Reasoning: Objects, Structure and Causality* (2022).

[19] MATTHEY, L., HIGGINS, I., HASSABIS, D., AND LERCHNER, A. dsprites: Disentanglement testing sprites dataset. https://github.com/deepmind/dsprites-dataset/, 2017.

[20] MONTAVON, G., BINDER, A., LAPUSCHKIN, S., SAMEK, W., AND MÜLLER, K.-R. *Layer-Wise Relevance Propagation: An Overview*. Springer International Publishing, Cham, 2019, pp. 193–209.

[21] MONTAVON, G., LAPUSCHKIN, S., BINDER, A., SAMEK, W., AND MÜLLER, K.-R. Explaining nonlinear classification decisions with deep taylor decomposition. *Pattern Recognition 65* (May 2017), 211–222.

[22] MORAFFAH, R., KARAMI, M., GUO, R., RAGLIN, A., AND LIU, H. Causal interpretability for machine learning - problems, methods and evaluation. *SIGKDD Explor. Newsl. 22*, 1 (may 2020), 18–33.

[23] NARENDRA, T., SANKARAN, A., VIJAYKEERTHY, D., AND MANI, S. Explaining deep learning models using causal inference. *ArXiv abs/1811.04376* (2018).

[24] PAHDE, F., DREYER, M., SAMEK, W., AND LAPUSCHKIN, S. Reveal to revise: An explainable ai life cycle for iterative bias correction of deep models, 2023.

[25] PARAFITA, A., AND VITRIA, J. Explaining visual models by causal attribution. In *2019 IEEE/CVF International Conference on Computer Vision Workshop (ICCVW)* (2019), pp. 4167–4175.

[26] SAMEK, W., MONTAVON, G., LAPUSCHKIN, S., ANDERS, C. J., AND MÜLLER, K.-R. Explaining deep neural networks and beyond: A review of methods and applications. *Proceedings of the IEEE 109*, 3 (2021), 247–278.

[27] SCHÖLKOPF, B., FOR INTELLIGENT SYSTEMS, M. P. I., MAX-PLANCK-RING, TÜBINGEN, ., AND GERMANY. Causality for machine learning. Tech. Rep. nature., 2019.

[28] SINGLA, S., AND FEIZI, S. Salient image net: How to discover spurious features in deep learning? In *ICLR* (2022).

[29] SIXT, L., GRANZ, M., AND LANDGRAF, T. When explanations lie: Why many modified bp attributions fail. In *Proceedings of the 37th International Conference on Machine Learning* (2020), ICML'20, JMLR.org.

[30] SIXT, L., AND LANDGRAF, T. A rigorous study of the deep taylor decomposition, 2022.

[31] SIXT, L., SCHUESSLER, M., POPESCU, O.-I., WEISS, P., AND LANDGRAF, T. Do users benefit from interpretable vision? a user study, baseline, and dataset, 2022.

[32] TRAN, T. Q., FUKUCHI, K., AKIMOTO, Y., AND SAKUMA, J. Unsupervised causal binary concepts discovery with vae for black-box model explanation. *Proceedings of the AAAI Conference on Artificial Intelligence 36*, 9 (Jun. 2022), 9614–9622.

[33] WILMING, R., KIESLICH, L., CLARK, B., AND HAUFE, S. Theoretical behavior of XAI methods in the presence of suppressor variables. In

Proceedings of the 40th International Conference on Machine Learning (23–29 Jul 2023), A. Krause, E. Brunskill, K. Cho, B. Engelhardt, S. Sabato, and J. Scarlett, Eds., vol. 202 of *Proceedings of Machine Learning Research*, PMLR, pp. 37091–37107.

[34] YEOM, S., SEEGERER, P., LAPUSCHKIN, S., WIEDEMANN, S., MÜLLER, K., AND SAMEK, W. Pruning by explaining: A novel criterion for deep neural network pruning. vol. abs/1912.08881.

A. Appendix

A.1. Additional Details to LRP rules and implementation best practices

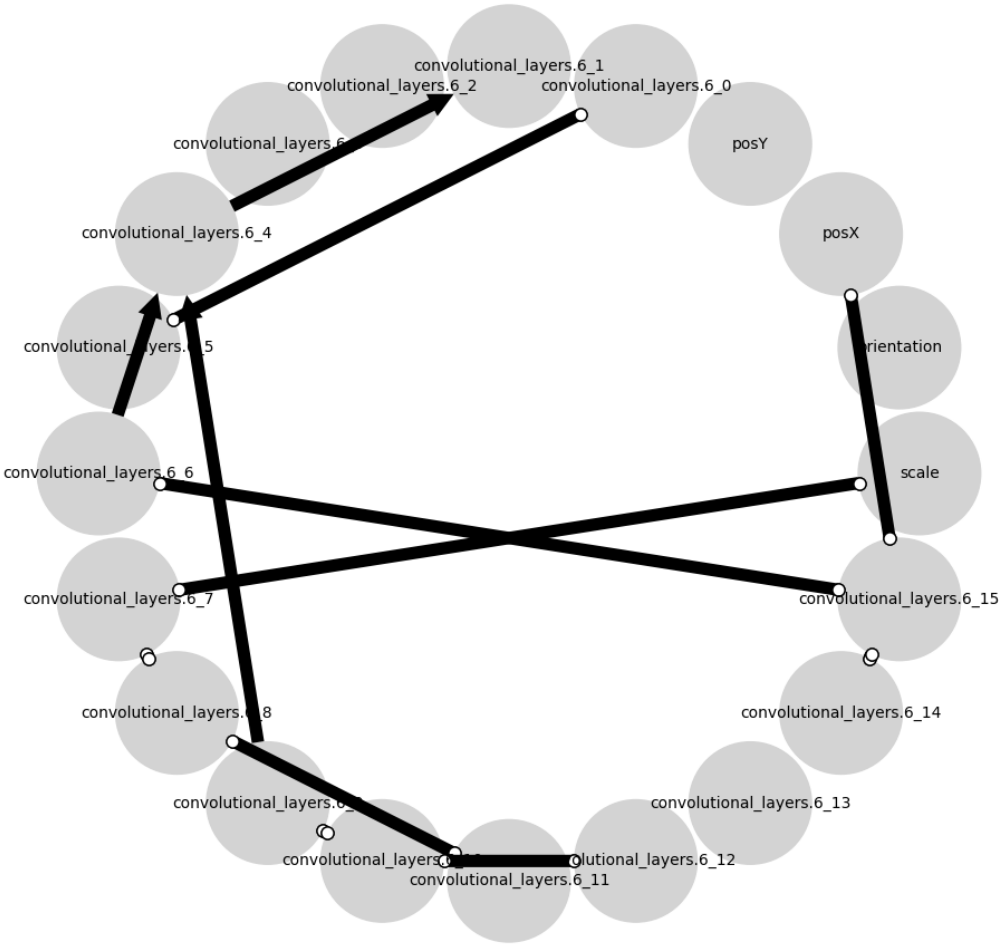

Figure A.1.: This is a test figure

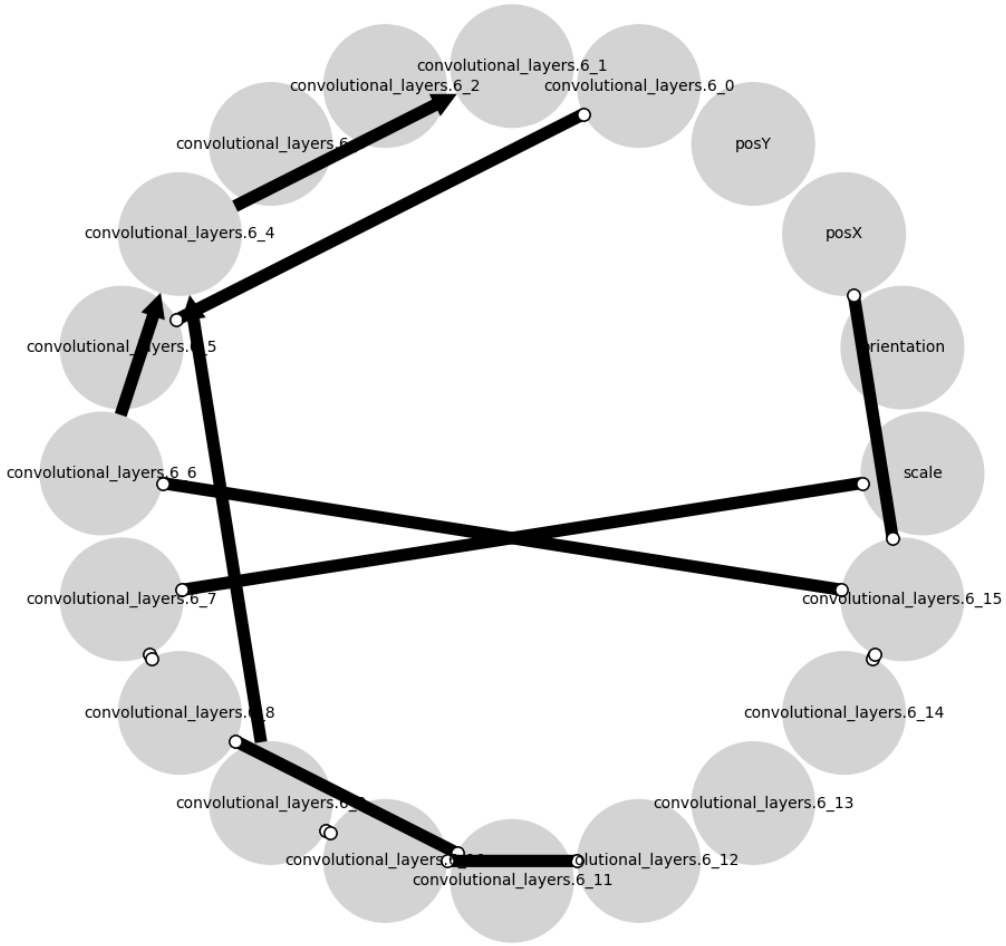

Figure A.2.: This is a test figure

A.2. Preliminary Experiments

A.2.1. Plots

A.2.2. Causal Discovery on Neural Network Models Idea and Implementation?

A.3. Details on Model Architecture?

```
self.convolutional_layers = nn.Sequential(
  nn.Conv2d(1, 8, kernel_size=3, stride=1, padding=0),
  nn.MaxPool2d(kernel_size=2, stride=2),
  nn.ReLU(),
  nn.Conv2d(8, 8, kernel_size=5, stride=1, padding=0),
  nn.MaxPool2d(kernel_size=2, stride=2),
  nn.ReLU(),
  nn.Conv2d(8, 8, kernel_size=7, stride=1, padding=0),
  nn.ReLU(),
)
self.linear_layers = nn.Sequential(
  nn.Linear(392, 6),
  nn.ReLU(),
  nn.Linear(6, 2),
)
```

A.4. Further Plots Groud Truth