

Deep learning evaluation using deep linguistic processing

Alexander Kuhnle Ann Copestake
University of Cambridge
{aok25, aac10}@cam.ac.uk

Abstract

We discuss problems with the standard approaches to evaluation for tasks like visual question answering, and argue that artificial data can be used to address these as a complement to current practice. We demonstrate that with the help of existing ‘deep’ linguistic processing technology we are able to create challenging abstract datasets, which enable us to investigate the language understanding abilities of multimodal deep learning models in detail.

1 Introduction & related work

In recent years, deep neural networks (DNNs) have established a new level of performance for many tasks in natural language processing (NLP), speech, computer vision and artificial intelligence (AI). Simultaneously, we observe a move towards simulated environments and artificial data, particularly in AI (Bellemare et al., 2013; Brockman et al., 2016). As outlined by Kiela et al. (2016), simulated data is appealing for various reasons. Most importantly, it acts as a prototypical problem presentation, abstracted from its noisy and intertwined real-world appearance.

However, with the exception of spoken dialogue systems (e.g., Scheffler and Young (2001)), artificial data is relatively little used in NLP. There are, nonetheless, a few recent examples, including the MazeBase game environment (Sukhbaatar et al., 2015), the long-term research proposal of Mikolov et al. (2015), or the bAbI tasks (Weston et al., 2015). Here we focus on the problem of *visually grounded language understanding* in the context of the recently popular task of visual question answering (VQA). In principle, this task is particularly interesting from a semantic perspective, since it combines general language understanding, reference resolution and grounded language reasoning in a simple and clear task. However, recent work (Goyal et al., 2016; Agrawal et al., 2016) has suggested that the popular VQA datasets are inadequate, due to various issues which allow an evaluated system to achieve competitive performance without truly learning these abilities.

To address this, several artificial VQA datasets have been released recently, including the SHAPES dataset (Andreas et al., 2016), the CLEVR dataset (Johnson et al., 2017a), the dataset of Suhr et al. (2017), and our ShapeWorld framework (Kuhnle and Copestake, 2017). They all consist of images showing abstract scenes with colored objects, and are introduced with the motivation to provide a challenging and clear evaluation for VQA systems. Johnson et al. (2017a) and Kuhnle and Copestake (2017) investigated popular VQA systems on their dataset, and demonstrate how artificial data provides us with detailed insights previously not possible. Despite its simplicity, they uncover fundamental shortcomings of current VQA models. Moreover, such datasets have been of great importance for the development of new VQA models based on reinforcement learning (Hu et al., 2017; Johnson et al., 2017b).

Our aims in this paper are threefold. First, we provide a brief but systematic review of the problems surrounding current standard evaluation practices in deep learning. Secondly, we use this to motivate the potential of artificial data from simulated microworlds to evaluate DNNs, particularly for (visually grounded) language understanding. Thirdly, we present a specific evaluation methodology based on the use of resources from the DELPH-IN (Deep Linguistic Processing with HPSG) collaboration, and show why compositional semantics from a bidirectional symbolic grammar is particularly suitable for the production of artificial datasets.

2 Problems of real-world datasets for deep learning evaluation

In the following, we review a variety of issues related to the practice of evaluating DNNs on popular real-world datasets for tasks like VQA.

2.1 Issues with crowd-sourced data

The fact that DNNs require immense amounts of data for successful training led to the practice of adopting online data, such as the Flickr photo sharing platform, and leveraging crowd-sourcing, usually via Amazon Mechanical Turk (AMT). For instance, MS COCO (Lin et al., 2014) is an image caption dataset which contains more than 300,000 images annotated with more than 2 million human-written captions, while the popular VQA dataset Antol et al. (2015) is based on MS COCO. There are, however, various problems related to this practice.

Data obtained this way tends to be comparatively simple in terms of syntax and compositional semantics, despite exhibiting a degree of lexical complexity due to its real-world breadth. Moreover, *repurposed* photos do not – and were never intended to – reflect the visual complexity of every-day scenarios (Pinto et al., 2008). Humans given the task of captioning such images will mostly produce descriptions which are syntactically simple. The way that workers on crowd-sourcing platforms are paid gives them an incentive to come up with captions quickly, and hence further increases the tendency to simplicity. Note also that, while this is a form of real-world data, it has very little relationship to the way that a human language learner perceives the world. For instance, the photo/question pairs are presented to a VQA system randomly and with no possibility of detailed interaction with a particular scene.

Natural language follows Zipf’s law for many aspects (sentence length, syntactic complexity, word usage, etc), and consequently has an inbuilt simplicity bias when considered in terms of probability mass. The contents of image datasets based on photos also have a Zipfian distribution, but with biases which relate to what people choose to photograph rather than to what they see. Animal images in the VQA dataset are predominantly cats and dogs, sport images mainly baseball and tennis (see Antol et al. (2015) for more statistics). Considering all these biases both in language and vision, the common evaluation measure – simple accuracy of questions answered correctly – is not a good reflection of a system’s general ability to understand visually grounded language.

2.2 The Clever Hans effect

Crowd-sourced visual questions have other unexpected properties. Goyal et al. (2016) and Mahendru et al. (2017) note how questions rarely talk about objects that are not present in the image, hence an existential question like “*Do you see a...?*” is often true. Agrawal et al. (2016) also give the example of questions like “*What covers the ground?*”, which can confidently be answered with “*snow*” because of biases in common real-world scenes, or, more precisely, biases in the photographs of real-world scenes. Such biases help to explain why some *text-only* systems turn out to perform well on visual question answering when evaluated on the VQA dataset.

Sturm (2014) compared such unexpected cues when evaluation machine learning systems to the story of “Clever Hans”, a horse exhibited in the early 20th century which was claimed to understand German and have extensive arithmetical and reasoning abilities. Hans was eventually found to be picking up on very subtle cues which were given completely unconsciously by his owner and which were not noticed by ordinary observers. Some of the recent findings for DNNs, particularly in NLP, suggest similarly problematic conclusions: Is the bag-of-words model actually able to encode sequential information, as its surprisingly strong performance in comparison to an LSTM suggests (Adi et al., 2017)? Is visual information really not as important to answer visually grounded questions, as the strong performance of text-only systems suggests (Jabri et al., 2016)? Or are these results indicating an instance of the *Clever Hans effect*, and due to unnoticed biases in the datasets?

A more fundamental form of this effect is illustrated by recent investigations in image recognition. Szegedy et al. (2014) and Nguyen et al. (2015) have shown surprisingly odd system behavior when

confronted with either only minimally modified images or almost random noise. This behavior seems due to the specific interplay of a few parameters which dominate the model’s decision, and have led to an entire research subfield on adversarial instances in vision. Such investigations are not yet as prominent in the NLP community, although see, e.g., Sproat and Jaitly (2016) and Arthur et al. (2016).

The ability to work with raw input data and to pick up correlations/biases, which humans cannot always manifest in explicit symbolic rules, is precisely the strength of DNNs as feature extractors. But given the often millions of parameters and large number of unstructured input values, it is difficult to avoid unexpected hidden cues. Real-world data with its enormous “sample space”, which is necessarily only sparsely reflected in a dataset, is hence particularly prone to this effect.

The immediate problem is that a system trained this way may not generalize appropriately to other situations. The longer-term problem is that, while we do not expect that DNNs will simulate human capabilities in a fine-grained way, there has to be some degree of comparability if they are ever to be capable of justifying or explaining their behavior. The Clever Hans effect refers to situations where we wrongly and prematurely attribute such human-like reasoning mechanisms to trained models, when more careful and systematic investigations would have revealed our misjudgement. We can conclude from this that we need to supplement existing datasets with data where the relationship between text and image is straightforwardly and explicitly available to the experimenter.

2.3 Deep neural networks are universal approximators

It has long been known that DNNs are universal approximators, able to fit every (well-behaved) function if appropriately configured. Recent work by Zhang et al. (2017) demonstrated how powerful common network architectures are in approximating mere noise. Furthermore, their experiments indicate that fitting noise is not more difficult than fitting meaningful data for DNNs. The only discriminating effect is that the latter model generalizes to new data, while the former does not.¹ The ability of DNNs to fit hidden correlations should consequently not be underestimated. We conclude from this that, ideally, datasets should be big enough to avoid having to repeatedly use instances at all, whether during training or evaluation, particularly in the case of huge, but sparsely covered sample spaces. In this respect, the VQA dataset is too small and complex to provide the means for a clear and detailed evaluation.

Shallower machine learning methods are less prone to uncover hidden correlations for fitting data more efficiently, since their more restrictive structure imposed by the underlying model as well as in the input/output format likely makes it more difficult to incorporate them properly. The optimization is hence sufficiently constrained such that evaluations based on abstract artificial data are less interesting, even trivial and prone to overfitting. The situation seems reversed in the case of DNNs with their huge parameter space, comparatively unrestricted and highly nonlinear optimization on raw input/output data. Here, models do well at extremely difficult tasks just by end-to-end training on enough data points, while more detailed investigations find that they, unexpectedly, struggle even with simple abstract abilities like counting or spatial relations (Jabri et al., 2016). We hence do not share the scepticism about artificial data, particularly language data, being too trivial to be interesting for the evaluation of DNNs.

2.4 Three guiding principles for deep learning evaluation

We propose three simple and principled ways of reducing the risk of encountering such problems:

- Avoid training for multiple epochs: do not iterate over a fixed set of instances, since this makes it possible for the system to memorize hidden artifacts in the data.
- Instead of keeping training and test data distributions similar, focus on the true, compositional generalization abilities required by dissimilar distributions.²
- Do at least some experiments with clean data, which reduces the likelihood of hidden biases or correlations compared to more “realistic” and complex data. For instance, the relationship between image and text should be explicitly controlled in multimodal data for tasks like VQA.

¹Or rather, the structure of the data for which it would generalize is not obvious.

²A more asymmetric dataset represents a harder, but hence potentially more interesting task.



```
size: 64, color: {name: black, rgb: (0,0,0), shade: 0.0}, noise-range: 0.1, entities:
[ { id: 0, shape: {name: cross, extent: {x: 0.10, y: 0.10}}, color: {name: yellow, rgb: (1,1,0), shade: -0.24}, center: {x: 0.47, y: 0.28}, rotation: 0.06 },
  { id: 1, shape: {name: cross, extent: {x: 0.08, y: 0.08}}, color: {name: red, rgb: (1,0,0), shade: 0.26}, center: {x: 0.49, y: 0.65}, rotation: 0.76 },
  { id: 2, shape: {name: pentagon, extent: {x: 0.09, y: 0.08}}, color: {name: yellow, rgb: (1,1,0), shade: -0.16}, center: {x: 0.15, y: 0.91}, rotation: 0.27 },
  { id: 3, shape: {name: circle, extent: {x: 0.12, y: 0.12}}, color: {name: red, rgb: (1,0,0), shade: -0.12}, center: {x: 0.80, y: 0.37}, rotation: 0.53 },
  { id: 4, shape: {name: cross, extent: {x: 0.09, y: 0.09}}, color: {name: yellow, rgb: (1,1,0), shade: -0.42}, center: {x: 0.92, y: 0.73}, rotation: 0.73 } ]
```

Figure 1: A randomly sampled abstract ShapeWorld model and its visualization.

3 Automatic generation of artificial data using deep linguistic systems

In the following, we describe our approach for automatic generation of artificial VQA data using existing deep linguistic processing technology. We argue that a compositional semantic approach using a bidirectional grammar gives us precisely the sort of data required by the principles in section 2.4. We propose this approach as a complementary evaluation step, since it is not intended to replace real-world evaluation, but instead aims to cover aspects of evaluation which existing datasets cannot provide.

3.1 Abstract microworlds

The generation process we use is based on randomly sampled abstract world models, i.e. values which specify the microworld, entities and all their attributes. In the case of our ShapeWorld framework (Kuhnle and Copestake, 2017) — see figure 1 for an example — these include the number of entities, their shape and color, position, rotation, shade, etc. Such a world model can be visualized straightforwardly.

In this context, datasets are generators which can create an unlimited amount of data instances, hence making multiple iterations over a fixed set of training instances obsolete. Importantly, different datasets constrain this general sampling process in different ways by, for instance, restricting the number of objects, the attribute values available, the global positioning of entities, and more. This addresses the point of specifying different data distributions for training and testing. Moreover, it makes it possible to partition evaluation instances as desired, which facilitates the detailed investigation of a system’s behavior for specific instance types, and consequently the discovery of systematic shortcomings.

3.2 Controlled and syntactically rich language generation

Of the recent abstract datasets mentioned in the introduction, Suhr et al. (2017) use human-written captions, the SHAPES dataset (Andreas et al., 2016) a minimalist grammar, and the CLEVR dataset (Johnson et al., 2017a) a more complex one based on functional building blocks, both specifically designed for their microworlds. For the ShapeWorld framework, we decided that we will use technology made available by the DELPH-IN consortium. In particular, we wanted to make use of the broad-coverage, bidirectional³, high-precision English Resource Grammar (Flickinger, 2000). This and other DELPH-IN grammars, available for a range of languages, share the compositional semantic framework of Minimal Recursion Semantics (MRS, Copestake et al. (2005)). For our system we use a variant of MRS, Dependency MRS (DMRS, Copestake (2009), Copestake et al. (2016)), and generate natural language sentences from abstract DMRS graphs using Packard’s parser-generator ACE⁴.

We have found that DMRS graphs can easily be enriched with appropriate *ShapeWorld semantics* to be evaluated on a given world model. This means that the internals of the language system are essentially using a form of model-theoretic semantics. However, the external presentation of our task is still natural, i.e. only consisting of image and natural language. A compositional representation like DMRS further gives us the ability to produce an infinite number of utterances of arbitrary syntactic complexity.

Figure 2 shows an example of a non-trivial caption with corresponding DMRS graph and logical representation over a world model. Both the abstractness and compositionality of the semantic representation are essential to allow us to scale beyond toy examples. The abstract scenario of ShapeWorld puts an emphasis on experiments with closed-class vocabulary and syntax, as compared to the open-

³The ability to parse generated utterances is also potentially important, for instance in investigating ambiguity effects.

⁴<http://sweaglesw.org/linguistics/ace/>

A pentagon is above a green ellipse, and no green shape is an ellipse.

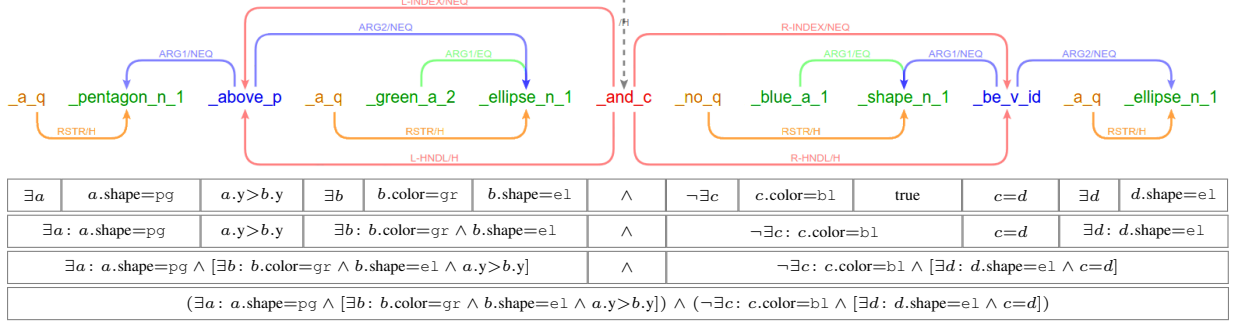


Figure 2: A caption with DMRS graph and semantic interpretation, illustrating how compositionality enables us to generate combinatorially large amounts of non-trivial captions from few atomic elements.

class dominated real-world datasets. However, the same approach could be extended to more complex domains, like the clip-art setting of Zitnick et al. (2016).

In the future, we plan to implement two interesting extensions for the ShapeWorld framework: On the one hand, paraphrase rules can be expressed on grammar-level and integrated into the generation process as post-processing step for increased linguistic variety. On the other hand, bidirectional (D)MRS-based grammars for other languages, such as the JACY grammar for Japanese (Siegel et al., 2016), could be used simply by translating the internal mapping of atomic DMRS components to corresponding ShapeWorld-semantic elements.

4 Conclusion: Why use generated artificial data?

Modularity Not only can the caption components be used in a compositional way, but also different constraint sets for the world model sampling process can be re-combined with different captioning modules. For instance, quantification and spatial relation statements both can use a world generator creating worlds containing multiple entities. All components can further be combined in mixer modules, for example a combined quantification and spatial relation captioner module.

Flexibility & reusability Real-world or human-created data essentially has to be obtained again for every change/update (Goyal et al., 2016)⁵. In contrast to that, modularity and detailed configurability makes our approach easily reusable for a wide range of potentially unforeseen changes in evaluation focus (or more general usage shifts).

Challenging data The interplay of abstract world model and semantic language representation enables us to generate captions requiring non-trivial multimodal reasoning. In fact, the resulting captions can be more complex than the sort of captions we could plausibly obtain from humans, and do not suffer from a Zipfian tendency to simplicity on average (although we could generate based on Zipfian distributions if that were desirable).

Avoid Clever Hans effect The simple, abstract domain and the controlled generation process based on randomly sampling microworlds makes such data comparatively unbiased and greatly reduces the possibility of hidden complex correlations. We can be confident that we cover the data space both relatively uniformly and much more exhaustively than this is the case in real-world datasets.

Rich evaluation Ultimately, our goal in providing datasets is to enable detailed evaluations of DNNs. By creating atomic test datasets specifically evaluating instance types individually (e.g., counting, spatial relations, or even more fine-grained), we can unit-test a DNN for specific subtasks. We believe that such a modular approach is a better way to establish trust in the understanding abilities of DNNs than a monolithic dataset and a single accuracy number to assess performance.

⁵Another interesting approach is to automatically process data afterwards (Hodosh and Hockenmaier, 2016; Shekhar et al., 2017), resulting in a form of “lightly” artificial data.

References

- Adi, Y., E. Kermany, Y. Belinkov, O. Lavi, and Y. Goldberg (2017). Fine-grained analysis of sentence embeddings using auxiliary prediction tasks. *Proceedings of the International Conference on Learning Representations 2017 (ICLR 2017)*.
- Agrawal, A., D. Batra, and D. Parikh (2016). Analyzing the behavior of visual question answering models. In *Proceedings of the 2016 Conference on Empirical Methods in Natural Language Processing, EMNLP 2016*, Austin, Texas, pp. 1955–1960.
- Andreas, J., M. Rohrbach, T. Darrell, and D. Klein (2016). Neural module networks. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2016*.
- Antol, S., A. Agrawal, J. Lu, M. Mitchell, D. Batra, C. L. Zitnick, and D. Parikh (2015). VQA: Visual question answering. In *Proceedings of the IEEE International Conference on Computer Vision, ICCV 2015*.
- Arthur, P., G. Neubig, and S. Nakamura (2016). Incorporating discrete translation lexicons into neural machine translation. In *Conference on Empirical Methods in Natural Language Processing (EMNLP)*, Austin, Texas, USA.
- Bellemare, M. G., Y. Naddaf, J. Veness, and M. Bowling (2013). The arcade learning environment: An evaluation platform for general agents. *Journal of Artificial Intelligence Research* 47(1), 253–279.
- Brockman, G., V. Cheung, L. Pettersson, J. Schneider, J. Schulman, J. Tang, and W. Zaremba (2016). OpenAI Gym.
- Copestake, A. (2009). Slacker semantics: Why superficiality, dependency and avoidance of commitment can be the right way to go. In *Proceedings of the 12th Meeting of the European Chapter of the Association for Computational Linguistics*, Athens, Greece, pp. 1–9.
- Copestake, A., G. Emerson, M. W. Goodman, M. Horvat, A. Kuhnle, and E. Muszyńska (2016). Resources for building applications with Dependency Minimal Recursion Semantics. In *Proceedings of the 10th International Conference on Language Resources and Evaluation (LREC-16)*, Portorož, Slovenia, pp. 1240–1247. European Language Resources Association (ELRA).
- Copestake, A., D. Flickinger, C. Pollard, and I. A. Sag (2005). Minimal Recursion Semantics: An introduction. *Research on Language and Computation* 3(4), 281–332.
- Flickinger, D. (2000). On building a more efficient grammar by exploiting types. *Natural Language Engineering* 6(1), 15–28.
- Goyal, Y., T. Khot, D. Summers-Stay, D. Batra, and D. Parikh (2016). Making the V in VQA matter: Elevating the role of image understanding in Visual Question Answering. *CoRR abs/1612.00837*.
- Hodosh, M. and J. Hockenmaier (2016). Focused evaluation for image description with binary forced-choice tasks. In *Proceedings of the 5th Workshop on Vision and Language*, Berlin, Germany.
- Hu, R., J. Andreas, M. Rohrbach, T. Darrell, and K. Saenko (2017). Learning to reason: End-to-end module networks for visual question answering. *ArXiv e-prints*.
- Jabri, A., A. Joulin, and L. van der Maaten (2016). *Revisiting Visual Question Answering Baselines*, pp. 727–739. Cham: Springer International Publishing.
- Johnson, J., B. Hariharan, L. van der Maaten, L. Fei-Fei, C. L. Zitnick, and R. Girshick (2017a). CLEVR: A diagnostic dataset for compositional language and elementary visual reasoning. In *CVPR*.

- Johnson, J., B. Hariharan, L. van der Maaten, L. Fei-Fei, C. L. Zitnick, and R. Girshick (2017b). CLEVR: A diagnostic dataset for compositional language and elementary visual reasoning. In *Computer Vision and Pattern Recognition (CVPR)*.
- Kiela, D., L. Bulat, A. L. Vero, and S. Clark (2016). Virtual embodiment: A scalable long-term strategy for artificial intelligence research. *CoRR abs/1610.07432*.
- Kuhnle, A. and A. Copestake (2017). Shapeworld - A new test methodology for multimodal language understanding. *ArXiv e-prints*.
- Lin, T.-Y., M. Maire, S. Belongie, J. Hays, P. Perona, D. Ramanan, P. Dollár, and C. L. Zitnick (2014). Microsoft COCO: Common objects in context. In *European Conference on Computer Vision (ECCV)*, Zürich.
- Mahendru, A., V. Prabhu, A. Mohapatra, D. Batra, and S. Lee (2017). The promise of premise: Harnessing question premises in visual question answering. *ArXiv e-prints*.
- Mikolov, T., A. Joulin, and M. Baroni (2015). A roadmap towards machine intelligence. *CoRR abs/1511.08130*.
- Nguyen, A., J. Yosinski, and J. Clune (2015). Deep neural networks are easily fooled: High confidence predictions for unrecognizable images. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2015*.
- Pinto, N., D. D. Cox, and J. J. DiCarlo (2008). Why is real-world visual object recognition hard? *PLOS Computational Biology* 4(1), 1–6.
- Scheffler, K. and S. Young (2001). Corpus-based dialogue simulation for automatic strategy learning and evaluation. In *Proceedings of the NAACL Workshop on Adaptation in Dialogue Systems*, pp. 64–70.
- Shekhar, R., S. Pezzelle, Y. Klimovich, A. Herbelot, M. Nabi, E. Sangineto, and R. Bernardi (2017). FOIL it! Find one mismatch between image and language caption. *ArXiv e-prints*.
- Siegel, M., E. M. Bender, and F. Bond (2016). *Jacy: An Implemented Grammar of Japanese*. CSLI Studies in Computational Linguistics. Stanford: CSLI Publications.
- Sproat, R. and N. Jaitly (2016). RNN Approaches to Text Normalization: A Challenge. *CoRR abs/1611.00068*.
- Sturm, B. L. (2014). A simple method to determine if a music information retrieval system is a “horse”. *IEEE Transactions on Multimedia* 16(6), 1636–1644.
- Suhr, A., M. Lewis, J. Yeh, and Y. Artzi (2017). A corpus of natural language for visual reasoning. In *55th Annual Meeting of the Association for Computational Linguistics, ACL 2017, Vancouver, Canada*. Association for Computational Linguistics.
- Sukhbaatar, S., A. Szlam, G. Synnaeve, S. Chintala, and R. Fergus (2015). MazeBase: A sandbox for learning from games. *CoRR abs/1511.07401*.
- Szegedy, C., W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. J. Goodfellow, and R. Fergus (2014). Intriguing properties of neural networks. *CoRR abs/1312.6199*.
- Weston, J., A. Bordes, S. Chopra, and T. Mikolov (2015). Towards AI-complete question answering: A set of prerequisite toy tasks. *CoRR abs/1502.05698*.
- Zhang, C., S. Bengio, M. Hardt, B. Recht, and O. Vinyals (2017). Understanding deep learning requires rethinking generalization. *International Conference on Learning Representations 2017 (ICLR 2017)*.
- Zitnick, C. L., R. Vedantam, and D. Parikh (2016). Adopting abstract images for semantic scene understanding. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 38(4), 627–638.