Towards Human-Compatible XAI: Explaining Data Differentials with Concept Induction over Background Knowledge

Cara Widmer\textsuperscript{a}, Md Kamruzzaman Sarker\textsuperscript{b}, Srikanth Nadella\textsuperscript{c}, Joshua Fiechter\textsuperscript{a}, Ion Juvina\textsuperscript{a,d}, Brandon Minnery\textsuperscript{a}, Pascal Hitzler\textsuperscript{c}, Joshua Schwartz\textsuperscript{c}, Michael Raymer\textsuperscript{a,d}

\textsuperscript{a}Kairos Research, LLC
\textsuperscript{b}University of Hartford, USA
\textsuperscript{c}Kansas State University, USA
\textsuperscript{d}Wright State University

Abstract

Concept induction, which is based on formal logical reasoning over description logics, has been used in ontology engineering in order to create ontology (TBox) axioms from the base data (ABox) graph. In this paper, we show that it can also be used to explain data differentials, for example in the context of Explainable AI (XAI), and we show that it can in fact be done in a way that is meaningful to a human observer. Our approach utilizes a large class hierarchy, curated from the Wikipedia category hierarchy, as background knowledge.

Key words: concept induction, explainable AI, class hierarchy

1. Introduction

Lack of explainability and understandability are pervasive problems in modern artificial intelligence. Many modern machine learning (ML) methods in particular involve little to no human intervention once training data has been provided, and the resulting models are often “black boxes” whose internal representations and decision mechanisms remain opaque to human users \cite{11}. In order for human operators to be able to trust an ML algorithm’s outputs, make actionable decisions based on those outputs, and detect and correct biases, it is important that the algorithm’s reasoning processes be understandable. Thus there has been an increased focus on explainable artificial intelligence (XAI) in recent years \cite{3}.

Two major approaches for improving explainability are implementing transparency in the ML models themselves and inferring explanations via post-hoc techniques \cite{3}. For example, transparency can be directly introduced to ML models by incorporating simulatability (i.e., developing the model in such a way that the model can be simulated in the thoughts of a human analyzing the model output) \cite{50} or decomposability (i.e., enabling understandability of each part of the model individually) \cite{35}.

In contrast, post-hoc explainability techniques do not directly alter a model to make it more explainable but rather infer an explanation based on analysis of the model’s behaviors. Examples of post-hoc techniques include generating human-understandable text explanations and visualizations of a model’s behavior, as well as analyses that compute quantitative measures of the influence of various input variables on the model’s output. While post-hoc methods explain a model’s decisions indirectly, they avoid the performance trade-offs that often accompany attempts to engineer transparency directly into the model \cite{15}.

In the current work we implement a different post-hoc explainability strategy by applying concept induction \cite{30} to provide human-interpretable explanations of machine learning classifications. We demonstrate that concept induction, together with a suitable class hierarchy as background knowledge, can be used to generate explanations for data differences that are meaningful for a human observer. A class hierarchy consisting of a curated form of the Wikipedia category hierarchy \cite{46} was used as background ontology for concept induction, and the ECII concept induction system \cite{45} was used for explanation generation. We report on experiments that we have conducted with Amazon Mechanical Turk to assess how meaningful the generated explanations are for humans. The first experiment assesses the quality of explanations generated by concept induction in a specific setting related to scene classification, and supports our hypothesis that these explanations are judged by human participants to be more accurate than semi-random explanation, but less accurate than human-authored explanations. The second experiment shows that concept induction can be used to generate explanations for errors made by a ML classifier; the study also shows that these explanations are inferior to human-generated expla-

\textsuperscript{*}This research was, in part, funded by the U.S. Government via contract FA86492099045. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Government.

Email addresses: cara@kairosresearch.com (Cara Widmer), sarker@hartford.edu (Md Kamruzzaman Sarker), srikanth@kairosresearch.com (Srikanth Nadella), josh@kairosresearch.com (Joshua Fiechter), ion.juvina@wright.edu (Ion Juvina), brandon.minnery@wright.edu (Brandon Minnery), hitzler@ksu.edu (Pascal Hitzler), joshua.schwartz@wright.edu (Joshua Schwartz), michael.raymer@wright.edu (Michael Raymer)
nations.

Data and other resources for the work reported herein are available from [https://osf.io/zjkcw/](https://osf.io/zjkcw/).

The paper is structured as follows. In Section 2 we review the concept induction technique and discuss the background knowledge and data mapping process underlying our work. In Sections 3 and 4 we detail our two experiments. In Section 5 we present related efforts, and in Section 6 we discuss future work and conclude.

2. Concept Induction and Utilized Background Knowledge

Concept Induction [30] in its general form can be defined as follows. As background knowledge we assume that we have a given description logic ontology \( O \) with TBox \( T \) and ABox \( A \). We further assume that we are given two sets \( P \) and \( N \) each consisting of individuals from \( O \): \( P \) is called the set of positive examples and \( N \) is called the set of negative examples. The concept induction task then consists of identifying complex description logic expressions \( C \) such that \( O \models C(p) \) for all \( p \in P \) and \( O \not\models C(n) \) for all \( n \in N \). If no such \( C \) exists, then a concept induction system is expected to return approximate solutions, together with some accuracy value.

Generally speaking, concept induction is computationally very expensive. Known provably correct algorithms, such as the one underlying the well-known DL-Learner system [31], proceed by concept refinement, which is an adaptation from inductive logic programming [35]. A candidate concept expression \( C_0 \) is assessed as to whether \( O \models C(p) \) for all \( p \in P \) and \( O \not\models C(n) \) for all \( n \in N \) hold, and if not, then several candidate refinements of \( C_0 \), meaning concept expressions that are somewhat more or less general than \( C_0 \), are assessed, and the best of these becomes the new candidate concept expression \( C_1 \). This process is repeated until either a perfect solution is found or some termination criterion is met. Note that for each candidate concept, several calls to a description logic reasoner have to be made for assessment, and in particular with large sets \( P, S, A \) and a large expressive ontology \( O \), each of these reasoner calls can take considerable time.

In this paper, we are thus basing our analysis on a heuristic algorithm and system, called ECII (Efficient Concept Induction from Individuals) [45]. The heuristic underlying ECII rests primarily on (a) using only a class hierarchy as ontology, rather than a more complex ontology, (b) a limited search space for candidate concept expressions, and (c) a priori materialization of logical consequences. With ECII, it is possible to perform concept induction over data sets that cannot otherwise be dealt with, and experiments have shown that output accuracy is still rather high [45].

Previous uses of concept induction have been in the context of ontology engineering [29, 7, 20]. We have previously proposed concept induction for explainability, and preliminary studies have been published [47, 48]. In particular, [45, 46] presented preparatory methods that enabled the work we discuss in this paper: the ECII system [45], and our curated Wikipedia category hierarchy [46].

The latter was produced by first retrieving the complete category hierarchy from Wikipedia. Since it is crowdsourced, it actually contains cycles which, if interpreted as a proper class hierarchy (i.e., in the sense of rdfs:subClassOf), would make parts of it collapse. We thus devised an algorithm for breaking these cycles heuristically. The resulting class hierarchy consists of 1,860,342 concepts. In addition, 6,079,748 individuals – which correspond to Wikipedia page URLs – are assigned to the classes according to the categorizations found on Wikipedia.

Using the Wikipedia category hierarchy also enabled us to establish an easy mapping process of examples into the hierarchy: Text labels (more details about the dataset we used can be found in Sections 3 and 4) were mapped to DBpedia [32] entities using DBpedia Spotlight. These entities in turn usually correspond to Wikipedia pages, from which we can obtain the Wikipedia categories the page belongs to.

3. First Experiment: Assessing the Quality of Explanations Generated by Concept Induction

In this first experiment we aimed to assess the perceived quality of machine-generated explanations (i.e., ECII’s explanations) compared to both human-generated (“gold standard”) explanations and semi-random explanations. Explanations in this study consist of brief textual descriptions of the key conceptual differences between two sets of natural images corresponding to two distinct scene categories (A and B). Note that the two image sets notionally represent the decision outputs of a binary scene classification algorithm; however, for this experiment the classifier was merely hypothetical, since the purpose of the experiment was to assess the ability of ECII to explain data differentials per se. The study had been reviewed and approved by New England IRB (now part of WCG IRB; protocol #17-132535-1) and pre-registered before it was conducted.

3.1. Hypothesis

We hypothesize that human-generated explanations will be judged most accurate by participants, followed by ECII explanations, followed by semi-random explanations.

3.2. Method

3.2.1. Participants

300 participants were recruited through Amazon Mechanical Turk using the Cloud Research platform. Participants were recruited from a listing describing the task and the compensation

---

1 See [23] for background on description logics and their relation to ontologies, in particular the Web Ontology Language OWL [24].

2 There are different ways to assess accuracy, including precision, recall, and F1 scores.

3 See [https://www.dbpedia-spotlight.org/](https://www.dbpedia-spotlight.org/)

structure. Participants were compensated $5 through Mechanical Turk ($7.50 per hour prorated to the estimated time of 40 minutes required to complete the task). Based on an estimated medium effect size of $f^2 = 0.15$ and 95% power, we needed a sample size of at least 89 observations (i.e., unique participant judgments) per trial for estimating the parameters of the Bradley-Terry model [5] that was used to model the data. To reach this target we aimed to collect data from 300 participants, which equates to 100 total observations for each trial. This ensured we reached the required total and still allowed for potential exclusions.

3.2.2. Materials

Image sets. A total of 45 image set pairs (A and B) were created for this study. Images were taken from the ADE20K image dataset [53][54], which includes approximately 20,000 human-curated images with scene category and object tagging. The tags (annotations) do not only indicate presence of an object but also number of such objects, occlusions, etc., but we ignored these detailed annotations for our purposes and used only the object labels, which were mapped to the Wikipedia categories as described at the end of Section 2. Each image set pair included images from two scene categories (90 scene categories in total). Each set within a pair consisted of eight images selected at random from a particular category (e.g., eight images selected randomly from the Gazebo category).

Also included were five “catch trial” image sets that were used to verify that participants were paying adequate attention. The images for these trials were selected in the same manner as the target trial image sets but included a different type of explanation (described below).

Explanations. Explanations in this study were defined as lists of up to seven concepts (i.e., strings corresponding to Wikipedia category names) that aimed to describe what was present in category A that was not present in category B (where categories A and B are the two distinct scene categories included in the image set). Concepts could be anything physically present in the images (like a computer or window), or an abstract category that fits the theme of the images (like science or entertainment).

Three types of explanations were created for each of the 45 target image sets: 1) ECII machine-generated explanations, 2) human “gold standard” explanations, and 3) semi-random machine-generated explanations.

ECII explanations were created by providing the image sets’ object tags (but not scene category tags) to the ECII algorithm. The algorithm then assessed the images and returned a rating of how well concepts matched images in category A but not category B. ECII explanations were then created by taking the seven highest rated unique concepts. ECII provides several different methods of ranking explanations. Explanations were created using rankings based on F1 scores, recall scores, precision scores, and a hybrid score. Pilot testing revealed that explanations created using F1 scores were seen as most accurate by participants, and so F1-based ECII explanations were selected for use.

Human “gold standard” explanations were created by providing the image sets (but not the object tags or scene category tags) to three human raters. Each rater independently assessed each image set and generated a list of 7 to 10 concepts that (on average) matched the images in category A but not category B. Once all raters had completed this task, gold standard explanations were created by first selecting any concept mentioned by all three raters, then concepts mentioned by two of the raters, and then finally filling the explanation with concepts randomly selected from the remaining concepts across the three raters until seven unique concepts were obtained.

Semi-random explanations were created by randomly shuffling the images in each image set to create new groupings of category A and category B that were not based on the scene category but instead contained a mixture of images from both categories. These new image sets were then provided to ECII, and explanations were generated in the same method as described above. The logic of this approach is that these explanations were likely to be viewed as more plausible than completely random explanations since they would still include concepts that are present in the images participants saw, but they would not (on average) align with one group over the other. Thus, semi-random explanations (hereafter referred to as “random” explanations) constitute a more reasonable baseline against which to assess ECII’s performance than fully random explanations, because the latter could be easily outperformed by even a low-quality explanation engine.

Catch trials included their own set of two types of explanations. One set were human explanations which were generated in the same way as the other human gold standard explanations. The other set of explanations for catch trials consisted of completely random concepts taken from a random word generator. This resulted in explanations that were very obviously inaccurate, allowing these trials to serve as an assessment of how well participants were paying attention to the task.

To standardize the presentation of explanations, all concepts in an explanation were presented in alphabetical order.

3.2.3. Design

Experiment 1 employed a within-subjects design in which each participant was presented with two explanations per trial and asked to choose the more accurate explanation (two-alternative forced choice design). Each participant saw all three explanation types across all trials, although only two explanation types were compared in any one trial. For each pair of image sets (A and B), the participant completed three trials comparing (1) the ECII versus human explanation; (2) the ECII versus semi-random explanation; and (3) the human versus semi-random explanation. For any given pair of image sets, a given participant completed all three comparisons (i.e., a within-subjects design).

The 45 total pairs of image sets in this study led to a total of 135 unique target trials. Because this was greater than the number of trials an individual participant was likely to be able to complete, participants were randomly assigned to 15 image sets (a total of
45 trials). Image sets were counterbalanced across participants such that all image sets received the same number of responses.

3.2.4. Procedure

After providing consent, participants completed brief training on the task, including instructions about how concepts and explanations were defined in this study. Participants then began completing trials. The 50 trials (45 assigned targets and 5 catch trials) were presented in a random order. Figure 1 shows what the stimuli presentation and response options looked like to participants.

3.3. Results

Prior to analysis, participant responses to the catch trials were assessed. Participants who failed more than one catch trial were excluded from analysis. While the vast majority of participants did not fail any catch trials (N=295) and one participant failed exactly one trial, four participants failed more (two failed two trials, and two failed three trials). These four participants were excluded from all analyses, leaving a total of 296 participants included in analyses. Across all image sets, human explanations were overwhelmingly chosen over ECII explanations (3856 vs 580; i.e., 87% of the time) and over random explanations (4287 vs 153; i.e., 97% of the time), and ECII explanations were chosen overwhelmingly over random explanations (3862 vs 578; i.e., 87% of the time). See Figure 2.

Participants’ pairwise judgments were used in a Bradley-Terry analysis to obtain “ability scores” for each type of explanation, where ability scores in this analysis provide a metric of how much an explanation type was preferred by participants. Ability scores were calculated for each of the 45 image sets. Analysis of these ability scores revealed that human explanations had the highest ability scores (M = 5.32, SD = 3.87), followed by ECII explanations (M = 3.08, SD = 3.99), F(2) = 30.37, p < 0.001, η² = 0.315). Random explanations were used as the comparison point in the Bradley-Terry analysis, and thus were set to 0 (with the ability scores for human and ECII explanations indicating how much they were preferred compared to the random explanations). A Tukey’s HSD test revealed that differences in the ability scores of human vs. random explanations and ECII vs. random explanations were both significant at p < 0.001, while differences in the ability scores of human vs. ECII explanations were significant at p = 0.004. See Table 1 for the individual human and ECII ability scores for each image set pair in Experiment 1.

3.4. Discussion

Analysis of the results of Experiment 1 provide evidence to support our main hypothesis. Participants found the human-generated explanations to be the most accurate at describing the difference in the image sets, followed by the ECII explanations, and the semi-random explanations proving to be the least accurate. This provides support for the value of ECII explanations. It is not surprising that explanations produced by the ECII algorithm are of lower quality than human-generated explanations at this stage of development. However, the ECII explanations do contain notable explanatory power, suggesting that ECII explanations can be useful. It should be noted also that there was some variability in ECII’s performance across the image sets. For some image sets the ECII explanations were chosen relatively more often than in others, in one case even being chosen more frequently than the human explanation, while in other image sets it was chosen less often than the random explanation. This suggests there is certainly still room for improvement in ECII explanations, but that on average there is promising evidence that ECII can produce explanations that accurately describe the differences between two groups of data.

4. Second Experiment: Identifying Errors Made by a Machine Learning Classifier

In Experiment 1 the quality of ECII-generated explanations was (subjectively) judged by human participants via comparison with human-generated (“gold standard”) and random-generated explanations. Our second experiment (Experiment 2) sought to obtain an objective measure of the utility of ECII’s explanations in helping human users evaluate the decisions of an actual ML system (more precisely, a logistic regression algorithm that classified images into scene categories based on semantic tags of objects present in each image). Specifically, the goal of this second experiment was to test how well ECII explanations (compared to human “gold standard” explanations) helped human participants identify the errors made by the AI. Note that a key difference between this experiment and Experiment 1 is that the explanations in Experiment 1 were of a (hypothetical) ML’s decisions, whereas the explanations in Experiment 2 were of a (real) ML’s decision errors. The study had been reviewed and approved by New England IRB (now part of WCG IRB; protocol #17-1325335-1) and pre-registered before it was conducted.

4.1. Hypothesis

We hypothesized that participants would be able to match human generated explanations to the correct image set more frequently than for ECII explanations, and that participants would be better than chance for both types of explanations.

4.2. Method

4.2.1. Participants

Amazon Mechanical Turk participants were recruited using the Cloud Research platform. Participants were recruited from a listing on Mechanical Turk describing the task and the compensation structure. Participants were compensated $5 through Mechanical Turk ($7.50 per hour prorated to the estimated time of 40 minutes required to complete the task). Following recommendations by [44], we initially planned to collect data from 100 participants and compute Bayes Factors for our effects of interest. If the Bayes Factors was not conclusive, then we would continue to collect data in groups of 50 participants, stopping to

---

5See https://aspredicted.org/blind.php?x=4FH_1X4 for complete study preregistration information.
<table>
<thead>
<tr>
<th>Image Set</th>
<th>H. Ability</th>
<th>E. Ability</th>
<th>H. v E. Wins</th>
<th>H. v R Wins</th>
<th>E. v R Wins</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set 1: Bedroom v Park</td>
<td>4.58</td>
<td>2.04</td>
<td>90 – 6</td>
<td>94 – 2</td>
<td>86 – 10</td>
</tr>
<tr>
<td>Set 2: Living Room v Parking Lot</td>
<td>7.40</td>
<td>3.91</td>
<td>97 – 2</td>
<td>98 – 1</td>
<td>98 – 1</td>
</tr>
<tr>
<td>Set 3: Office v Playground</td>
<td>6.09</td>
<td>4.80</td>
<td>76 – 20</td>
<td>95 – 1</td>
<td>96 – 0</td>
</tr>
<tr>
<td>Set 4: Airport v Amusement Park</td>
<td>2.60</td>
<td>0.09</td>
<td>93 – 4</td>
<td>87 – 10</td>
<td>54 – 43</td>
</tr>
<tr>
<td>Set 5: Bathroom v Art Studio</td>
<td>5.10</td>
<td>3.66</td>
<td>78 – 18</td>
<td>95 – 1</td>
<td>94 – 2</td>
</tr>
<tr>
<td>Set 6: Beauty Salon v Forest Path</td>
<td>4.25</td>
<td>3.60</td>
<td>65 – 33</td>
<td>96 – 2</td>
<td>96 – 2</td>
</tr>
<tr>
<td>Set 7: Bookstore v Child Room</td>
<td>5.42</td>
<td>2.80</td>
<td>91 – 6</td>
<td>96 – 1</td>
<td>92 – 5</td>
</tr>
<tr>
<td>Set 8: Hotel Room v Cockpit</td>
<td>5.35</td>
<td>4.17</td>
<td>78 – 22</td>
<td>98 – 2</td>
<td>100 – 0</td>
</tr>
<tr>
<td>Set 9: Shoe Store v Alcove</td>
<td>4.12</td>
<td>3.09</td>
<td>75 – 26</td>
<td>99 – 2</td>
<td>97 – 4</td>
</tr>
<tr>
<td>Set 10: Alley v Wet Bar</td>
<td>4.94</td>
<td>1.19</td>
<td>98 – 2</td>
<td>99 – 1</td>
<td>77 – 23</td>
</tr>
<tr>
<td>Set 11: Closet v Construction Site</td>
<td>7.76</td>
<td>4.61</td>
<td>93 – 4</td>
<td>97 – 0</td>
<td>96 – 1</td>
</tr>
<tr>
<td>Set 12: Gazebo v Bowling Alley</td>
<td>5.31</td>
<td>2.49</td>
<td>93 – 5</td>
<td>97 – 1</td>
<td>91 – 7</td>
</tr>
<tr>
<td>Set 13: Garage v Hallway</td>
<td>28.74</td>
<td>27.86</td>
<td>70 – 29</td>
<td>99 – 0</td>
<td>99 – 0</td>
</tr>
<tr>
<td>Set 14: Laundromat v Pantry</td>
<td>6.77</td>
<td>3.54</td>
<td>98 – 4</td>
<td>102 – 0</td>
<td>99 – 3</td>
</tr>
<tr>
<td>Set 15: Conference Room v Waterfall</td>
<td>6.97</td>
<td>3.49</td>
<td>95 – 3</td>
<td>98 – 0</td>
<td>95 – 3</td>
</tr>
<tr>
<td>Set 16: Home Office v Bow Window</td>
<td>4.29</td>
<td>1.93</td>
<td>93 – 7</td>
<td>97 – 3</td>
<td>89 – 11</td>
</tr>
<tr>
<td>Set 17: Dining Room v Kitchen</td>
<td>1.77</td>
<td>1.64</td>
<td>54 – 44</td>
<td>81 – 16</td>
<td>83 – 14</td>
</tr>
<tr>
<td>Set 18: Fast Food v Office Building</td>
<td>4.09</td>
<td>1.26</td>
<td>91 – 6</td>
<td>96 – 1</td>
<td>75 – 22</td>
</tr>
<tr>
<td>Set 19: Jacuzzi v Greenhouse</td>
<td>5.83</td>
<td>2.24</td>
<td>98 – 3</td>
<td>101 – 0</td>
<td>91 – 10</td>
</tr>
<tr>
<td>Set 20: Gymnasium v Corridor</td>
<td>3.23</td>
<td>-0.12</td>
<td>93 – 4</td>
<td>94 – 3</td>
<td>45 – 52</td>
</tr>
<tr>
<td>Set 21: Bus v Broadleaf Forest</td>
<td>6.75</td>
<td>3.22</td>
<td>99 – 2</td>
<td>100 – 1</td>
<td>98 – 3</td>
</tr>
<tr>
<td>Set 22: Casino v Arrival Gate</td>
<td>6.17</td>
<td>3.55</td>
<td>95 – 5</td>
<td>98 – 2</td>
<td>99 – 1</td>
</tr>
<tr>
<td>Set 23: Library v Gas Station</td>
<td>4.61</td>
<td>3.40</td>
<td>77 – 23</td>
<td>94 – 1</td>
<td>92 – 3</td>
</tr>
<tr>
<td>Set 24: Valley v Yard</td>
<td>3.74</td>
<td>-1.17</td>
<td>98 – 0</td>
<td>95 – 3</td>
<td>24 – 74</td>
</tr>
<tr>
<td>Set 25: Mountain v Coast</td>
<td>0.64</td>
<td>0.32</td>
<td>58 – 40</td>
<td>63 – 35</td>
<td>58 – 40</td>
</tr>
<tr>
<td>Set 26: Dinette Vehicle v Farm Field</td>
<td>4.81</td>
<td>2.92</td>
<td>90 – 11</td>
<td>98 – 3</td>
<td>98 – 3</td>
</tr>
<tr>
<td>Set 27: Poolroom v Driveway</td>
<td>1.61</td>
<td>2.78</td>
<td>23 – 75</td>
<td>82 – 16</td>
<td>92 – 6</td>
</tr>
<tr>
<td>Set 28: Bridge v Auditorium</td>
<td>5.15</td>
<td>3.04</td>
<td>87 – 10</td>
<td>96 – 1</td>
<td>94 – 3</td>
</tr>
<tr>
<td>Set 29: Museum v Youth Hostel</td>
<td>1.85</td>
<td>-0.10</td>
<td>89 – 11</td>
<td>85 – 15</td>
<td>49 – 51</td>
</tr>
<tr>
<td>Set 30: Supermarket v Restaurant</td>
<td>6.16</td>
<td>3.97</td>
<td>88 – 9</td>
<td>96 – 1</td>
<td>96 – 1</td>
</tr>
<tr>
<td>Set 31: Classroom v Archive</td>
<td>3.97</td>
<td>2.27</td>
<td>84 – 14</td>
<td>95 – 3</td>
<td>90 – 8</td>
</tr>
<tr>
<td>Set 32: Dentist Office v Ballroom</td>
<td>3.79</td>
<td>1.25</td>
<td>88 – 6</td>
<td>95 – 3</td>
<td>77 – 21</td>
</tr>
<tr>
<td>Set 33: Lighthouse v River</td>
<td>4.51</td>
<td>2.08</td>
<td>91 – 7</td>
<td>97 – 1</td>
<td>88 – 10</td>
</tr>
<tr>
<td>Set 34: Creek v Basement</td>
<td>6.87</td>
<td>2.94</td>
<td>97 – 1</td>
<td>97 – 1</td>
<td>94 – 4</td>
</tr>
<tr>
<td>Set 35: Building Facade v Ocean</td>
<td>4.32</td>
<td>2.00</td>
<td>90 – 8</td>
<td>96 – 2</td>
<td>87 – 11</td>
</tr>
<tr>
<td>Set 36: Courthouse v Parking Garage</td>
<td>2.28</td>
<td>-0.45</td>
<td>90 – 8</td>
<td>91 – 7</td>
<td>36 – 62</td>
</tr>
<tr>
<td>Set 37: Balcony v Skyscraper</td>
<td>5.39</td>
<td>2.69</td>
<td>96 – 7</td>
<td>103 – 0</td>
<td>96 – 7</td>
</tr>
<tr>
<td>Set 38: Game Room v Waiting Room</td>
<td>4.70</td>
<td>3.83</td>
<td>69 – 30</td>
<td>99 – 0</td>
<td>96 – 3</td>
</tr>
<tr>
<td>Set 39: Landing Deck v Window Seat</td>
<td>4.82</td>
<td>2.28</td>
<td>93 – 6</td>
<td>97 – 2</td>
<td>91 – 8</td>
</tr>
<tr>
<td>Set 40: Bar v Warehouse</td>
<td>4.81</td>
<td>2.87</td>
<td>86 – 11</td>
<td>95 – 2</td>
<td>93 – 4</td>
</tr>
<tr>
<td>Set 41: Bakery v Apartment Building</td>
<td>5.41</td>
<td>3.64</td>
<td>86 – 14</td>
<td>99 – 1</td>
<td>98 – 2</td>
</tr>
<tr>
<td>Set 42: Needleleaf Forest v Playroom</td>
<td>7.03</td>
<td>4.70</td>
<td>92 – 9</td>
<td>101 – 0</td>
<td>100 – 1</td>
</tr>
<tr>
<td>Set 43: Outdoor Window v Roundabout</td>
<td>4.58</td>
<td>1.10</td>
<td>98 – 2</td>
<td>98 – 2</td>
<td>76 – 24</td>
</tr>
<tr>
<td>Set 44: Reception v Golf Course</td>
<td>4.03</td>
<td>1.73</td>
<td>94 – 7</td>
<td>97 – 4</td>
<td>88 – 13</td>
</tr>
<tr>
<td>Set 45: Staircase v Plaza</td>
<td>6.46</td>
<td>4.78</td>
<td>85 – 16</td>
<td>101 – 0</td>
<td>100 – 1</td>
</tr>
</tbody>
</table>

Table 1: Ability Scores and Number of Wins for Human (H.), ECII (E.), and Random (R.) Explanations. Note that random explanations were set as the reference point in the Bradley-Terry analysis and so their ability scores were always equal to 0, and thus are not displayed here.
analyze the data after each new cohort, ceasing data collection if we reached a sample size of 250. We did not need to collect more than the initial 100 responses.

4.2.2. Materials

Image sets. A total of 16 image sets were created for this study. Images were taken from the Google Open Images database, which includes object tagging and scene category tags. The annotated tags in these images are crowd-generated and thus noisy. Limited manual curation was therefore performed as part of the image selection process: for example, images with very few object tags (5 or fewer) were removed from the dataset, as images with too few labels would not provide the classifier with enough context to make a classification. Each training set included images from both the target category and images from multiple non-target categories. All images from the target category with sufficient object tags were included. An equal number of images were drawn randomly from non-target categories to provide a balanced dataset for each image set. We utilized the following 16 scene categories: bakeries, bathrooms, bedrooms, bridges, cafes, classrooms, dining rooms, gazebos, greenhouses, kitchens, lobbies, offices, pantries, parks, parking lots, and libraries.

Selected images were fed to a logistic regression classifier to classify scene images into target / non-target categories based on their tags. We utilized 10-fold cross validation to train and test the classifier. The input stimuli were represented as binary object vectors indicating the presence or absence of each object tag in that image. The vector space was generated by taking a set of all the objects present in the image dataset for a target scene category (e.g., all object tags present in the kitchen vs. non-kitchen image set). The classifier then outputs a binary decision as to whether each image is part of the target set or not. These classifications were then grouped into four categories based on ground truth scene categories: true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN). Up to nine images from each grouping were included in final image sets displayed to participants, randomly selected from the full set of images in each error group. The same five catch trial image sets from Experiment 1 were also included in Experiment 2.
Explanations. Explanation generation in Experiment 2 followed the same process as in Experiment 1, with the exception that only two types of explanations were used for Experiment 2: 1) ECII (machine-generated) explanations and 2) human “gold standard” explanations. Due to the particular design of the study, the semi-random explanations would not have provided additional information and therefore were not used.

ECII explanations were again created by providing the image set’s object tags (but not scene category tags) to the ECII algorithm, which provided ratings of concepts in the same manner as in Experiment 1. Object tags from all images in a set were provided to ECII, not only those in the subset of images displayed to participants. Explanations were generated for four image sets for each scene category: FP vs TN, TP vs FN, TP vs FP, and FN vs TN. These four comparisons were chosen because they were deemed most likely to have explainable differences. For example, we reasoned that FP scenes might contain a restricted set of defining elements that distinguish them from TN scenes — e.g., FP kitchen images might be more likely to contain kitchen-relevant features that TN kitchens do not have, such as images of offices that contain microwave ovens). In contrast, FP scenes could contain a wide variety of elements that distinguish them from TP scenes (e.g., a FP kitchen could contain an oven in a warehouse filled with myriad other objects) or from FN scenes (e.g., a FP kitchen and FN kitchen could both contain a large set of kitchen-irrelevant features that are hard to capture concisely).

Explanations in Experiment 1 tended to be more abstract, featuring thematic or high-level category concepts, unlike the very concrete explanations created by human raters, which tended to feature specific objects in the image sets. In order to equate the concreteness of the ECII and human explanations in Experiment 2, we conducted an analysis of the concreteness of the terms used in human explanations (described below), using concreteness ratings provided by [5]. We assessed the concreteness of each concept provided by human raters and in the ECII explanations and confirmed that ECII concepts were noticeably more concrete than the concepts provided by all three human raters. In order to adjust the concreteness of ECII explanations, we eliminated all concepts provided by ECII with a concreteness score of less than 3.5 (See Figure 3 for an example of the concreteness of ECII explanations before and after adjustment, compared to the concreteness of the concepts provided by the three human raters). Explanations were then created by taking the seven highest rated concepts from the filtered set returned by ECII.

Explanations generated by ECII can be ranked with respect to several criteria; to determine which criteria would be most helpful for human participants, we ran a pilot study in which we compared the effectiveness of explanations maximized with respect to F1, precision, and recall. Discriminability from this pilot study is plotted in Figure 4. Overall, we found that all three explanation types generated similar discriminability for our “TP vs. FP” and “TP vs. TN” comparisons, and that explanations maximized with respect to F1 and precision yielded similar discriminability for the remaining two comparisons. However, only F1 generated higher discriminability than recall-based explanations for the “FN vs. TN” comparison, whereas precision discriminability was not convincingly better than that of recall (i.e., BF < 3). We therefore elected to use explanations that were generated with respect to F1 scores in Experiment 2.

Human “gold standard” explanations were again created by providing the image sets (but not object tags or scene category tags) to three human raters. Raters again independently generated concepts for the same four comparisons for each scene category that ECII did. Gold standard explanations were created by pooling the concepts humans provided following the same procedure as in Experiment 1.

Catch trials utilized the same explanations as in Experiment 1, although the randomly generated explanations were not included due to the design of Experiment 2.

Because participants did not need to compare two different explanations in Experiment 2, concepts were not presented in alphabetical order, unlike in Experiment 1.

4.2.3. Design
Experiment 2 utilized a fully crossed within-subjects design with 2 (explanation type: ECII, human) × 4 (comparison sets: FP vs TN, TP vs FN, TP vs FP, FN vs TN) conditions for a total of 8 conditions. Participants were randomly assigned to 8 (out of 16) scene categories. For each scene category, partici-
pants saw all four comparisons. For half of the categories, they saw the human explanations, and for the other half they saw the ECII explanation. This resulted in a total of 32 target trials for each participant (4 in each explanation type × comparison set condition).

4.2.4. Procedure
After providing consent, participants completed brief training on the task, including instructions about how concepts and explanations were defined in this study. Participants then began completing trials. The 37 trials (32 assigned targets and 5 catch trials) were presented in a random order. Figure 5 shows what the stimuli presentation and response options looked like to participants.

4.3. Results
We analyzed choice data from Experiment 2 with a Bayesian hierarchical signal-detection model (SDT; [21]). In its simplest form, SDT parameterizes binary choices as a function of discriminability (i.e., \(d\)) and bias (i.e., \(c\)). Discriminability is the distance between a posited mental Gaussian distribution of noise and a Gaussian distribution of signal. Bias is the degree to which an individual’s decision threshold varies from ideal placement (i.e., the point at which the signal and noise distributions are equally likely); negative or positive bias indicates a tendency to respond with one choice over another. This separation of discriminability from bias ensures that individuals are not misjudged as accurate when they generate one response more often than the other (e.g., consider a student who achieves 50% accuracy on a balanced true-false exam by always responding “true”).

Our SDT model was estimated in Stan probabilistic language [9] via the “brms” package [8] in R statistical software. We estimated population-level coefficients for discriminability and bias for each comparison and explanation type (i.e., ECII versus humans), as well as participant- and scene-level effects for discriminability and bias. Population-level coefficients were assessed with Bayes factors, which were estimated via Savage-Dickey ratios [32]. Following recommendations from [25], we considered evidence as convincing once it supported one hypothesis over another by a 3:1 ratio.

Because our analyses were rooted in Bayesian estimation, we took advantage of optional stopping during data collection [44]. Our primary interest was in evaluating whether (a) human- and ECII-generated explanations facilitated set discrimination to different degrees and (b) whether human- and ECII-generated explanations yielded non-zero discriminability. We therefore elected to initially collect data from 100 individuals, and then collect data in cohorts of 50 participants either until we (a) found convincing evidence in favor of either the null or alternative hypothesis (i.e., a Bayes factor either \(\geq 3\) or \(\leq 0.33\)) or else (b) collected data from 250 people total. We ultimately stopped data collection after 100 participants.

Estimates of participants’ discriminability are plotted in Figure 6. Population-level estimates of discriminability and bias as a function of explanation type are reported in Table 2. Differential values between humans and ECII are reported in Table 3. Human-generated explanations yielded higher discriminability for all four of our comparisons. For both human-generated and ECII-generated explanations, we found evidence for non-zero \(d\). Thus, while ECII is not as effective as humans at generating helpful descriptions of set differences, it is nonetheless still an effective intervention across all comparisons that we evaluated. Additionally, both sets of explanations yielded a bias toward responding with “Set A” (but note that correct responses were balanced across “Set A” and “Set B”), and this bias was consistently stronger for human-generated explanations.

4.4. Discussion
Experiment 2 suggests that ECII can generate sensible explanations that help humans to distinguish misclassified scenes from correctly classified ones. Explanations generated by humans were even more helpful, which is not entirely unexpected, but our findings nonetheless suggest that ECII may be deployed to effectively facilitate human analysts’ error detection for AI classification. Another notable result from Experiment 2 is that human explanations generated more biased responding in addition to more discriminative responses; while we did not anticipate such an outcome, one plausible explanation is that participants were randomly responding more frequently when viewing
Figure 5: Experiment 2 task interface, with ECII explanation referring to image group B.

Figure 6: Discriminability as a function of comparison (noted on the abscissa) and explanation type (noted in the panel titles) for Experiment 2. Violins indicate the distribution of participants’ $d'$ values. Black dots indicate group means. Note the different scales in the ordinates.

ECII explanations (i.e., because ECII was not as interpretable, despite our attempts to increase the concreteness of its terms), whereas human explanations encouraged more systematic (if also biased) responding. Overall, our findings suggest that ECII could serve as an effective teammate for facilitating human analysts’ detection of misclassified entities.

One question that we have not addressed directly in Experiment 2 is how humans detect misclassified sets. For example, did participants notice that the error images include/exclude certain objects that the correct images do/do not contain? Future research on this topic could employ eye-tracking methods to evaluate which particular scenes, or specific features thereof, people tend to assess prior to making their choices.

5. Related Work

Despite significant recent research efforts regarding approaches to XAI, this area of research is still in its infancy and in need of new ideas. Explanation methods so far can be divided into two broad categories, one focusing on local explanations, and one focusing on global explanations. Local explanation algorithms seek understanding of individual predictions, while global explanation algorithms seek understanding of the overall behavior of the deep learning model.

Local explanation approaches can in turn be divided into 4 broad categories, a) those focusing on feature importance, b) those using saliency maps, c) those that are prototypes or examples based, and d) those based on counterfactuals. As the name suggests, feature importance algorithms attempt to identify which input features are more important for the prediction. Popular feature importance algorithms are LIME [43] and SHAP [34]. State-of-the-art saliency map based algorithms are [48] [38]. Prototype/example based algorithms seek to explain
individual decisions in terms of other examples (whether artificial or based on real data). Popular algorithms in this category make use of so-called influence functions [23], and a corresponding survey on this can be found in [37]. A popular counterfactuals based algorithm was provided in [20], and an overview of counterfactual explanations can be found in [51].

Global explanation approaches can be categorized into 3 broad categories, a) those that are based on collections of local explanations like SP-LIME [43], b) those that are representation based like TCAV [26], and c) those based on model distillation like [49] [16]. State of the art algorithms have issues regarding faithfulness [1], stability [2, 4] and fragility [27, 19].

The use of background or domain knowledge to produce or enhance explanations is gaining attention very recently. Domain knowledge comes in the form of simple concept tags, knowledge graphs (essentially data organized in graphs) or ontologies (knowledge bases using formal logic with formal semantics). For the use of concepts, one of the pioneering contributions was by Been Kim et. al. who showed the value of simple concepts to produce human understandable explanations [25]. Knowledge graph were used, for example, to explain individual decisions in the context of stock trend predictions [14]. Ontologies have been used in several lines of research for explanation. In the transfer learning domain, they were used to obtain an understanding which features are worth transferring or not [18]. The publication [39] introduced Doctor XAI as a model-agnostic explainer that focuses on explaining medical diagnosis predictions. They show how exploiting temporal dimensions in the data together with domain knowledge encoded as a medical ontology improves the quality of mined explanations. Trepan-reloaded [12] is an extension of the original Trepan [13] algorithm, and the authors demonstrate the use of ontologies for producing explanations that are more understandable by humans. Though, as we have just seen, there exists XAI research that makes use of domain knowledge, concept induction for making use of background knowledge is not yet a prevalent method. We are only aware of our own preliminary investigations [47] and [42] that make use of concept induction.

Among the many approaches to XAI, some explanations are generated for end users, and some explanations are meant for system developers, but in any case it remains an important criterion that an explanation makes sense to a human. To evaluate which explanations are better than others in this respect, different methods are being proposed [41] [17] [10] [24]. And while the different approaches are being evaluated, it is also important to keep in mind the variability of human understanding [36].

6. Conclusions and Future Work

The results reported herein clearly indicate that concept induction is an approach to explanation generation over background knowledge that produces explanations that are meaningful at a human level. But of course, the studies presented herein are only first steps on a longer journey towards making the approach useful in practice. We discuss several lines of investigation that can follow up on the presented results.

It appears a reasonable hypothesis that more expressive background knowledge – e.g. a highly axiomatized ontology – could yield even better and more fine-grained explanations. In fact, explanations could even include individuals in the form of nominal classes, i.e. reasoning would be over the schema (ontology) and a corresponding knowledge graph to derive explanations. A key technical hurdle remains for this, though: While ECII scales to the task, its heuristic relies on an ontology that is merely a class hierarchy, and other algorithms like those underlying DL-Learner do not scale sufficiently. Improved algorithms and systems – heuristic or not – for concept induction therefore need developing, before expressive background knowledge can be used at scale.

Another rather obvious avenue is in exploring concept induction for explanation generation in other settings, and in particular for deep learning systems that are inherently black boxes. One the one hand, an analysis of type 1 and type 2 errors by a trained network could lead to the identification of commonalities of inputs that produce errors, which could then be corrected, e.g., by including more training samples of the error-producing type. Another possible line of research is the use of concept induction to explain hidden layer activation patterns.

While concept induction is the key mechanism underlying our study, it appears to us that the choice of background knowledge is probably rather critical. Indeed, we also experimented with other hierarchies, e.g., SUMO [46], but the results were not as convincing. To advance, a systematic exploration of the effects of different types of background knowledge appears to be in order.

Besides the above mentioned immediate next steps, of course there also remains the broader vision for our work: The engineering of a human-machine data analysis support system that uses background information to provide explanations to a human analyst.

Acknowledgement

This research was funded by the U.S. Government via contract FA8649-20-9-9045 to Kairos Research. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Government.

References


