Human-Guided Learning of Column Networks: Knowledge Injection for Relational Deep Learning

Mayukh Das
mayukh.das@samsung.com
Samsung R&D Institute, Bangalore

Devendra Singh Dhami
devendra.dhami@utdallas.edu
The University of Texas at Dallas

Yang Yu
yangyu@hlt.utdallas.edu
The University of Texas at Dallas

Gautam Kunapuli
gautam.kunapuli@verisk.com
Verisk Analytics, Inc.

Sriraam Natarajan
sriraam.natarjan@utdallas.edu
The University of Texas at Dallas

ABSTRACT

Recently, deep models have been successfully adopted in several applications, especially where low-level representations are needed. However, sparse, noisy samples and structured domains (with multiple objects and interactions) are some of the major challenges in most deep models. Column Networks, a deep architecture, can succinctly capture domain structure and interactions, but may still be prone to sub-optimal learning from sparse and noisy samples. Inspired by the success of human-knowledge guided learning in AI, especially in data-scarce domains, we propose Knowledge-augmented Column Networks that leverage human advice/knowledge for better learning with noisy/sparse samples. Our experiments demonstrate that our approach leads to either superior overall performance or faster convergence (i.e., both effective and efficient).

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

CODS COMAD 2021, January 2–4, 2021, Bangalore, India
© 2021 Association for Computing Machinery.
ACM ISBN 978-1-4503-8817-7/21/01...
https://doi.org/10.1145/3430984.3431018

1 INTRODUCTION

The re-emergence of Deep Learning (Goodfellow et al., 2016) has found significant and successful applications in complex real-world tasks such as image (Krizhevsky et al., 2012), audio (Lee et al., 2009) and video processing. However, the combinatorial complexity of reasoning in relational domains over a large number of relations and objects has remained a significant bottleneck to overcome. Recent work in relational deep learning has sought to address this particular challenge (França et al., 2014, Kaur et al., 2017, Kazemi and Poole, 2018, Šourek et al., 2015). Column Networks, CLN (Pham et al., 2017), a deep architecture composed of several (feedforward) interconnected mini-columns each of which represents an entity in the domain, is a particularly promising approach for several reasons - (1) hidden layers of a CLN share parameters, which restricts the parameter space from exploding with increasing depth, (2) as the depth increases, the CLN can begin to model feature interactions of considerable complexity and well as long range relational dependencies and (3) learning and inference are linear in the size of the network and the number of relations, which makes CLNs highly efficient. In brief CLNs can fundamentally represent relational structure in an implicit fashion, unlike other graph-centric deep models which learn numerical embeddings of relational structures. However, as our evaluation also illustrates, CLNs have not overcome the necessity to rely on vast amounts of data for optimal learning since it does not leverage any knowledge about the problem domain, similar to most deep architectures. This problem is even more critical in structured domains since only a small fraction of relationships are actually true rendering implicit sample sparsity. It is well known that inductive bias is necessary for optimal generalization over new instances (Mitchell, 1980). One of the fundamental forms of inductive bias comes from knowledge of the target domain/task. While deep learning does incorporate domain knowledge (for example, through parameter tying, convolutions, attention mechanisms or denoising encoders) but they are limited in their scope and treatment of such knowledge. We are motivated to develop systems that can incorporate richer and more general forms of domain knowledge. Human experts can guide learning by providing rules over training examples and features. The earliest such approaches combined explanation-based learning (EBL-NN, (Shavlik and Towell, 1989)) or symbolic domain rules with ANNs (KBANN, (Towell and Shavlik, 1994)). Another natural way a human could guide learning is by expressing preferences and has been studied extensively within the preference-elicitation framework due to Boutilier et al. (2006). We are inspired by this form of knowledge as they have been successful within the context of inverse reinforcement learning (Kunapuli et al., 2013), imitation learning (Odom et al., 2015) and planning (Das et al., 2018).

These approaches span diverse machine learning formalisms, and they all exhibit the same remarkable behavior: better generalization with fewer training examples because they effectively exploit and incorporate domain knowledge as an inductive bias. This is the prevailing motivation for our approach: to develop a framework that allows a human to guide deep learning by incorporating rules and constraints that define the domain and its aspects. Incorporation of prior knowledge into deep learning has begun to receive interest recently, for instance, the recent work on incorporating prior knowledge of color and scene information into deep learning for image classification (Ding et al., 2018). However,
in many such approaches, the guidance is not through a human, but rather through a pre-processing algorithm to generate guidance. Our framework is much more general in that a human provides guidance during learning. Furthermore, the human providing the domain knowledge is not an AI/ML expert but rather a domain expert who provides rules naturally. We exploit the rich representation power of relational methods to capture, represent and incorporate such rules into relational deep learning models. Note that our focus is not combining logic and deep networks as several others have explored this connection for decades since the origin of neuro-symbolic reasoning to more recent ILP-based neural models (Kaur et al., 2017, Kazemi and Poole, 2018). We use first-order logic as a representation language for human knowledge and employ it in the context of CLNs.

We make the following contributions: (1) we propose the formalism of Knowledge-augmented Column Networks, (2) we present, inspired by previous work (such as KBANN), an approach to inject generalized domain knowledge in a CLN and develop the learning strategy that exploits this knowledge, and (3) we demonstrate, across four real problems in some of which CLNs have been previously employed, the effectiveness and efficiency of injecting domain knowledge. Specifically, our results across the domains clearly show statistically superior performance with small amounts of data. As far as we are aware, this is the first work on human-guided CLNs.

2 BACKGROUND AND RELATED WORK

Using domain knowledge as inductive bias to accelerate learning has long been explored (Fung et al., 2003, Kunapuli et al., 2010, Le et al., 2006a, Odom and Natarajan, 2018, Towell and Shavlik, 1994). Fu et al., (1995) presents a unified view of different variations of knowledge-based neural networks. Such knowledge based learning has been proposed for support vector machines (Fung et al., 2003, Le et al., 2006b) in propositional cases and probabilistic logic models (Odom and Natarajan, 2018) for relational cases. (Towell and Shavlik, 1994) introduce the KBANN algorithm which compiles first order logic rules into a neural network and (Kunapuli et al., 2010) present the first work on applying knowledge, in the form of constraints, to the perceptron. The knowledge-based neural network framework has been applied successfully to various real world problems such as recognizing genes in DNA sequences (Noordewier et al., 1991), robotic control (Handelman et al., 1990) and recently in personalised learning systems (Melesko and Kurilovas, 2018). Combining relational (symbolic) and deep learning methods has recently gained significant research thrust since relational approaches are indispensable in faithful and explainable modeling of implicit domain structure, which is a major limitation in most deep architectures in spite of their success. While extensive literature exists that aim to combine the two (Battaglia et al., 2016, Lodhi, 2013, Rocktäschel et al., 2014, Sutskever et al., 2009), to the best of our knowledge, there has been little or no work on incorporating knowledge in any such framework.

Column networks transform relational structures into a deep architecture in a principled manner and are designed especially for collective classification tasks (Pham et al., 2017). The architecture and formulation of the column network are suited for adapting it to the advice framework. The GraphSAGE algorithm (Hamilton et al., 2017) shares similarities with column networks since both architectures operate by aggregating neighborhood information but differs in the way the aggregation is performed. Graph convolutional networks (Kipf and Welling, 2016) is another architecture that is very similar to the way CLN operates, again differing in the aggregation method. Diligenti et al., (2017) presents a method of incorporating constraints, as a regularization term, which are first order logic statements with fuzzy semantics, in a neural model and can be extended to collective classification problems. While it is similar in spirit to our proposed approach it differs in its representation and problem setup.

Several recent approaches aim to make deep architectures robust to label noise by either learning from easy samples with importance weights or by additional noise-adaptation layers or, may be, by regularization over virtual adversarial randomization (Goldberger and Ben-Reuven, 2017, Jiang et al., 2018, Miyato et al., 2018, Patrini et al., 2017).

While the above approaches enable effective learning of deep models in presence of noise, there are some fundamental differences with our problem setting.

(1) [Type of noise]: We aim to handle systematic noise (Odom and Natarajan, 2018) which is frequent in real-world due to cognitive bias or sample sparsity.

(2) [Type of error]: Systematic noise leads to generalization errors (see Example 1).

(3) [Structured data]: K-CLN works in the context of structured data (entities/relations). Though crucial, structured data is inherently sparse (most relations are false in the real world).

(4) [Noise prior]: Most noise handling approaches for deep models explicitly try to model the noise, which is impossible for systematic noise. K-CLN instead allows expert knowledge to guide the learner towards better generalization via an inductive bias.

Augmented learning with human knowledge has been proven to be an effective strategy in machine learning, probabilistic learning or sequential decision making, in presence of systematic noise (sparsity + sample bias + errors in data recording). Although, pseudo-labels introduced by Lee, (2013) are used for constructing efficient semi-supervised methods in deep learning, weak supervision is not always successful as it assumes presence of large amounts of data and certainly not the best approach with noisy data (since the pseudo-labels are derived from the fully observed label set where noise could propagate). Advice is typically provided before the data set is encountered i.e., by a domain expert and hence is independent of the fully labeled data (which can be noisy). Data programming (Patrini et al., 2016) can be viewed as constraining the data using weak labels and is orthogonal to our setting since which can be regarded as constraining the model or hypotheses space.

3 KNOWLEDGE-AUGMENTED COLUMN NETWORKS

3.1 Column Network: A brief background

Column Networks (Pham et al., 2017) allow for encoding interactions/relations between entities as well as the attributes of such
entities in a principled manner without explicit relational feature construction or vector embedding. This enables us to seamlessly transform a multi-relational knowledge graph into a deep architecture making them one of the robust relational deep models. Figure 1 illustrates an example column network, with respect to the knowledge graph on the left. Note how each entity forms its own column and relations are captured via the sparse inter-column connectors. Consider a graph $G = (V, A)$, where $V = \{e_i\}_{i=1}^{V_i}$ is the set of vertices/entities. Without loss of generality, we assume only one entity type. $A$ is the set of arcs/edges between two entities $e_i$ and $e_j$ denoted as $r(e_i, e_j)$. Note that the graph is multi-relational, i.e., $r \in R$ where $R$ is the set of relation types in the domain. To obtain the equivalent Column Network $C$ from $G$, let $x_i$ be the feature vector representing the attributes of an entity $e_i$ and $y_i$ its label predicted by the model. $h_i^f$ denotes a hidden node w.r.t. entity $e_i$ at the hidden layer $t$ ($t = 1, ..., T$ is the index of the hidden layers). The context between 2 consecutive layers captures the dependency of the immediate neighborhood (based on edges/inter-column connectors). For entity $e_i$, the context w.r.t. $r$ and hidden nodes are computed as,

$$c_{i,r}^t = \frac{1}{|N_r(i)|} \sum_{j \in N_r(i)} h_{j}^{t-1};$$

$$h_{i}^{t} = g(b^t + W^t h_{i}^{t-1} + \sum_{r \in R} V_{r}^{t} c_{i,r}^{t})$$

where $N_r(i)$ are all the neighbors of $e_i$ w.r.t. $r$ in the knowledge graph $G$. Note the absence of context connectors between $h_{i}^{t}$ and $h_{i}^{t}$ (Figure 1, right) since there does not exist any relation between $e_2$ and $e_4$ (Figure 1, left). The activation of the hidden nodes is computed as the sum of the bias, the weighted output of the previous hidden layer and the weighted contexts where $W^t \in \mathbb{R}^{K^t \times K^{t-1}}$ and $V_r^t \in \mathbb{R}^{K^t \times K^{t-1}}$ are weight parameters and $b^t$ is a bias for some activation function $g$. $z$ is a pre-defined constant that controls the parameterized contexts from growing too large for complex relations. Setting $z$ to the average number of neighbors of an entity is a reasonable assumption. The final output layer is a softmax over the pre-final layer, $T, P(y_i = t|h_{i}^{T}) = \text{softmax} \left( b_t + W_t h_{i}^{T} \right)$ where $t \in L$ is the label ($L$ is the set of labels).

### 3.2 Problem Setting

For a clearer perspective of the problem we aim to address, let us consider the following example,

**Example 1.** We wish to classify whether a published article is about carcinoid metastasis (Zuetenhorst and Taal, 2005) or is irrelevant, from a citation network, and textual features of articles. There are several challenges: (1) Data is implicitly sparse due to rarity of clinical studies, (2) Some articles may cite other articles about carcinoid and contain some textual features, but may actually address another topic and (3) Finally, the presence of systematic noise, introduced by the citation parser or uninformative abstracts.

The above cases may lead to the model not being able to effectively capture certain dependencies, or converge slower, even if they are captured somewhere in the advanced layers of the deep network. We use $\text{cites}(E_2, E_1)$ to denote that article $E_2$ cites article $E_1$, i.e., $E_2 \rightarrow E_1$. To model this dependency we can either have just the preferred label in head of the clause and assume all others as non-preferred, or assume the entire expression as a single literal. Intuitively a rule can be interpreted as conditional rule. We denote a set of preference rules by $\mathcal{P}$.

**Example 2.** For the prediction task mentioned in Example 1, a possible preference rule could be:

$\text{hasWord}(E_1, "\text{AI}"angle \land \text{hasWord}(E_2, "\text{domain}) \land$

$cites(E_2, E_1) \Rightarrow label(E_2, "\text{irrelevant}"angle$

Intuitively, this rule denotes that an article is not a relevant clinical work to carcinoid metastasis if it cites an ‘AI’ article and contains the word ‘domain’, since it is likely to be another AI article that uses carcinoid metastasis as an evaluation domain.

### 3.4 Knowledge Injection

Given that knowledge is provided as partially-instantiated preference rules $\mathcal{P}$, more than one entity may satisfy a preference rule. Also, more than one preference rules may be applicable for a single entity. The main intuition is that we aim to consider the error of
the trained model w.r.t. both the data and the advice. Consequently, in addition to the “data gradient” as with original CLNs, there is a “advice gradient”. This gradient acts a feedback to augment the learned weight parameters (both column and context weights) towards the direction of the advice gradient. It must be mentioned that not all parameters will be augmented. Only the parameters w.r.t. the entities and relations (contexts) that satisfy the win conditions, should be

in the column network aligned with the direction of the “advice gradient”. We choose the gating function \( F() \) as an exponential \( \exp(\mathcal{F}(\alpha \psi_i^{(c)})) \). The intuition is that soft gates are natural, as they are multiplicative and a positive gradient will result in \( \exp(\alpha \psi_i^{(c)}) > 1 \) increasing the value/contribution of the respective term, while a negative gradient results in \( \exp(\alpha \psi_i^{(c)}) < 1 \) pushing them down. We now present the “advice gradient” (the gradient with respect to preferred labels).

**Proposition 1.** Under the assumption that the loss function with respect to advice / preferred labels is a log-likelihood, of the form \( \mathcal{L}_{\psi} = \log P(y_{i}^{(\psi)} | h_{i}^{T}) \), then the advice gradient is, \( \nabla_{\psi} = I(y_{i}^{(\psi)}) - P(y_{i}) \), where \( y_{i}^{(\psi)} \) is the preferred label of entity \( i \) and \( \psi_i \) is an indicator function over the preferred label. For binary classification, the indicator is inconsequential but for multi-class scenarios it is essential (\( l = 1 \) for preferred label \( l \) and \( l = 0 \) for \( \bar{l} \)).

Since an entity can satisfy multiple advice rules we take the most preferred label, i.e., we take the label \( y_{i}^{(\psi)} = \tau \) to the preferred label if \( \tau \) is given by most of the advice rules that \( e_j \) satisfies. In case of conflicting advice (i.e. different labels are equally advised), we simply set the advice label to be the label given by the data, \( y_{i}^{(\psi)} = y_{i} \) (Proof in supplementary appendix). As illustrated in the K-CLN architecture (Figure 2), at the end of every epoch of training the advice gradients are computed and soft gates are used to augment the value of the hidden units (Equation 3).

**Proof for Proposition 1.** Most advice based learning methods formulate the effect of advice as a constraint on the parameters or a regularization term on the loss function. We consider a regularization term based on the advice loss \( \mathcal{L}_{\psi}^{(\psi)} = \log P(y_{i}^{(\psi)} | h_{i}^{T}) \) and we know that \( P(y_{i}) = \softmax(h_{i}) \). We consider \( b_{r} + W_{r}h_{i}^{T} = \Psi_{r}(y_{i}, h_{i}^{T}) \) in its functional form following prior non-parametric boosting approaches (Odom et al., 2015). Thus \( P(y_{i} = y_{i}^{(\psi)} | h_{i}^{T}) = \exp(\Psi_{r}(y_{i}, h_{i}^{T})) \sum_{y_{i}' \in L} \exp(\Psi_{r}(y_{i}', h_{i}^{T})) \). A functional gradient w.r.t. \( \psi \) of \( \mathcal{L}_{\psi}^{(\psi)} \) yields,

\[
\nabla_{\psi} = \frac{\partial \log P(y_{i} = y_{i}^{(\psi)} | h_{i}^{T})}{\partial \Psi_{r}(y_{i}, h_{i}^{T})} = I(y_{i}^{(\psi)}) - P(y_{i})
\]

Alternatively, assuming a squared loss such as \( (y_{i}^{(\psi)} - P(y_{i}))^2 \), would result in an advice gradient of the form \( 2(y_{i}^{(\psi)} - P(y_{i}))(1 - P(y_{i}))P(y_{i}) \). We observe that in a functional form the advice gradient is the difference between the true label distribution and the predicted distribution (or some function of that difference), irrespective of the type of loss we choose to optimize. As illustrated in the K-CLN architecture (main paper), at the end of every epoch of training the advice gradients are computed and soft gates are used to augment the value of the hidden units as shown in the main section,

\[
\nabla_{\psi} = \frac{\partial \log P(y_{i} = y_{i}^{(\psi)} | h_{i}^{T})}{\partial \Psi_{r}(y_{i}, h_{i}^{T})} = I(y_{i}^{(\psi)}) - P(y_{i})
\]
prediction case, where the objective function is now a binary cross-entropy of the form, $H = - \frac{1}{N} \sum_{i=1}^{N} y_{i} \log(P(y_{i})) + (1 - y_{i}) \log(1 - P(y_{i}))$.

Ignoring the summation for brevity, for every entity $i$, $H_{i} = y_{i} \log(P(y_{i})) + (1 - y_{i}) \log(1 - P(y_{i}))$. Extension to the multi-label prediction case with a sparse categorical cross-entropy is straightforward and is an algebraic manipulation task. Thus, from Proposition 1, the loss function w.r.t. advice is the log likelihood of the form, $L_{d}^\Psi = \log P(y_{i}^\Psi | h)$. Thus the modified objective is,

\[ H_{i}^{\prime} = (1 - \alpha) \left[ y_{i} \log(P(y_{i})) + (1 - y_{i}) \log(1 - P(y_{i})) \right] + \alpha \log(P(y_{i}^\Psi)) \]

(6)

where $\alpha$ is the trade-off parameter. $P(y) = P(y|h^T)$ can be implicitly understood. Now we know from Proposition 1 that the distributions, $P(y_{i})$ and $P(y_{i}^\Psi)$, can be expressed in their functional forms, given that the activation function of the output layer is a softmax, as $P(y_{i}) = \exp(\Psi_{y_{i}}^{h_{i}T})/\sum_{y_{i}'} \exp(\Psi_{y_{i}'}^{h_{i}T})$. Taking the functional (partial) gradients w.r.t. $\Psi_{y_{i}}^{h_{i}T}$ and $\Psi_{y_{i}'}^{h_{i}T}$ of the modified objective function (Equation 6), followed by some algebraic manipulation we get,

\[ \nabla(H_{i}^{\prime}) = \left(1 - \alpha\right) \left[ y_{i} I_{i} - y_{i} P(y_{i}) - P(x_{i}) + y_{i} P(y_{i}) \right] + \alpha \left( I_{i}^{\Psi} - P(y_{i}^\Psi) \right) \]

Hence, it follows from Proposition 2 that the data and the advice balance the training of the K-CLN network parameters $\theta^\Psi$ via the trade-off hyperparameter $\alpha$. When data is noisy (or sparse with negligible examples for a region of the parameter space) the advice/knowledge (if correct) induces a bias on the output distribution towards the correct label. Even if the advice is incorrect, the network still tries to learn the correct distribution to some extent from the data (if not noisy). The contribution of the effect of data vs effect of advice will primarily depend on $\alpha$. If both data and human advice are sub-optimal, correct label distribution is not learnable.

3.5 The Algorithm

Algorithm 1 outlines all the key steps. KCLN($\mathcal{G}$), the main procedure [lines: 1-14], trains a Column Network using both the data (the knowledge graph $\mathcal{G}$) and the human advice (set of preference rules $\mathcal{P}$). It returns a K-CLN $\mathcal{C}^\Psi$ where $\theta^\Psi$ are the network parameters, which are initialized to any arbitrary value (0 in our case; line: 3). Our gating functions are piece-wise/non-smooth and apply only to the subspace entities, features and relations that satisfy the preference rules. So, as a pre-processing step, we create tensor masks that compactly encode such a subspace via the procedure CREATE_MASK() [line: 4].

The network $\mathcal{C}^\Psi(\theta^\Psi)$ is then trained through multiple epochs till convergence [lines: 6-12]. At the end of every epoch the output probabilities and the gradients are computed and stored in a shared data structure [line: 11] to be accessed in the next epoch. Training is largely similar to original CLN with two key modifications [line: 9]: (1) Equation 3 is the modified expression for hidden units. (2) The data trade-off $1 - \alpha$ augments the original loss and the advice trade-off $\alpha$, is used to compute the gates. Procedure CREATE_MASK() constructs the tensor mask(s) over the space of entities, features and relations/contexts that are required to compute the gates (as seen in line: 8). There are 3 key components of the advice mask. They are - (1) Entity mask $M_W(\#entities \times #features)$, indicates entities and relevant features are affected by the advice, (2) Context mask $M_C(\#entities \times #entities)$, indicates the contexts that are affected (relations are directed, so it is asymmetric), (3) Label mask $M_{label}$, indicates the preferred label of the affected entities, in a one-hot encoding. The masks are iteratively computed for every preference [lines: 19-25]. This includes satisfiability checking, $p \in \mathcal{P}$ [line: 20], which is achieved via subgraph matching on the knowledge graph $\mathcal{G}$ (preference rule $\mathcal{G}$ subgraph template) ((Das et al., 2019, 2016)). The components $M_W$ and $M_C$ are used in gate computation in main procedure and $M_{label}$ is used for the indicator $I_{i}^{\Psi}$ in the advice gradient.

4 EXPERIMENTS

We investigate the following questions via our evaluation,

(1) Can K-CLNs learn efficiently with noisy sparse samples i.e., performance?
(2) Can K-CLNs learn effectively with noisy sparse samples i.e., speed of learning?
(3) How does quality of advice affect the performance of K-CLN i.e., reliance on robust advice?

We compare against the original Column Networks architecture with no advice (Vanilla CLN indicates the original Column Network architecture (Pham et al., 2017)) as a baseline. Our intention is to show how advice/knowledge can guide model learning towards better predictive performance and efficiency, in the context of collective classification using Column Networks. Also, our problem setting is distinct from most existing noise robust deep learning approaches. Thus, we restrict our comparisons to the original work.

**System:** K-CLN extends original CLN architecture, which uses Keras as the functional deep learning API with a Theano backend for tensor manipulation. We extend this system to include: (1) advice gradient feedback at the end of every epoch, (2) modified hidden layer computations and (3) a pre-processing wrapper to parse the advice/preference rules and create appropriate tensor masks. Since it is not straightforward to access final layer output probabilities from inside any hidden layer using keras, we use Callbacks to write/update the predicted probabilities to a shared data structure at the end of every epoch. This data structure is then fed via inputs to the hidden layers. Each mini-column with respect to an entity is a dense network of 10 hidden layers with 40 hidden nodes in each layer (similar to the most effective settings outlined in (Pham et al., 2017)). The advice masks encode $\mathcal{P}$, i.e., the set of entities and contexts where the gates are applicable (Algorithm 1).

**Domains:** We evaluate our approach on four relational domains – Pubmed Diabetes and Corporate Messages, (multi-class), and Internet Social Debates and Social Network Disaster Relevance (binary). Pubmed Diabetes$^2$ is a citation network for predicting whether a peer-reviewed article is about Diabetes Type 1, Type 2 or none, using textual features (TF-IDF vectors) from 19717 pubmed abstracts and 44,338 citation relationships among them. Here articles are entities with 500 bag-of-words features (TF-IDF vectors). Internet Social Debates$^3$ is for predicting stance (‘for’/‘against’) about a debate topic from online posts on social debates. It contains 6662 posts (entities) characterized by TF-IDF vectors and $\sim$25000 relations of 2 types, ‘sameAuthor’ and ‘sameThread’. Corporate Messages$^4$ is an intention prediction data set of 3119 flier messages sent by corporate groups in the finance domain, with 1,000,000 sameSourceGroup relations. We predict the intention of the message (Information, Action or Dialogue). Finally, Social Network Disaster Relevance is a relevance prediction data set of 8000 Twitter posts, curated and annotated by crowd with relevance scores. Besides textual ones, we use score features and 35$k$ relations among tweets.

<table>
<thead>
<tr>
<th>Domains</th>
<th>#Entities</th>
<th>#Relations</th>
<th>#Features</th>
<th>Target Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pubmed</td>
<td>19717</td>
<td>44,338</td>
<td>500</td>
<td>Multi-class</td>
</tr>
<tr>
<td>Corporate</td>
<td>3119</td>
<td>$\sim$1,000,000</td>
<td>750</td>
<td>Multi-class</td>
</tr>
<tr>
<td>Debates</td>
<td>6662</td>
<td>$\sim$25000</td>
<td>500</td>
<td>Binary</td>
</tr>
<tr>
<td>Disaster</td>
<td>8000</td>
<td>35000</td>
<td>504</td>
<td>Binary</td>
</tr>
</tbody>
</table>

$^2$https://linqs.soe.ucsc.edu/data
$^3$http://nldslab.soe.ucsc.edu/iac/v2/
$^4$https://www.figure-eight.com/data-for-everyone/
Human-Guided Learning of Column Networks: Knowledge Injection for Relational Deep Learning CODS COMAD 2021, January 2–4, 2021, Bangalore, India

Figure 4: Performance w.r.t. varying samples. Sample size is varied from 3% to 48% of total.

(of types ‘same author’ and ‘same location’). Table 1 outlines the important aspects of the 4 domains.

**Metrics:** Following (Pham et al., 2017), we report macro-F1 and micro-F1 scores for the multi-class problems, and F1 scores and AUC-PR for the binary ones. Macro-F1 computes the F1 score independently for each class and takes the average whereas a micro-F1 aggregates the contributions of all classes to compute the average F1 score. Due to space limitation, we show only the Micro-F1 and the AUC-PR results (complete set of plots - in supplementary appendix). For all experiments we use 10 hidden layers and 40 hidden units per column in each layer. All results are averaged over 5 runs.

**Human Advice:** K-CLN is designed to handle arbitrarily complex expert advice encoded as preference rules. However, even with some relatively simple preference rules K-CLN is more effective in sparse samples. E.g. In Pubmed, the most complex preference rule is, \( \text{HasWord}(e_1, \text{'fat'}) \land \text{HasWord}(e_1, \text{'obese'}) \land \text{Cites}(e_2, e_1) \Rightarrow [\text{label}(e_2, \text{type}_2)] \). Note how a simple rule, indicating an article citing another one discussing obesity is likely to be about Type2 diabetes, proved to be effective. Knowledge from real physicians can thus, be extremely effective. In Disaster Relevance even advice rules without domain expertise, such as a tweet is likely to be NOT about disaster, if posted by the same user who usually posts non-disaster tweets. Advice rules for experiments in other domains are designed in a similar fashion as well, i.e. via simple inspection and understanding of the domains. Another notable aspect is that, sub-optimal advice may lead to a wrong direction of the Advice Gradient. However, our soft gates do not alter the loss, but instead are akin to attention mechanisms that promote/demote the contribution of nodes/contexts. The trade-off parameter \( \alpha \) balances the effect of advice and data during training.

**4.1 Results**

**Efficiency (Q1):** We present the aforementioned metrics with varying sample size and with increasing epochs and compare our model against Vanilla CLN. We split the data sets into a training set and a hold-out test set with 60%-40% ratio. For varying epochs we only learn on 40% of our pre-split training set (i.e., 24% of the complete data) to train the model and test on the hold-out test set. Figure 3 shows that, although both K-CLN and Vanilla CLN converge to the same predictive performance (Micro-F1 for PubMed & Corporate and AUC-PR for the rest), K-CLN converges significantly faster (less epochs). Also, for the corporate and the debate, K-CLN not only converges faster but also has a better predictive performance than Vanilla CLN (Figure 3). We have similar observations in Macro-F1 results (see appendix) These results show that K-CLNs learn more efficiently with noisy sparse samples thereby answering (Q1) affirmatively.

**Effectiveness (Q2):** The intuition is, domain knowledge should guide the model to learn better when the training data is sparse. Thus they are trained on gradually varying sample sizes from 5% of the training data (3% of the complete data) till 80% of the training data (48% of complete data) and tested on the hold-out test set. Figure 4 presents the performance results with varying sample sizes for all data sets. K-CLN outperforms Vanilla CLN across all sample sizes, on both metrics, which suggests that the advice is relevant throughout the training phase with varying sample sizes.
with reasonably low values of \( \alpha \) which controls the robustness of K-CLN to advice quality. Hence, while applying to the rest, effectively averaging out in Macro-F1.

Thus K-CLN outperforms CLN, with noisy sparse samples. However, we have observed that, for Macro-F1, the performance is similar for both, although K-CLN performs better with very small samples. This could happen, in multi-class prediction, when the advice may not apply to some of the classes, while applying to the rest, effectively averaging out in Macro-F1.

Thus K-CLN outperforms CLN, with noisy sparse samples (Q2).

**Robustness (Q3):** An obvious question is – how robust is our learning system to that of noisy/incorrect advice? Conversely, how does the choice of \( \alpha \) affect the quality of the learned model? To answer these, we consider the Internet Social Debates domain by augmenting the learner with incorrect advice. The incorrect advice is created by changing the preferred label of the advice rules to incorrect values (as per our understanding). Also, recall that the contribution of advice is dependent on the trade-off parameter \( \alpha \), which controls the robustness of K-CLN to advice quality. Hence, we experimented with different values of \( \alpha \) (0.2, 0.4, …, 1.0), across varying sample sizes. Figure 5 shows how with higher \( \alpha \) values the performance deteriorates due to the effect of noisy advice. \( \alpha = 0 \) is equivalent to no-advice/Vanilla CLN. Note, with reasonably low values of \( \alpha \) K-CLN is robust to quality of advice (Q3). We picked one domain to present robustness but observed similar behavior in all domains.

5 DISCUSSION

For Corporate Messages, K-CLN outperforms with small number of samples, gradually converging to a similar prediction performance with larger samples. However, we have observed that, for Macro-F1, the performance is similar for both, although K-CLN performs better with very small samples. This could happen, in multi-class prediction, when the advice may not apply to some of the classes, while applying to the rest, effectively averaging out in Macro-F1. Thus K-CLN outperforms CLN, with noisy sparse samples (Q2).

6 CONCLUSION

We considered the problem of providing guidance for CLNs. Specifically, we assume that the advice givers as true domain experts and not CLN experts and we developed a formulation based on preferences. This formulation allowed for natural specification of guidance. We derived the gradients based on advice and outlined the theoretical analysis. We found that when \( \alpha \leq 0.5 \), K-CLN performs well even with noisy advice. In the earlier experiments where we use potentially good advice, we report the results with \( \alpha = 1 \), since the advice gradient is piecewise (affects only a subset of entities/relations). So it is reasonable to assign higher weight to the advice and the contribution of the entities and relations/contexts affected by it, given the advice is noise-free. Also, note that the drop in performance towards very low sample sizes (in Figure 5) highlights how learning is challenging in the noisy-data and noisy-advice scenario and aligns with our general understanding of most human-in-the-loop/advice-based approaches in AI. Trade-off between data and advice via a weighted combination of both is a well-studied solution (Odom and Natarajan, 2018) and, hence, we adapt the same. Again, Figure 6 illustrates the effect of amount advice (on Debates) when advice is optimal. Earlier experiments in Fig 3 & 4 where done with 6 advice rules. Note, although increasing \# rules beyond 6 helps in low sample sizes, the difference is not significant since the most important rules were given first.
ACKNOWLEDGMENTS
MD, GK & SN gratefully acknowledge the support of CwC Program Contract W911NF-15-1-0461 with the US Defense Advanced Research Projects Agency (DARPA) and the Army Research Office (ARO). SN also acknowledges the NSF grant IIS-1836565 and AFOSR award FA9500-18-1-0462. DSD acknowledges the National Institute of Health (NIH) grant no. RO1 GM097628. Any opinions, findings and conclusion or recommendations are those of the authors and do not necessarily reflect the view of the DARPA, ARO, AFOSR or the US government.

REFERENCES

Darius Braziunas and Craig Boutilier. 2006. Preference elicitation and generalized additive utility. In AAAI.


Lu Jiang, ZhengyuanZhou, Thomas Leung, Li-Jia Li, and LiFei-Fei. 2018. Mentornet: Learning data-driven curriculum for very deep neural networks on corrupted labels. In ICML.


Gautam Kunapuli, Kristin P Bennett, Richard Maclin, and Jude W Shavlik. 2010. The adviceptron: Giving advice to the perceptron. In ANNIE.

Gautam Kunapuli, Phillip Odom, Jude W Shavlik, and Sriraam Natarajan. 2013. Guiding autonomous agents to better behaviors through human advice. In ICDM.

Quoc V. Le, Alex J Smola, and Thomas G"artner. 2006a. Simpler knowledge-based support vector machines. In ICML.


Honglak Lee, Peter Pham, Yan Largman, and Andrew Y. Ng. 2009. Unsupervised feature learning for audio classification using convolutional deep belief networks.

In NIPS.


Trang Pham, Truyen Tran, Dinh Q Phung, and Svetla Venkatesh. 2017. Column Networks for Collective Classification. In AAAI.

Alexander J Ratner, Christopher M deSa, Sen Wu, Daniel Selsam, and Christopher Ré. 2016. Data programming: Creating large training sets, quickly. In NIPS.


Ilya Sutskever, Joshua B Tenenbaum, and Ruslan B Salakhutdinov. 2009. Modelling relational data using bayesian clustered tensor factorization. In NIPS.

