Systematic Generalization: What Is Required and Can It Be Learned?

Anonymous Author(s)
Affiliation
Address
e-mail

Abstract
Numerous models for grounded language understanding have been recently proposed, including (i) generic models that can be easily adapted to any given task and (ii) intuitively appealing Neural Module Networks (Andreas et al., 2016a) that require background knowledge to be instantiated. We compare generic and modular models in how much they lend themselves to a particular form of systematic generalization. Our findings show that the generalization of modular models is much more systematic and that it is highly sensitive to the module layout, i.e. to how exactly the modules are connected. We furthermore investigate if modular models that generalize well could be made more end-to-end by learning their layout and parametrization. We show how end-to-end methods from prior work often learn spurious layouts and parametrizations that do not facilitate systematic generalization. Our results suggest that, in addition to modularity, systematic generalization in language understanding may require explicit regularizers or priors.

1 Introduction

In recent years, neural network based models have become the workhorse of natural language understanding and generation showing state-of-the-art performance on numerous benchmarks, including Recognizing Textual Entailment (RTE) (Gong et al., 2017), Visual Question Answering (VQA) (Jiang et al., 2018), and Reading Comprehension (Wang et al., 2018). Despite these successes, a growing body of literature suggests that these approaches latch onto statistical regularities which are omnipresent in existing datasets (Agrawal et al., 2016; Gururangan et al., 2018; Jia & Liang, 2017) and do not generalize outside of the specific distributions they are trained on. These findings have recently been corroborated by Lake & Baroni (2018), who showed that seq2seq models (Sutskever et al., 2014; Bahdanau et al., 2015) show little systematicity (Fodor & Pylyshyn, 1988) in how they generalize, i.e. they fail to learn general rules on how to compose words.

Introduced by Andreas et al. (2016b), Neural Module Networks (NMNs) approach aims to improve the generalization capabilities of neural models by adding modularity and structure to their design to make them resemble the kind of rules they are supposed to learn. The NMN approach, while intuitively appealing, has seen limited adoption because of the large amount of domain knowledge it requires to decide (Andreas et al., 2016a) or predict (Johnson et al., 2017; Hu et al., 2017) how the modules should be created (parametrization) and how they should be connected (layout) based on a query. Besides, their performance has often been matched by more generic neural models, such as FiLM (Perez et al., 2017), Relations Networks (Santoro et al., 2017), and CAN (Hudson & Manning, 2018), and their generalization, to the best of our knowledge, has not been a subject of a focused study. In this work we investigate the impact of explicit modularity and structure on systematic generalization by studying the generalization of NMNs and contrasting it to those of generic models. We choose to focus on the following basic generalization requirement: a good model should be able
to reason about all possible object combinations despite being trained on a small subset of them. We instantiate this requirement in form of a simple yes-no Visual Question Answering (VQA) dataset.

Our first finding is that NMNs do generalize better than other neural models when an appropriate choice of layout and parametrization is made. We furthermore experiment with existing methods for making NMNs more end-to-end by inducing the module layout (Johnson et al., 2017) or learning module parametrization through soft-attention over the question (Hu et al., 2017). We show how such end-to-end approaches often fail to find the right structural settings and instead prefer a wrong chain layout or spurious parametrization and do not generalize better than the generic models. We believe that our findings challenge the intuition of researchers in the field and provide a foundation for improving systematic generalization of neural approaches to language understanding.

2 Setup

Dataset: SQOOP (Spatial Queries Over Object Pairs, Figure 1) is a minimalistic VQA task designed to test a particular type of generalization: the ability to disentangle the meaning of relation words and object words and then compose these meanings in novel contexts to perform basic relational reasoning in a consistent way. Concretely, SQOOP requires answering a yes-no question \( q = X R Y \) about whether objects \( X \) and \( Y \) are in a spatial relation \( R \), given a 64 × 64 RGB image \( x \). \( x \) contains 5 randomly chosen and randomly positioned objects. There are 36 objects: letters A-Z and digits 0-9, and 4 relations: \( \text{LEFT} \_ \text{OF} \), \( \text{RIGHT} \_ \text{OF} \), \( \text{ABOVE} \), and \( \text{BELOW} \). Our goal is to discover which models can correctly answer questions about all \( 36 \cdot 36 \) possible object pairs in the SQOOP dataset after having been trained on only a subset. Therefore, we train on \( 36 \cdot 4 \cdot k \) unique questions, where for every left-hand-side (LHS) object \( X \), we randomly sample \( k \) different right-hand-side objects (RHS), and test on the remaining \( 36 \cdot 4 \cdot (36 - k) \) questions. We refer to \( k \) as the \#rhs/lhs parameter of the dataset. To exclude a possible compounding factor of overfitting on training images, all our training sets contain 1 million examples obtained by sampling multiple images per question.

Models: We experiment with models from 2 broad categories. Generic models such as FiLM (Perez et al., 2017), Relation Networks (RelNet, Santoro et al. (2017)) and CAN Hudson & Manning (2018), and modular and structured Neural Module Networks (NMN). NMNs (Andreas et al., 2016b) construct question-specific networks by composing together trainable neural modules. To answer a question with an NMN, a computation graph is constructed by making 2 decisions: layout - the number of modules, their types and how they are connected, and parametrization - how these modules are parametrized based on the question. For our study we adapt the N2NMN (Hu et al., 2017) paradigm from this family, which predicts the layout with a seq2seq model (Sutskever et al., 2014) and computes the parametrization of the modules using a soft attention mechanism. Since all the questions in SQOOP have the same structure, we can get away with a single trainable layout variable and separate trainable attention variables per each module. We also experiment with hard-coded layout and parametrization setting, in the spirit of original NMN (Andreas & Klein, 2015).

Formally, our NMN is constructed by repeatedly applying a generic neural module \( f(\theta, \gamma, h_l, h_r) \), which takes as inputs the shared parameters \( \theta \), the question-specific parametrization \( \gamma \) and the left-
Table 1: Comparing the performance of generic models to the structured NMN-Tree model on the hardest version of our dataset (lower #rhs/lhs is more difficult).

<table>
<thead>
<tr>
<th>model</th>
<th>train. acc (%)</th>
<th>test acc. (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conv+LSTM</td>
<td>97.9</td>
<td>64.4±1.8</td>
</tr>
<tr>
<td>RelNet</td>
<td>95.6</td>
<td>63.1±1.0</td>
</tr>
<tr>
<td>FiLM</td>
<td>100</td>
<td>66.6±2.5</td>
</tr>
<tr>
<td>MAC</td>
<td>99.5</td>
<td>72.6±3.4</td>
</tr>
<tr>
<td>NMN-Tree (Residual)</td>
<td>100</td>
<td>100.0±0.0</td>
</tr>
<tr>
<td>NMN-Tree (Find)</td>
<td>100.0</td>
<td>99.7±0.3</td>
</tr>
<tr>
<td>NMN-Chain (Find)</td>
<td>99.2</td>
<td>51.4±2.8</td>
</tr>
<tr>
<td>NMN-Chain-XTY (Residual)</td>
<td>100</td>
<td>51.6±1.6</td>
</tr>
<tr>
<td>NMN-Chain-XXY (Residual)</td>
<td>99.7</td>
<td>54.1±1.7</td>
</tr>
<tr>
<td>NMN-Chain-RXY (Residual)</td>
<td>98.7</td>
<td>50.5±0.9</td>
</tr>
</tbody>
</table>

3 Experiments

Find the Right Kind of NMN Be Induced: The generalization of NMN-Tree model, while impressive, is somewhat unsurprising because both the layout and parametrization of this model encode a significant amount of prior knowledge about the task. We therefore investigate whether the amount of such prior knowledge can be reduced by fixing one of the structural aspects and inducing the other. For inducing a layout, we use the Stochastic N2NMN model. We experiment with both Find and
Table 2: Layout induction results for Stochastic N2NMNs using Residual modules and Find modules. For each setting of \(p_0(tree)\), we report results on 1 rhs/lhs and 18 rhs/lhs datasets.

(a) Residual modules

<table>
<thead>
<tr>
<th>#rhs/lhs</th>
<th>(p_0(tree))</th>
<th>test acc. (%)</th>
<th>(p_{50K}(tree))</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.1</td>
<td>52.7 ± 2.2</td>
<td>0.003</td>
</tr>
<tr>
<td></td>
<td>0.5</td>
<td>57.0 ± 4.4</td>
<td>0.026</td>
</tr>
<tr>
<td></td>
<td>0.9</td>
<td>99.9 ± 0.1</td>
<td>0.997</td>
</tr>
<tr>
<td>18</td>
<td>0.5</td>
<td>97.7 ± 5.1</td>
<td>0.999</td>
</tr>
<tr>
<td></td>
<td>0.9</td>
<td>99.1 ± 2.3</td>
<td>0.999</td>
</tr>
</tbody>
</table>

(b) Find modules

<table>
<thead>
<tr>
<th>#rhs/lhs</th>
<th>(p_0(tree))</th>
<th>test acc. (%)</th>
<th>(p_{50K}(tree))</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.1</td>
<td>81.2 ± 2.9</td>
<td>0.100</td>
</tr>
<tr>
<td></td>
<td>0.5</td>
<td>93.2 ± 7.1</td>
<td>0.999</td>
</tr>
<tr>
<td></td>
<td>0.9</td>
<td>95.9 ± 1.6</td>
<td>0.999</td>
</tr>
<tr>
<td>18</td>
<td>0.5</td>
<td>78.6 ± 20.7</td>
<td>0.2</td>
</tr>
<tr>
<td></td>
<td>0.9</td>
<td>91.6 ± 6.5</td>
<td>0.999</td>
</tr>
</tbody>
</table>

Residual modules and report results with diverse initial conditions, \(p_0(tree) = 0.1, 0.5, 0.9\), where \(p_0(tree)\) is the initial value of \(p(T_{tree})\). The results obtained on the #rhs/lhs=1 dataset (Table 2) show that the correct layout was not induced for \(p_0(tree) = 0.1\) and \(p_0(tree) = 0.5\) with the Residual module and for \(p_0(tree) = 0.1\) with the Find module. We also run similar experiments on an easy-to-generalize #rhs/lhs=18 version. Here, the NNN with Residual module preferred the tree layout for all initializations. It is notable, however, that in the setting with #rhs/lhs=1 where the correct choice of the layout is the only way to generalize, only a very lucky initialization \(p_0(tree) = 0.9\) resulted in successful layout induction for the Residual module.

For parameterization induction, we experiment with the Attention N2NMM model on #rhs/lhs=1 and #rhs/lhs=18. The model often did not find the attention settings that lead to generalization on the challenging #rhs/lhs=1 split (83.8% test accuracy). That should be contrasted with the close-to-perfect 99.2% accuracy of the model that was trained on #rhs/lhs=18 version of the task, suggesting that the parameterization induction did not work due to the difficulty of our #rhs/lhs=1 split. To analyze the learnt attention weights, we compute a sharpness ratio \(\rho = \max(\alpha^{k,X}, \alpha^{k,Y})/\min(\alpha^{k,X}, \alpha^{k,Y})\) for modules \(k = 1\) and \(k = 2\) for each of the trained modules. We find that the learnt attention weights on #rhs/lhs=1 are generally blurry with \(\rho < 2\) for 40% of the modules (details in Appendix-A.4).

4 Related Work

Using synthetic VQA datasets to study grounded language understanding is a recent trend started by CLEVR (Johnson et al., 2016), and recently the ShapeWorld dataset (Kuhnle & Copestake, 2017), that involves a number of VQA generalization tests. Closely related to our work is the recent study on generalization to long-tail questions about rare objects by Bingham et al. (2018). They do not, however, consider as many models as we do and do not study whether the best-performing models can be made end-to-end. Andreas et al. (2016a) introduced NMNs as a modular, structured VQA model where a fixed number of hand-crafted neural modules are chosen and composed together in a layout determined by the dependency parse of the question. Hu et al. (2017) and Johnson et al. (2017) followed up with end-to-end NMNs, removing the non-differentiable parser. Recent concurrent work by (Hu et al., 2018) attempts to remove the need for hard stochastic layout decisions.

5 Conclusion and Discussion

We have conducted a rigorous investigation of an important form of systematic generalization required for grounded language understanding: the ability to reason about all possible pairs of objects despite being trained on a small subset. The intuitive appeal of modularity and structure in designing neural architectures for language is now supported by our results. Our other key finding is that coming up with an end-to-end and/or soft version of modular models may be not sufficient for strong generalization, because in the very setting where strong generalization is required, end-to-end methods may find a different, less compositional solution (e.g. a chain layout or blurred attention). This conclusion is relevant in the view of recent work done in the direction of making Neural Module Networks more end-to-end (Suarez et al., 2018; Hu et al., 2018; Hudson & Manning, 2018). We hope that our findings will inform researchers working on language understanding and provide them with a useful intuition about what facilitates strong generalization and what is likely to inhibit it.
References


A Appendix

A.1 Additional Details

Dataset: To make negative examples in SQOOP challenging, we ensure that both X and Y of a question are always present in the associated image and that there are always distractor objects $Y' \neq Y$ and $X' \neq X$ such that $XRY'$ and $X'R Y$ are both true for the image. These extra precautions guarantee that answering a question requires the model to locate all possible X and Y then check if any pair of them are in the relation R.

Hyperparameters: All models share the same stem architecture which is a CNN based architecture of 6 layers. Each layer is a Conv $\rightarrow$ BatchNorm $\rightarrow$ ReLU with a MaxPool after layers 1 and 3. The input to the stem is a $64 \times 64 \times 3$ image, and the feature dimension used throughout the stem is 64. All models are optimized using Adam Kingma & Ba (2014) with a learning rate of 3e-4, and with minibatches of size 128.

A.2 Generic Models

We consider four generic models in this paper: CNN+LSTM, FiLM, Relation Networks (RelNet), and Compositional Attention Networks (CAN). For CNN+LSTM, FiLM, and RelNet models, the question $q$ is first encoded into a fixed-size representation $h_q$ using a unidirectional LSTM network.

CNN+LSTM flattens the 3D tensor $h_x$ to a vector and concatenates it with $h_q$ to produce $h_{q,x}$.

$$h_{q,x} = [\text{vec}(h_x); h_q] \quad (3)$$

RelNet uses a network $g$ which is applied to all pairs of feature columns of $h_x$ concatenated with the question representation $h_q$, all of which is then pooled to obtain $h_{q,x}$:

$$h_{q,x} = \sum_{i,j} g(h_x(i), h_x(j), h_q) \quad (4)$$

where $h_x(i)$ is the $i$-th feature column of $h_x$.

FiLM networks use $N$ convolutional FiLM blocks applied to $h_x$. A FiLM block is a residual block (He et al., 2016) in which a feature-wise affine transformation (FiLM layer) is inserted after the 2nd convolutional layer. The FiLM layer is conditioned on the question at hand via prediction of the scaling and shifting parameters $\gamma_n$ and $\beta_n$:

$$[\gamma_n; \beta_n] = W_q^n h_q + b_q^n \quad (5)$$

$$\hat{h}^n_{q,x} = \text{BN}(W^n_2 \ast \text{ReLU}(W^n_1 \ast h^{n-1}_{q,x} + b^n_1)) \quad (6)$$

$$h_{q,x} = h^{n-1}_{q,x} + \text{ReLU}(\gamma_n \odot \hat{h}^n_{q,x} + \beta_n) \quad (7)$$

where $BN$ stands for batch normalization, $\ast$ stands for convolution and $\odot$ stands for element-wise multiplications. $h^n_{q,x}$ is the output of the $n$-th FiLM block and $h^0_{q,x} = h_x$. The output of the last FiLM block $h^N_{q,x}$ undergoes an extra $1 \times 1$ convolution and max-pooling to produce $h_{q,x}$.

CAN networks of Hudson & Manning (2018) produces $h_{q,x}$ by repeatedly applying a Memory-Attention-Control (MAC) cell that is conditioned on the question through an attention mechanism. The CAN model is quite complex and we refer the reader to the original paper for details.

A.3 NMN Modules

As mentioned in the text, our experiments are performed with the Find module from Hu et al. (2017) and the Residual module from Johnson et al. (2017) with very minor modifications - we use 64 dimensional CNNs in our Residual blocks since our dataset consists of $64 \times 64$ images. The equations for the Residual module are as follows:

$$\theta = \emptyset, \quad (8)$$

$$\gamma = [W_1; b_1; W_2; b_2; W_3; b_3], \quad (9)$$

$$\tilde{h} = \text{ReLU}(W_3 [h_t; h_r] + b_3), \quad (10)$$

$$f_{\text{Residual}}(\gamma, h_t, h_r) = \text{ReLU}(\tilde{h} + W_1 \ast \text{ReLU}(W_2 \ast \tilde{h} + b_2)) + b_1), \quad (11)$$
and for Find module as follows:

\[
\theta = [W_1; b_1; W_2; b_2],
\]

\[
f_{\text{Find}}(\gamma, h_l, h_r) = \text{ReLU}(W_1 \ast \gamma \odot \text{ReLU}(W_2 \ast [h_l; h_r] + b_2) + b_1).
\]

In formulas above \( W_1, W_2, W_3 \) are convolution weights, and \( b_1, b_2, b_3 \) are biases. The main difference between Residual and Find is that in Residual all parameters depend on the questions words, whereas in Find convolutional weights are the same for all questions, and only the element-wise multipliers \( \gamma \) vary based on the question.

A.4 Additional Results

**Structure Induction:** We visualize the progress of structure induction for the Residual module with \( p_0(\text{tree}) = 0.5 \) in Figure 3. The figure shows \( p(\text{tree}) \) saturates to 0.0 or 1.0 eventually in \#rhs/lhs=1 and \#rhs/lhs=18 settings respectively.

**Parametrization Induction:** Figure 5 shows how attention weights evolve for an Attention N2NMN model in the same context. It is notable that unlike in the gold-standard NMN-Tree model, the relation word is mixed with the object words for modules 1 and 2. We also noticed that the model did not learn to focus modules 1 and 2 on different words in the \#rhs/lhs=1 setting (Figure 5b) as sharply as it did in \#rhs/lhs=18 (Figure 5a). To substantiate this observation with quantitative results, we compute a sharpness ratio \( \rho = \max(\alpha^{k,X}, \alpha^{k,Y})/\min(\alpha^{k,X}, \alpha^{k,Y}) \) for modules \( k = 1 \) and \( k = 2 \) for each of the 20 modules that we have trained. One can observe from the histogram in Figure 4 that attention weights learnt on \#rhs/lhs=1 are generally blurry, with \( \rho \) being less than 2 for 8 modules out of 20.
Figure 5: All three modules’ attention weights for parametrization of the three question words for (a) 18 rhs/lhs and (b) 1 rhs/lhs version of SQOOP. The model learns to disentangle between X and Y much better with more rhs/lhs.