ACKNOWLEDGEMENTS

I would like to thank the following people who played important roles along different dimensions of my life as a PhD student.

First of all, I am deeply thankful to my PhD advisor, Dhruv Batra. When I applied for the PhD program, I was just excited to do computer vision research, but did not have enough knowledge of machine learning. Thank you for accepting me as your student in the first place! Thank you for your constant guidance, support and encouragement since then – be it explaining a concept patiently multiple times till I finally get a hold of it, be it reading and providing elaborate comments on paper / research statement drafts so that it does not just make the current draft better, but also teaches me how to write in general, be it giving me ample freedom and time to explore what I want to do next, be it providing encouraging comments on my successes as well as failures, be it standing up for me! You have always guided me to seek to the best and push beyond what seems achievable. You have cared about me not just as your student but as your kid! Thank you for shaping my career, my life!

Similarly, I am immensely grateful to Devi Parikh, who I not just collaborated with during almost my entire PhD, but also reached out to seek solutions to various problems of my work life (both research related and otherwise). And surprisingly, Devi always had a solution! Your quick and useful replies, no matter how busy you are, your staying up till late night (even when you were not planning to!) to provide feedback on paper drafts, your getting excited when we (your students) are giving talks, your being considerate of everyone’s feelings – all these make me admire you a lot! You have not only shaped my research, but also my thinking, my outlook towards life! Thank you for giving me an opportunity to be a part of your life!
I would also like to thank Larry Zitnick for being a wonderful collaborator and mentor. I have always been awed by your data visualization skills (!) and creative thinking in general. Thank you for helping shape my research and for providing useful advice at critical points of my PhD career!

I am also thankful to Oriol Vinyals for engaging in very informative brainstorming sessions with me while I was an intern at DeepMind, for agreeing to be a part of my PhD committee and providing useful feedback on my thesis, and for providing useful advice about life in general!

I would also like to thank James Hays for agreeing to be a part of my PhD committee and providing useful feedback about future directions of my PhD research!

During my PhD, I had the opportunity to intern at a few amazing places in the world. I am grateful to all my internship mentors and collaborators for providing me one of the best experiences of my PhD and for teaching me so much, both about work and life – Margaret Mitchell, Xiaodong He, Aniruddha Kembhavi, Tejas Kulkarni, Mateusz Malinowski, Felix Hill, Ali Eslami, and Jianfeng Gao.

One person who turned out to be like an angel in my life when I started my grad school was my labmate Stanislaw Antol. Stan and I collaborated on two research projects (the first two projects of my PhD). Stan being part of those projects was immensely helpful to me. He helped me with every little thing— from how to run jobs on cluster to how to write good code, from how to setup mechanical turk experiments to how to make sure the incoming data is good. In addition to helping me get settled in a new work environment, he was always helpful outside work too. I still miss his cookies, the hiking trips and Thanksgiving dinner with him. Thank you for all your kindness and support!

I am also immensely thankful to Jiasen Lu, Gordon Christie, Ankit Laddha, Akrit Mohapatra, and Sainandan Ramakrishnan, who I had the pleasure to work closely with and learn a lot from. Thank you for being such wonderful collaborators!
I would like to express my deep gratitude towards my colleagues-cum-friends – Stefan Lee, Ramakrishna Vedantam, Arjun Chandrasekaran, Abhishek Das, Harsh Agrawal, Ramprasaath Selvaraju, and Ashwin Kalyan, who acted as mentors by providing useful advice during critical times, as well as acted as family by filling my life with fun and sweet memories! Thank you for all your support!

I would like to thank all the past and present members of the CVMLP group for making my PhD journey so wonderful and unforgettable – Neelima Chavali, Qing Sun, Michael Cogswell, Xiao Lin, Peng Zhang, Shrenik Lad, Jianwei Yang, Nirbhay Modhe, Samyak Datta, Deshraj Yadav, Viraj Prabhu, Prithvijit Chattopadhyay, Karan Desai, Rishabh Jain, Sanyam Agrawal, Ayush Shrivastava, Mohit Sharma, Purva Tendulkar, Erik Wijmans, Peter Anderson, Zhile Ren, Faruk Ahmed, Clint Solomon, Arijit Ray, Aroma Mahendru, Latha Pemula, Tejas Khot, Khushi Gupta, Avi Singh, Ahmed Osman, Senthil Purushwalkam, Varun Manjunatha, Mayu Sakurada, and Tanmay Batra. It is an honor for me that I got to be a part of the CVMLP group.

I am deeply grateful to my parents Indu Agrawal and Sanjay Agrawal for sacrificing comforts of their life so that they could provide me the best possible education, for letting me follow my dreams even if that meant being thousands of miles away from their only child, for understanding my life choices and being happy about them, for everything! This PhD would not have been possible if you were not this understanding and supportive!

One person who has always believed in me and helped me emotionally, mentally, as well as intellectually is my partner-cum-colleague Yash Goyal. I admire your empathetic nature, I admire your ability to see and show me the positive side of most of the negative-seeming situations of my life. Thank you for being with me during the highs and lows of my life. Thank you for your constant support and encouragement. My PhD would not be a success if it were not for you!
# TABLE OF CONTENTS

ACKNOWLEDGEMENTS ....................................................... iii

LIST OF TABLES ............................................................... ix

LIST OF FIGURES ............................................................. xi

SUMMARY ........................................................................ xx

I INTRODUCTION ................................................................. 1

  1.1 Free-form and Open-Ended VQA (chapter 3) ....................... 2
  1.2 Analyzing the Behavior of VQA Models (chapter 4) ............. 3
  1.3 Overcoming Priors in VQA (chapter 5) ............................. 4
  1.4 Contributions ............................................................. 5
  1.5 List of Publications ..................................................... 6

II RELATED WORK ............................................................. 8

  2.1 Visual Question Answering (VQA) ................................... 8
  2.2 Analyzing the Behavior of VQA Models ........................... 10
  2.3 Overcoming Priors in VQA ........................................... 11

III VISUAL QUESTION ANSWERING (VQA) ......................... 14

  3.1 Introduction ............................................................. 14
  3.2 VQA Dataset Collection .............................................. 17
  3.3 VQA Dataset Analysis ................................................ 22
      3.3.1 Questions ......................................................... 23
      3.3.2 Answers .......................................................... 24
      3.3.3 Commonsense Knowledge .................................... 28
      3.3.4 Captions *vs.* Questions ...................................... 29
  3.4 VQA Baselines and Methods ........................................ 30
      3.4.1 Baselines .......................................................... 30
      3.4.2 Methods ........................................................... 31
      3.4.3 Results ............................................................ 34
3.5 VQA Challenge and Workshop ........................................... 41
3.6 Conclusion and Discussion ............................................. 42

IV ANALYZING THE BEHAVIOR OF VISUAL QUESTION ANSWERING MODELS ........................................... 44
4.1 Introduction ............................................................... 44
4.2 Behavior Analyses ...................................................... 44
4.2.1 Generalization to novel instances .............................. 46
4.2.2 Complete question understanding .............................. 48
4.2.3 Complete image understanding ................................. 50
4.3 Conclusion ............................................................... 52

V OVERCOMING PRIORS IN VISUAL QUESTION ANSWERING 54
5.1 Visual Question Answering under Changing Priors (VQA-CP) .................................................. 54
5.1.1 Introduction ........................................................... 54
5.1.2 VQA-CP: Dataset Creation and Analysis .................... 55
5.1.3 Benchmarking VQA Models on VQA-CP ................. 58
5.1.4 Conclusion ........................................................... 60
5.2 Grounded Visual Question Answering (GVQA) .................. 60
5.2.1 Introduction ........................................................... 60
5.2.2 GVQA model .......................................................... 61
5.2.3 Experiments on VQA-CP v1 and VQA-CP v2 ............. 66
5.2.4 Role of GVQA Components .................................... 67
5.2.5 Experiments on VQA v1 and VQA v2 ....................... 69
5.2.6 Transparency .......................................................... 71
5.2.7 Conclusion ........................................................... 73
5.3 Adversarial Regularization for Visual Question Answering ........ 73
5.3.1 Introduction ........................................................... 73
5.3.2 Reducing Language Bias Through Adversarial Regularization 75
5.3.3 Experiments ........................................................... 80
1 Test-standard accuracy of human subjects when asked to answer the question without seeing the image (Question), seeing just a caption of the image and not the image itself (Question + Caption), and seeing the image (Question + Image). Results are shown for all questions, “yes/no” & “number” questions, and other questions that are neither answered “yes/no” nor number. All answers are free-form and not multiple-choice. *These accuracies are evaluated on a subset of 3K train questions (1K images). .......................................................... 30

2 Accuracy of our methods for the open-ended and multiple-choice tasks on the VQA test-dev for real images. Q = Question, I = Image, C = Caption. (Caption and BoW Q + C results are on val). See text for details. .......................................................... 34

3 Open-ended test-dev results for different question types on real images (Q+C is reported on val). Machine performance is reported using the bag-of-words representation for questions. Questions types are determined by the one or two words that start the question. The percentage of questions for each type is shown in parentheses. Last and second last columns respectively show the average human age and average degree of commonsense required to answer the questions (as reported by AMT workers), respectively. See text for details. .......................................................... 36

4 Accuracy of ablated versions of our best model (deeper LSTM Q + norm I) for the open-ended and multiple-choice tasks on the VQA test-dev for real images. Q = Question, I = Image. See text for details. .......................................................... 41

5 Test-standard accuracy of our best model (deeper LSTM Q + norm I) compared to test-standard accuracies of other entries for the open-ended and multiple-choice tasks in the respective VQA Real Image Challenge leaderboards (as of October 28, 2016). .......................................................... 42

6 We compare the performance of existing VQA models on VQA-CP v1 test splits (when trained on VQA-CP v1 train splits) to their performance on VQA v1 val splits (when trained on VQA v1 train splits). We find that the performance of all tested existing models degrades significantly in the new Changing Priors setting compared to the original VQA setting. .......................................................... 58
We compare the performance of existing VQA models on VQA-CP v2 test splits (when trained on VQA-CP v2 train splits) to their performance on VQA v2 val splits (when trained on VQA v2 train splits). We find that the performance of all tested existing models degrades significantly in the new Changing Priors setting compared to the original VQA setting.

Performance of GVQA (our model) compared to SAN on VQA-CP datasets. GVQA consistently outperforms SAN.

Experimental results when each component in GVQA (denoted by “-<component>”) is replaced with its corresponding traditional counterpart (denoted by “+<traditional counterpart>”).

Results of GVQA and SAN on VQA v1 and VQA v2 when trained on the corresponding train splits.

Performance on VQA-CP v2 test and VQA v2 val. We significantly improve the accuracy of base models and achieve state-of-the-art performance on the VQA-CP dataset.

Performance on VQA-CP v1 test and VQA v1 val.

For each of the two datasets, real and abstract, first two rows are the human accuracies for multiple-choice questions when subjects were shown both the image and the question. Majority vote means we consider the answer picked by majority of the three subjects to be the predicted answer by humans and compute accuracy of that answer for each question. Average means we compute the accuracy of each of the answers picked by the subjects and record their average for each question. The last row is the inter-human agreement for open-ended answers task when subjects were shown both the image and the question. All accuracies are evaluated on a random subset of 3000 questions.

Performance of SAN \(-Q_{full} + Q_{main}\) compared to SAN and GVQA (our model) on VQA-CP v2 dataset. GVQA outperforms both SAN and SAN \(-Q_{full} + Q_{main}\).

Results of GVQA, GVQA - VCC\(_{loss}\) and SAN on VQA v1 val split when trained on the VQA v1 train split. Please see text for more details.

Results of GVQA, GVQA - VCC\(_{loss}\) and SAN on VQA v2 val split when trained on the VQA v2 train split. Please see text for more details.
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Examples of free-form, open-ended questions in our VQA dataset.</td>
</tr>
<tr>
<td>2</td>
<td>This figure illustrates outputs from a baseline model (SAN [495]) and the proposed model (GVQA [12]). For the given test questions, SAN predicts the prior answers from the training data for the respective question types, resulting in incorrect answers. However, GVQA, being more visually grounded than SAN, correctly answers the test questions.</td>
</tr>
<tr>
<td>3</td>
<td>Examples of free-form, open-ended questions collected for images via Amazon Mechanical Turk. Note that commonsense knowledge is needed along with a visual understanding of the scene to answer many questions.</td>
</tr>
<tr>
<td>4</td>
<td>Examples of questions (black), (a subset of the) answers given when looking at the image (green), and answers given when not looking at the image (blue) for numerous representative examples of the dataset. See the appendix for more examples.</td>
</tr>
<tr>
<td>5</td>
<td>Distribution of questions by their first four words for a random sample of 60K questions for real images (left) and all questions for abstract scenes (right). The ordering of the words starts towards the center and radiates outwards. The arc length is proportional to the number of questions containing the word. White areas are words with contributions too small to show.</td>
</tr>
<tr>
<td>6</td>
<td>Percentage of questions with different word lengths for real images and abstract scenes.</td>
</tr>
<tr>
<td>7</td>
<td>Distribution of answers per question type for a random sample of 60K questions for real images when subjects provide answers when given the image (top) and when not given the image (bottom).</td>
</tr>
<tr>
<td>8</td>
<td>Number of questions per average confidence score (0 = not confident, 1 = confident) for real images and abstract scenes (black lines). Percentage of questions where 7 or more answers are same, 3-7 are same, less than 3 are same (color bars).</td>
</tr>
<tr>
<td>9</td>
<td>Example questions judged by Mturk workers to be answerable by different age groups. The percentage of questions falling into each age group is shown in parentheses.</td>
</tr>
</tbody>
</table>
Our best performing model (deeper LSTM Q + norm I). This model uses a two layer LSTM to encode the questions and the last hidden layer of VGGNet [408] to encode the images. The image features are then $l_2$ normalized. Both the question and image features are transformed to a common space and fused via element-wise multiplication, which is then passed through a fully connected layer followed by a softmax layer to obtain a distribution over answers.

Pr (system is correct | answer) for 50 most frequent ground truth answers on the VQA validation set (plot is sorted by accuracy, not frequency). System refers to our best model (deeper LSTM Q + norm I).

Pr (answer | system is correct) for 50 most frequently predicted answers on the VQA validation set (plot is sorted by prediction frequency, not accuracy). System refers to our best model (deeper LSTM Q + norm I).

Pr (system is correct | age of question) on the VQA validation set. System refers to our best model (deeper LSTM Q + norm I).

Pr (age of question | system is correct) on the VQA validation set. System refers to our best model (deeper LSTM Q + norm I).

Leaderboard showing test-standard accuracies for VQA Real Image Challenge (Open-Ended) on left and leaderboard showing test-standard accuracies for VQA Real Image Challenge (Multiple-Choice) on right (snapshot from October 28, 2016).

Examples from test set where the CNN+LSTM model makes mistakes and their corresponding nearest neighbor training instances. See appendix for more examples.

X-axis shows length of partial question (in %) fed as input. Y-axis shows percentage of questions for which responses of these partial questions are the same as full questions and VQA accuracy of partial questions.

Examples where the CNN+LSTM model does not change its answer after first few question words. On doing so, it is correct for some cases (the extreme left example) and incorrect for other cases (the remaining three examples). See appendix for more examples.

Percentage of questions for which responses remain same (compared to entire question) as a function of POS tags dropped from the question.
20 Histogram of percentage of images for which model produces same answer for a given question and its comparison with test accuracy. The cumulative plot shows the % of questions for which model produces same answer for *at least* x % of images. .......................... 52

21 Examples where the predicted answers do not change across images for a given question. See appendix for more examples. .......................... 52

22 Distribution of answers per question type vary significantly between VQA-CP v1 train (left) and test (right) splits. For instance, ‘white’ and ‘red’ are commonly seen answers in train for ‘What color’, where as ‘black’ is the most frequent answer in test. These have been computed for a random sample of 60K questions. .......................... 57

23 The proposed Grounded Visual Question Answering (GVQA) model. 62

24 Qualitative examples from GVQA. **Left:** We show top three answer cluster predictions (along with random concepts from each cluster) by ACP. Corresponding to each cluster predicted by ACP, we show the top visual concept predicted by VCC. Given these ACP and VCC predictions, the Answer Predictor (AP) predicts the correct answer ‘*baseball*’. **Right:** Smiling is the concept extracted by the CE whose visual presence in VCC’s predictions is verified by the Visual Verifier, resulting in ‘*yes*’ as the final answer. .......................... 71

25 **Left:** GVQA’s prediction (‘green’) can be explained as follows – ACP predicts that the answer should be a *color*. Of the various visual concepts predicted by VCC, the only concept that is about color is *green*. Hence, GVQA’s output is ‘green’. SAN incorrectly predicts ‘*yellow*’. SAN’s architecture doesn’t facilitate producing an explanation of why it predicted what it predicted, unlike GVQA. **Right:** Both GVQA and SAN incorrectly answer the question. GVQA is incorrect perhaps because VCC predicts ‘black’, instead of ‘gray’. In order to dig further into why VCC’s prediction is incorrect, we can look at the attention map (in appendix), which shows that the attention is on the pants for the person’s left leg, but on the socks (black in color) for the person’s right leg. So, perhaps, VCC’s ‘*black*’ prediction is based on the attention on the person’s right leg. .......................... 72
Given an arbitrary base VQA model (A), we introduce two regularizers. First, we build a question-only adversary (B) that takes the question embedding $q_i$ from the VQA model and is trained to output the correct answer from this information alone. For this network to succeed, $q_i$ must capture language biases from the dataset – the same biases that lead the base VQA model to ignore visual content. To reduce these biases, we set the base VQA model and the question-only adversary against each other, with the base VQA network modifying its question embedding to reduce question-only performance (shown here as gradient negation of the question-only model loss). Further, the question-only model allows estimation of the change in answer confidence given image (C), which we maximize explicitly.

Maximizing difference of entropies (DoE) along with the question-only adversarial regularization for the SAN model, not only improves results on changing priors, but also stabilizes training.

Answer distribution for SAN+Q-Adv+DoE mimic the prior less for questions with high language bias.

The table-top setup and an example dialog from the SHRDLU [477] project (studied by Terry Winograd in 1972).

Given an instruction (‘There is a small sphere’), the task for an agent is to execute actions to create scenes that are consistent with the given instruction (i.e., each such scene consists of a small sphere).

Proportions of spatial prepositions in the captions and question & answers for real images (left) and abstract scenes (right).

Venn-style word clouds [100] for nouns with size indicating the normalized count for real images.

Venn-style word clouds [100] for verbs with size indicating the normalized count for real images.

Venn-style word clouds [100] for adjectives with size indicating the normalized count for real images.

Venn-style word clouds [100] for nouns with size indicating the normalized count for abstract scenes.

Venn-style word clouds [100] for verbs with size indicating the normalized count for abstract scenes.

Venn-style word clouds [100] for adjectives with size indicating the normalized count for abstract scenes.
Distribution of questions starting with “What is” by their first five words for a random sample of 60K questions for real images (left) and all questions for abstract scenes (right). The ordering of the words starts towards the center and radiates outwards. The arc length is proportional to the number of questions containing the word. White areas are words with contributions too small to show.

Distribution of answers for questions starting with “What is” for a random sample of 60K questions for real images (top) and all questions for abstract scenes (bottom). Each column corresponds to questions ending in different words, such as “doing?” “on?” etc.

Left: A small subset of the objects present in the abstract scene dataset. Right: The AMT interface for collecting abstract scenes. The light green circles indicate where users can select to manipulate a person’s pose. Different objects may be added to the scene using the folders to the right.

Our AMT interface for collecting the third question for an image, when subjects were shown previous questions that were collected and were asked to ask a question different from previous questions.

The AMT interface used to collect answers to a question when subjects were shown the image while answering the question.

The AMT interface used to collect answers to a question when subjects were not shown the image while answering the question using only commonsense to collect the plausible, but incorrect, multiple-choice answers.

Random examples of questions (black), (a subset of the) answers given when looking at the image (green), and answers given when not looking at the image (blue) for numerous representative examples of the real image dataset.

Random examples of questions (black), (a subset of the) answers given when looking at the image (green), and answers given when not looking at the image (blue) for numerous representative examples of the abstract scene dataset.

Random examples of multiple-choice questions for numerous representative examples of the real and abstract scene dataset.

Test accuracy vs. average distance of the test points from k-NN training points for the CNN+LSTM model.

Test QI pairs for which the CNN+LSTM model produces the correct response and their nearest neighbor QI pairs from training set.
Test QI pairs for which the CNN+LSTM model produces incorrect response and their nearest neighbor QI pairs from training set.

X-axis shows length of partial “yes/no” question (in %) fed as input. Y-axis shows percentage of “yes/no” questions for which responses of these partial “yes/no” questions are the same as full “yes/no” questions and VQA accuracy of partial “yes/no” questions.

X-axis shows length of partial “number” question (in %) fed as input. Y-axis shows percentage of “number” questions for which responses of these partial “number” questions are the same as full “number” questions and VQA accuracy of partial “number” questions.

X-axis shows length of partial “other” question (in %) fed as input. Y-axis shows percentage of “other” questions for which responses of these partial “other” questions are the same as full “other” questions and VQA accuracy of partial “other” questions.

Percentage of “yes/no” questions for which responses remain same (compared to entire “yes/no” question) as a function of POS tags dropped from the “yes/no” question.

Percentage of “number” questions for which responses remain same (compared to entire “number” question) as a function of POS tags dropped from the “number” question.

Percentage of “other” questions for which responses remain same (compared to entire “other” question) as a function of POS tags dropped from the “other” question.

Examples where the CNN+LSTM model converges on a predicted answer without listening to the entire question.

Histogram of percentage of images for which model produces same answer for a given “yes/no” question. The cumulative plot shows the % of “yes/no” questions for which model produces same answer for atleast $x$ % of images.

Histogram of percentage of images for which model produces same answer for a given “number” question. The cumulative plot shows the % of “number” questions for which model produces same answer for atleast $x$ % of images.

Histogram of percentage of images for which model produces same answer for a given “other” question. The cumulative plot shows the % of “other” questions for which model produces same answer for atleast $x$ % of images.
Examples where the CNN+LSTM model produces the same answer for at least half the images for each of the questions shown above. “Q” denotes the question for which model produces same response for at least half the images, “A” denotes the answer predicted by the model (which is same for at least half the images), “Number of Images” denotes the number of images for which the question is repeated in the VQA validation set and “Average Accuracy” is the VQA accuracy for these QI pairs (with same question but different images).

Distribution of answers per question type vary significantly between VQA-CP v2 train (left) and test (right) splits. For instance, ‘white’ and ‘black’ are commonly seen answers in train for ‘What color’, where as ‘red’ is the most frequent answer in test. These have been computed for a random sample of 60K questions.

Performance of SAN and GVQA for different VQA-CP v2 splits. GVQA consistently outperforms SAN across all splits.

VCC’s attention map for the example shown in Fig. 25 (right).

Transparency of GVQA. For each of the above examples, GVQA’s intermediate predictions can help explain why it predicted what it predicted. Top-left: VCC predicts the following visual concepts – blue, person, skiing and jacket. ACP predicts the cluster corresponding to colors. Finally, GVQA predicts ‘blue’ as the answer. So, we can see why GVQA predicts ‘blue’ – because, of all the visual concepts predicted by VCC, only ‘blue’ represents a color. Looking at the attention maps can further indicate why GVQA is “seeing” blue (because it is “looking” at the jacket as well, unlike SAN which is only “looking” at the pants). SAN’s prediction is ‘orange’ and unlike GVQA, SAN’s architecture does not facilitate producing such an explanation, which makes it difficult to understand why it is saying what it is saying. Top-right: Both GVQA and SAN are “looking” at the regions covered with snow, but GVQA correctly predicts ‘winter’, whereas SAN incorrectly predicts ‘summer’ which is unclear why. Bottom-left: The Concept Extractor (CE) predicts ‘happy’ whose visual presence is verified by VCC which is “looking” at the region corresponding to the kid’s face. Bottom-right: GVQA focuses on a larger part of the scene and correctly recognizes it as ‘bathroom’.
Transparency of GVQA. For the above examples, both GVQA and SAN incorrectly answer the question. However, GVQA’s intermediate predictions can help explain why it is incorrect. **Top-left:** For GVQA, VCC’s predictions indicate that it is perhaps “looking” at the field, which can be further verified by the attention map. SAN’s attention map suggests that it is “looking” at the ball but still does not explain why it is predicting ‘soccer’. Perhaps, it is confusing the ball with a soccer ball. **Top-right:** The attention maps from GVQA and SAN look similar to each other. However, looking at ACP’s and VCC’s prediction (for GVQA) suggest that it is indeed “seeing” ‘pasta’ (the correct answer), but still predicting ‘carrots’ because the ACP is incorrectly predicting the cluster corresponding to vegetables instead of the cluster corresponding to pasta. **Bottom:** GVQA is “looking” at the smartphone (unlike SAN), but yet incorrectly answers ‘no’, because the VCC does not recognize the phone as a smartphone. It however correctly predicts ‘phone’, ‘electronic’, ‘black’ and ‘right’. . . . . . . . . 133
Existing deep visual question answering models tend to rely on language correlations, but can be trained to resist these correlations via appropriate inductive biases and objective functions.
In this dissertation, I propose and study a multi-modal Artificial Intelligence (AI) task called Visual Question Answering (VQA) – given an image and a natural language question about the image (e.g., ‘What kind of store is this?’, ‘Is it safe to cross the street?’), the machine’s task is to automatically produce an accurate natural language answer (‘bakery’, ‘yes’). Applications of VQA include – aiding visually impaired users in understanding their surroundings, aiding analysts in examining large quantities of surveillance data, teaching children through interactive demos, interacting with personal AI assistants, and making visual social media content more accessible.

Specifically, I study the following – 1) how to create a large-scale dataset and define evaluation metrics for free-form and open-ended VQA, 2) how to develop techniques for characterizing the behavior of VQA models, and 3) how to build VQA models that are less driven by language biases in training data and are more visually grounded, by proposing – a) a new evaluation protocol, b) a new model architecture, and c) a novel objective function.

Most of my past work has been towards building agents that can ‘see’ and ‘talk’. However, for a lot of practical applications (e.g., physical agents navigating inside our houses executing natural language commands) we need agents that can not only ‘see’ and ‘talk’ but can also take actions. In chapter 6, I present future directions towards generalizing vision and language agents to be able to take actions.
CHAPTER I

INTRODUCTION

One of the goals of Artificial Intelligence (AI) is to develop systems that can ‘see’ (i.e. understand the contents of an image: who, what, where, doing what?) and ‘talk’ (i.e. communicate the understanding to humans in free-form natural language). Applications of such systems include:

- Aiding visually impaired users in understanding their surroundings (Human: ‘What is on the shelf above the microwave?’, AI: ‘Canned containers’),
- Aiding analysts in making decisions based on large quantities of surveillance data (Human: ‘What kind of car did the man in red shirt leave in?’, AI: ‘Blue Toyota Prius’),
- Teaching children through interactive demos (Kid: ‘What animal is that?’, AI: ‘That is Dall Sheep. You can find those in Alaska.’),
- Interacting with personal AI assistants (such as Alexa, Siri) (Human: ‘Is my laptop in my bedroom upstairs?’, AI: ‘Yes’, Human: ‘Is the charger plugged in?’),
- Making visual social media content more accessible (AI: ‘Your friend Bob just uploaded a picture from his Hawaii trip’, Human: ‘Great, is he at the beach?’, AI: ‘No, on a mountain’).

As a first step towards building machines that can convey their understanding of visual content via natural language, in this dissertation, I introduce and study open-ended and free-form Visual Question Answering (VQA) – Given an image and a natural language question about the image (e.g., ‘What kind of store is this?’, ‘How many people are waiting in the queue?’, ‘Is it safe to cross the street?’),
the machine’s task is to automatically produce an accurate natural language answer (‘bakery’, ‘5’, ‘yes’). Akin to a visual Turing test, answering any possible question about an image is one of the ‘holy grails’ of semantic understanding. VQA is directly applicable to a variety of applications of high societal impact that involve humans working in collaboration with machines to elicit and extract situationally-relevant information from visual data. Examples include aiding visually-impaired users in understanding their surroundings (‘What temperature is my oven set to?’), analysts in making decisions based on large quantities of surveillance data (‘What kind of car did the man in the red shirt drive away in?’), and users in interacting with a robot (‘Is my laptop in my bedroom upstairs?’). This research has the potential to fundamentally improve the way visually-impaired users live their daily lives, and revolutionize how society at large interacts with ever-growing visual data.

I provide below an overview of the specific dimensions of VQA that I study in this dissertation.

1.1 Free-form and Open-Ended VQA (chapter 3)

My colleagues and I introduced the task of free-form and open-ended VQA [27, 18]. In order to train and benchmark algorithms on the task of free-form and open-ended VQA, we collect and analyze a large scale dataset (>0.25M images, >0.76M questions, ~10M answers) [27, 18]. The questions and answers in the dataset are provided by human workers on Amazon Mechanical Turk, on top of existing images [269, 516]. Unlike existing computer vision tasks which either represent single narrowly-defined problem (e.g., image classification, activity recognition), or are difficult to evaluate (e.g., image captioning), the questions in our VQA dataset require a potentially vast set of AI capabilities to answer (Fig. 3) – fine-grained recognition (e.g., ‘What kind of cheese is on the pizza?’), object detection (e.g., ‘How many bikes are there?’), and commonsense (e.g., ‘Does this person have 20/20 vision?’). Moreover, VQA
is amenable to automatic evaluation, since many open-ended answers contain only a few words or a closed set of answers that can be provided in a multiple-choice format. We also develop and present experimental results of some baselines and methods for VQA. Finally, in order to push the state-of-the-art (SOTA) on VQA, we organize annual challenges and workshops on VQA and discuss the how these challenges and workshops improved the SOTA on VQA and benefitted the language and vision community in general.

1.2 Analyzing the Behavior of VQA Models (chapter 4)

After the release of our VQA dataset, a number of deep-learning models were proposed for VQA [27, 84, 495, 485, 208, 24, 465, 217, 280, 25, 400, 227, 150, 321, 197, 480, 483, 510, 381]. Curiously, the performance of most methods was clustered around 60-70% (compared to human performance of 83%) with a mere 5% gap between the top-9 entries on the VQA Challenge 2016. In order to identify the most fruitful directions for progress, we develop novel techniques for characterizing the behavior of VQA models [9]. We analyze several representative state-of-the-art VQA models [27, 280, 150], including the models developed by us [27] and present three novel findings that expand our understanding of VQA models – despite the progress, the VQA models are ‘myopic’ (tend to fail on sufficiently novel instances), often ‘jump
Figure 2: This figure illustrates outputs from a baseline model (SAN [495]) and the proposed model (GVQA [12]). For the given test questions, SAN predicts the prior answers from the training data for the respective question types, resulting in incorrect answers. However, GVQA, being more visually grounded than SAN, correctly answers the test questions.

to conclusions’ (converge on a predicted answer after ‘listening’ to just half the question), and are ‘stubborn’ (do not change their answers across images).

1.3 Overcoming Priors in VQA (chapter 5)

Motivated by the findings of our previous work [9] (and work by others [505, 168, 211]) that VQA models are heavily driven by superficial correlations in the training data and lack sufficient image grounding and compositionality, we address some of these issues by proposing:

a) a new evaluation protocol (section 5.1). We propose a new evaluation protocol for VQA – train and test sets have different prior distributions of answers for different question types (first few words of the question) [12]. Specifically, we create a new split of the VQA dataset [27] – Visual Question Answering under Changing Priors (VQA-CP). We evaluate several existing VQA models on the new split and find that their performance degrades significantly compared to the original VQA split. Thus, the proposed split can serve as a benchmark to evaluate the degree of visual groundedness in VQA models.

b) a new model architecture (section 5.2). We propose a novel Grounded
Visual Question Answering (GVQA) model [12] that contains inductive biases and restrictions in the architecture specifically designed to prevent the model from ‘cheating’ by primarily relying on priors in the training data. Specifically, GVQA explicitly disentangles the recognition of visual concepts present in the image from the identification of plausible answer space for a given question, enabling the model to more robustly generalize across different distributions of answers. GVQA significantly out-performs the baseline VQA model (SAN) [495] on VQA-CP. Fig. 2 illustrates outputs from GVQA and SAN. For the given test questions, SAN predicts the prior answers from the training data for the respective question types, resulting in incorrect answers. However, GVQA, being more visually grounded than SAN, correctly answers the test questions.

c) a novel objective function (section 5.3). Although GVQA can be built on top of any existing VQA model, it does require non-trivial changes in the architecture. To address this issue, we propose a simple drop-in regularizer that can be added to any existing VQA model’s objective function [359]. To do this, we introduce a question-only model that takes the question encoding from the VQA model and must leverage language biases in order to succeed. We then pose training as an adversarial game between the VQA model and this question-only adversary – discouraging the VQA model from capturing language biases in its question encoding. This approach improves performance significantly for multiple base models (including GVQA), achieving state-of-the-art on VQA-CP.

1.4 Contributions

In this dissertation, we:

1. introduce the task of free-form and open-ended Visual Question Answering (VQA). We collect a large scale dataset (>0.25M images, >0.76M questions, ∼10M answers) and make it publicly available (www.visualqa.org). We present
baselines and methods for VQA, and organize annual challenges and workshops to push the state-of-art on VQA.

2. develop novel techniques to characterize the behavior of VQA models. We analyze several representative VQA models and present three novel findings that expand our understanding of VQA models.

3. address the issue of VQA models being driven by superficial correlations in training data and lacking sufficient image grounding by proposing:
   (a) a new evaluation protocol to evaluate the degree of visual groundedness in VQA models.
   (b) a novel Grounded VQA (GVQA) model that contains inductive biases and restrictions in the architecture specifically designed to prevent the model from ‘cheating’ by primarily relying on priors in the training data.
   (c) a novel adversarial regularization scheme that can be added to any existing VQA model’s objective function, without significantly changing the underlying VQA model’s architecture.

1.5 List of Publications


CHAPTER II

RELATED WORK

In this chapter, I will discuss how our work on Visual Question Answering (VQA) is related to other research efforts in similar directions. I will first discuss related work on VQA, then Analyzing the Behavior of VQA Models followed by Overcoming Priors in VQA.

2.1 Visual Question Answering (VQA)

VQA Efforts. Several recent papers have studied visual question answering [158, 286, 439, 51]. However, unlike our work, these are fairly restricted (sometimes synthetic) settings with small datasets. For instance, [286] only considers questions whose answers come from a predefined closed world of 16 basic colors or 894 object categories. [158] also considers questions generated from templates from a fixed vocabulary of objects, attributes, relationships between objects, etc. In contrast, our proposed task involves open-ended, free-form questions and answers provided by humans. Our goal is to increase the diversity of knowledge and kinds of reasoning needed to provide correct answers. Critical to achieving success on this more difficult and unconstrained task, our VQA dataset is two orders of magnitude larger than [158, 286] (>250,000 vs. 2,591 and 1,449 images respectively). The proposed VQA task has connections to other related work: [439] has studied joint parsing of videos and corresponding text to answer queries on two datasets containing 15 video clips each. [51] uses crowdsourced workers to answer questions about visual content asked by visually-impaired users. In concurrent work, [289] proposed combining an LSTM for the question with a CNN for the image to generate an answer. In their model, the LSTM question representation is conditioned on the CNN image features.
at each time step, and the final LSTM hidden state is used to sequentially decode the answer phrase. In contrast, the model developed by us explores “late fusion” – i.e., the LSTM question representation and the CNN image features are computed independently, fused via an element-wise multiplication, and then passed through fully-connected layers to generate a softmax distribution over output answer classes. [272] generates abstract scenes to capture visual common sense relevant to answering (purely textual) fill-in-the-blank and visual paraphrasing questions. [378] and [448] use visual information to assess the plausibility of common sense assertions. [499] introduced a dataset of 10k images and prompted captions that describe specific aspects of a scene (e.g., individual objects, what will happen next). Concurrent with our work, [156] collected questions & answers in Chinese (later translated to English by humans) for COCO images. [369] automatically generated four types of questions (object, count, color, location) using COCO captions.

Text-based Q&A is a well studied problem in the NLP and text processing communities (recent examples being [129, 128, 473, 372]). Other related textual tasks include sentence completion (e.g., [372] with multiple-choice answers). These approaches provide inspiration for VQA techniques. One key concern in text is the grounding of questions. For instance, [473] synthesized textual descriptions and QA-pairs grounded in a simulation of actors and objects in a fixed set of locations. VQA is naturally grounded in images – requiring the understanding of both text (questions) and vision (images). Our questions are generated by humans, making the need for commonsense knowledge and complex reasoning more essential.

Describing Visual Content. Related to VQA are the tasks of image tagging [112, 243], image captioning [247, 134, 309, 89, 131, 451, 116, 222, 290, 229] and video captioning [374, 172], where words or sentences are generated to describe visual content. While these tasks require both visual and semantic knowledge, captions can often be non-specific (e.g., observed by [451]). The questions in VQA require detailed
specific information about the image for which generic image captions are of little use [51].

Other Vision+Language Tasks. Several recent papers have explored tasks at the intersection of vision and language that are easier to evaluate than image captioning, such as coreference resolution [235, 361] or generating referring expressions [225, 312] for a particular object in an image that would allow a human to identify which object is being referred to (e.g., “the one in a red shirt”, “the dog on the left”). While task-driven and concrete, a limited set of visual concepts (e.g., color, location) tend to be captured by referring expressions. As we demonstrate, a richer variety of visual concepts emerge from visual questions and their answers.

2.2 Analyzing the Behavior of VQA Models

Our work is inspired by previous works that diagnose the failure modes of models for different tasks. [223] constructed a series of oracles to measure the performance of a character level language model. [189] provided analysis tools to facilitate detailed and meaningful investigation of object detector performance. Our work aims to perform behavior analyses as a first step towards diagnosing errors for VQA.

[495] categorize the errors made by their VQA model into four categories – model focuses attention on incorrect regions, model focuses attention on appropriate regions but predicts incorrect answers, predicted answers are different from labels but might be acceptable, labels are wrong. While these are coarse but useful failure modes, we are interested in understanding the behavior of VQA models along specific dimensions – whether they generalize to novel instances, whether they listen to the entire question, whether they look at the image.
2.3 Overcoming Priors in VQA

Countering Priors in VQA: In order to counter the language priors in the VQA v1 dataset, [168] balance every question by collecting complementary images for every question. Thus, for every question in the proposed VQA v2 dataset, there are two similar images with different answers to the question. By construction, language priors are significantly weaker in the VQA v2 dataset. However, the train and test distributions are still similar, unlike our work where the train and test answer distributions are by design different (section 5.1). So, leveraging priors from the train set will still benefit the model at test time. [505] balance the yes/no questions on abstract scenes from the VQA v1 dataset in a similar manner. More recently, [216] propose two new evaluation metrics that compensate for the skewed distribution of question types and for the skewed distribution of answers within each question type in the test set. As a remedy for machines using “shortcuts” to solve multiple-choice VQA, [79] describe several principles for automatic construction of good decoys (the incorrect candidate answers). [80] study cross-dataset adaptation for VQA. They propose an algorithm for adapting a VQA model trained on one dataset to apply to another dataset with different statistical distribution. All these works indicate that there is an increasing interest in the community to focus on models that are less driven by training priors and are more visually grounded.

Compositionality. Related to the ability to generalize across different answer distributions is the ability to generalize to novel compositions of known concepts learned during training. Compositionality has been studied in various forms in the vision community. Zero-shot object recognition using attributes is based on the idea of composing attributes to detect novel object categories [256, 206]. [31] have studied compositionality in the domain of image captioning by focusing on structured representations (subject-relation-object triplets). We study compositionality for visual question answering where the questions and answers are open-ended and in free-form
natural language. The work closest to us is [211] where they study compositionality in the domain of VQA. However, their dataset (images as well as questions) is synthetic and has only limited number of objects and attributes. On the contrary, our C-VQA splits consist of real images and questions (asked by humans) and hence involve a variety of objects and attributes, as well as activities, scenes, etc. Andreas et al. [24, 25] have developed compositional models for VQA that consist of different modules each specialized for a particular task. These modules can be composed together based on the question structure to create a model architecture for the given question. Although, compositional by design, these models have not been evaluated specifically for compositionality. Our C-VQA splits can be used to evaluate such models to test the degree of compositionality. In fact, we report the performance of Neural Module Networks on our C-VQA splits and find that its performance degrades significantly from the original VQA setting to the proposed C-VQA setting (section ??).

Zero-shot VQA has also been explored in [428]. They study a setting for VQA where the test questions (the question string itself or the multiple choices) contain at least one unseen word. [360] propose answering questions about unknown objects (e.g., ‘Is the dog black and white?’ where ‘dog’ is never seen in training questions or answers). These are orthogonal efforts to our work in that our focus is not in studying if unseen words/concepts can be recognized during testing. We are instead interested in studying – 1) the extent to which a model is visually grounded by evaluating its ability to generalize to a different answer distribution for each question type, 2) the extent to which a model is able to answer questions about unseen compositions of seen concepts. In both the splits proposed by us (VQA-CP and C-VQA), we ensure that concepts seen during test time are present during training to the extent possible.

Adversarial Learning. Generative Adversarial Networks (GANs) [164] have received significant recent interest for their ability to model complex distributions – finding use in a variety of image and language generation tasks [164, 356, 504, 102,
Recently, other adversarial training schemes have been proposed to encourage various forms of invariance in intermediate model representations [257, 277, 442].

Most related to our work on adversarial regularization for VQA (section 5.3), Lample et al. [257] introduce an autoencoder framework with an adversarial loss for attribute-based image manipulation. Given an input image and a set of attributes (e.g., a photo of a person and their gender or age), the task is to manipulate the image such that it has the desired attributes. Unfortunately, without multiple pairings of the same image with different attributes, it is challenging to learn disentangled image representations that generalize to new input-attribute combinations. An adversarial model is introduced that is trained to predict attributes from the input image encoding alone. In combating this adversary, the image encoder model learns to produce attribute invariant image encodings. This improves generalization by forcing the attribute-augmented decoder to meaningfully rely on input attributes to accurately reproduce input images.

Similarly, the question-only adversary in our work (section 5.3), encourages the VQA question encoder to remove answer-discriminative features from the question representation. However, breaking the parallels with [257], the answer themselves are not added back as inputs to controllably recondition the model on these features. Rather, the VQA model must rely on the combination of question and image features to recover the answer information. In this way, the language-level answer information (e.g., that most grass is green) is removed from the question and instance-specific information from the image must be used instead. We take this notion further by leveraging the question-only adversary to estimate and directly maximize the change in confidence after observing the image, which we show provides substantial benefits when paired with the question-only adversary.
CHAPTER III

VISUAL QUESTION ANSWERING (VQA)

3.1 Introduction

We are witnessing a renewed excitement in multi-discipline Artificial Intelligence (AI) research problems. In particular, research in image and video captioning that combines Computer Vision (CV), Natural Language Processing (NLP), and Knowledge Representation & Reasoning (KR) has dramatically increased in the past year [131, 89, 116, 290, 229, 222, 451]. Part of this excitement stems from a belief that multi-discipline tasks like image captioning are a step towards solving AI. However, the current state of the art demonstrates that a coarse scene-level understanding of an image paired with word $n$-gram statistics suffices to generate reasonable image captions, which suggests image captioning may not be as “AI-complete” as desired.

What makes for a compelling “AI-complete” task? We believe that in order to spawn the next generation of AI algorithms, an ideal task should (i) require multi-modal knowledge beyond a single sub-domain (such as CV) and (ii) have a well-defined quantitative evaluation metric to track progress. For some tasks, such as image captioning, automatic evaluation is still a difficult and open research problem [447, 125, 186].

In this chapter, we introduce the task of free-form and open-ended Visual Question Answering (VQA). A VQA system takes as input an image and a free-form, open-ended, natural-language question about the image and produces a natural-language answer as the output. This goal-driven task is applicable to scenarios encountered when visually-impaired users [51] or intelligence analysts actively elicit visual information. Example questions are shown in Fig. 3.
Figure 3: Examples of free-form, open-ended questions collected for images via Amazon Mechanical Turk. Note that commonsense knowledge is needed along with a visual understanding of the scene to answer many questions.

Open-ended questions require a potentially vast set of AI capabilities to answer – fine-grained recognition (e.g., “What kind of cheese is on the pizza?”), object detection (e.g., “How many bikes are there?”), activity recognition (e.g., “Is this man crying?”), knowledge base reasoning (e.g., “Is this a vegetarian pizza?”), and commonsense reasoning (e.g., “Does this person have 20/20 vision?”, “Is this person expecting company?”). VQA [158, 286, 439, 51] is also amenable to automatic quantitative evaluation, making it possible to effectively track progress on this task. While the answer to many questions is simply “yes” or “no”, the process for determining a correct answer is typically far from trivial (e.g. in Fig. 3, “Does this person have 20/20 vision?”). Moreover, since questions about images often tend to seek specific information, simple one-to-three word answers are sufficient for many questions. In such scenarios, we can easily evaluate a proposed algorithm by the number of questions it answers correctly. In this work, we present both an open-ended answering
task and a multiple-choice task [372, 271]. Unlike the open-ended task that requires a free-form response, the multiple-choice task only requires an algorithm to pick from a predefined list of possible answers.

We present a large dataset that contains 204,721 images from the MS COCO dataset [269] and a newly created abstract scene dataset [516, 29] that contains 50,000 scenes. The MS COCO dataset has images depicting diverse and complex scenes that are effective at eliciting compelling and diverse questions. We collected a new dataset of “realistic” abstract scenes to enable research focused only on the high-level reasoning required for VQA by removing the need to parse real images. Three questions were collected for each image or scene. Each question was answered by ten subjects along with their confidence. The dataset contains over 760K questions with around 10M answers.

While the use of open-ended questions offers many benefits, it is still useful to understand the types of questions that are being asked and which types various algorithms may be good at answering. To this end, we analyze the types of questions asked and the types of answers provided. Through several visualizations, we demonstrate the astonishing diversity of the questions asked. We also explore how the information content of questions and their answers differs from image captions. For baselines, we offer several approaches that use a combination of both text and state-of-the-art visual features [243]. As part of the VQA initiative, we have been organizing annual challenges and associated workshops to discuss state-of-the-art methods and best practices.

VQA poses a rich set of challenges, many of which have been viewed as the holy grail of automatic image understanding and AI in general. However, it includes as building blocks several components that the CV, NLP, and KR [72, 88, 261, 273, 57] communities have made significant progress on during the past few decades. VQA provides an attractive balance between pushing the state of the art, while being
accessible enough for the communities to start making progress on the task.

### 3.2 VQA Dataset Collection

We now describe the Visual Question Answering (VQA) dataset. We begin by describing the real images and abstract scenes used to collect the questions. Next, we describe our process of collecting questions and their corresponding answers. Analysis of the questions and answers gathered as well as baselines' & methods' results are provided in following sections.

**Real Images.** We use the 123,287 training and validation images and 81,434 test images from the Microsoft Common Objects in Context (MS COCO) [269] dataset. The MS COCO dataset was gathered to find images containing multiple objects and rich contextual information. Given the visual complexity of these images, they...
are well-suited for our VQA task. The more diverse our collection of images, the more diverse, comprehensive, and interesting the resultant set of questions and their answers.

**Abstract Scenes.** The VQA task with real images requires the use of complex and often noisy visual recognizers. To attract researchers interested in exploring the high-level reasoning required for VQA, but not the low-level vision tasks, we create a new abstract scenes dataset [29, 516, 517, 518] containing 50K scenes. The dataset contains 20 “paperdoll” human models [29] spanning genders, races, and ages with 8 different expressions. The limbs are adjustable to allow for continuous pose variations. The clipart may be used to depict both indoor and outdoor scenes. The set contains over 100 objects and 31 animals in various poses. The use of this clipart enables the creation of more realistic scenes (see bottom row of Fig. 4) that more closely mirror real images than previous papers [516, 517, 518]. See the appendix for the user interface, additional details, and examples.

**Splits.** For real images, we follow the same train/val/test split strategy as the MC COCO dataset [269] (including test-dev, test-standard, test-challenge, test-reserve). For the VQA challenge (see section ??), test-dev is used for debugging and validation experiments and allows for unlimited submission to the evaluation server. Test-standard is the ‘default’ test data for the VQA competition. When comparing to the state of the art (e.g., in papers), results should be reported on test-standard. Test-standard is also used to maintain a public leaderboard that is updated upon submission. Test-reserve is used to protect against possible overfitting. If there are substantial differences between a method’s scores on test-standard and test-reserve, this raises a red-flag and prompts further investigation. Results on test-reserve are not publicly revealed. Finally, test-challenge is used to determine the winners of the challenge.

For abstract scenes, we created splits for standardization, separating the scenes
into 20K/10K/20K for train/val/test splits, respectively. There are no subsplits (test-dev, test-standard, test-challenge, test-reserve) for abstract scenes.

**Captions.** The MS COCO dataset [269, 86] already contains five single-sentence captions for all images. We also collected five single-captions for all abstract scenes using the same user interface\(^1\) for collection.

**Questions.** Collecting interesting, diverse, and well-posed questions is a significant challenge. Many simple questions may only require low-level computer vision knowledge, such as “What color is the cat?” or “How many chairs are present in the scene?”. However, we also want questions that require commonsense knowledge about the scene, such as “What sound does the pictured animal make?”. Importantly, questions should also require the image to correctly answer and not be answerable using just commonsense information, *e.g.*, in Fig. 3, “What is the mustache made of?”. By having a wide variety of question types and difficulty, we may be able to measure the continual progress of both visual understanding and commonsense reasoning.

We tested and evaluated a number of user interfaces for collecting such “interesting” questions. Specifically, we ran pilot studies asking human subjects to ask questions about a given image that they believe a “toddler”, “alien”, or “smart robot” would have trouble answering. We found the “smart robot” interface to elicit the most interesting and diverse questions. As shown in the appendix, our final interface stated:

\(^1\)https://github.com/tylin/coco-ui
“We have built a smart robot. It understands a lot about images. It can recognize and name all the objects, it knows where the objects are, it can recognize the scene (e.g., kitchen, beach), people’s expressions and poses, and properties of objects (e.g., color of objects, their texture). Your task is to stump this smart robot!

Ask a question about this scene that this smart robot probably can not answer, but any human can easily answer while looking at the scene in the image.”

To bias against generic image-independent questions, subjects were instructed to ask questions that require the image to answer.

The same user interface was used for both the real images and abstract scenes. In total, three questions from unique workers were gathered for each image/scene. When writing a question, the subjects were shown the previous questions already asked for that image to increase the question diversity. In total, the dataset contains over ∼0.76M questions.

Answers. Open-ended questions result in a diverse set of possible answers. For many questions, a simple “yes” or “no” response is sufficient. However, other questions may require a short phrase. Multiple different answers may also be correct. For instance, the answers “white”, “tan”, or “off-white” may all be correct answers to the same question. Human subjects may also disagree on the “correct” answer, e.g., some saying “yes” while others say “no”. To handle these discrepancies, we gather 10 answers for each question from unique workers, while also ensuring that the worker answering a question did not ask it. We ask the subjects to provide answers that are “a brief phrase and not a complete sentence. Respond matter-of-factly and avoid using conversational language or inserting your opinion.” In addition to answering the questions, the subjects were asked “Do you think you were able to answer the question correctly?” and given the choices of “no”, “maybe”, and “yes”. See the appendix for more details about the user interface to collect answers. See Section 3.3
for an analysis of the answers provided.

For testing, we offer two modalities for answering the questions: (i) open-ended and (ii) multiple-choice.

For the open-ended task, the generated answers are evaluated using the following accuracy metric:

\[
\text{accuracy} = \min\left(\frac{\text{# humans that provided that answer}}{3}, 1\right)
\]

\textit{i.e.,} an answer is deemed 100% accurate if at least 3 workers provided that exact answer.\(^2\) Before comparison, all responses are made lowercase, numbers converted to digits, and punctuation & articles removed. We avoid using soft metrics such as Word2Vec [303], since they often group together words that we wish to distinguish, such as “left” and “right”. We also avoid using evaluation metrics from machine translation such as BLEU and ROUGE because such metrics are typically applicable and reliable for sentences containing multiple words. In VQA, most answers (89.32%) are single word; thus there no high-order n-gram matches between predicted answers and ground-truth answers, and low-order n-gram matches degenerate to exact-string matching. Moreover, these automatic metrics such as BLEU and ROUGE have been found to poorly correlate with human judgement for tasks such as image caption evaluation [87].

For multiple-choice task, 18 candidate answers are created for each question. As with the open-ended task, the accuracy of a chosen option is computed based on the number of human subjects who provided that answer (divided by 3 and clipped at 1). We generate a candidate set of correct and incorrect answers from four sets of answers: \textbf{Correct:} The most common (out of ten) correct answer. \textbf{Plausible:} To generate incorrect, but still plausible answers we ask three subjects to answer the questions without seeing the image. See the appendix for more details about

\(^2\)In order to be consistent with ‘human accuracies’ reported in Section ??, machine accuracies are averaged over all \(\binom{10}{9}\) sets of human annotators
the user interface to collect these answers. If three unique answers are not found, we gather additional answers from nearest neighbor questions using a bag-of-words model. The use of these answers helps ensure the image, and not just commonsense knowledge, is necessary to answer the question. **Popular:** These are the 10 most popular answers. For instance, these are “yes”, “no”, “2”, “1”, “white”, “3”, “red”, “blue”, “4”, “green” for real images. The inclusion of the most popular answers makes it more difficult for algorithms to infer the type of question from the set of answers provided, *i.e.*, learning that it is a “yes or no” question just because “yes” and “no” are present in the answers. **Random:** Correct answers from random questions in the dataset. To generate a total of 18 candidate answers, we first find the union of the correct, plausible, and popular answers. We include random answers until 18 unique answers are found. The order of the answers is randomized. Example multiple choice questions are in the appendix.

Note that all 18 candidate answers are unique. But since 10 different subjects answered every question, it is possible that more than one of those 10 answers be present in the 18 choices. In such cases, according to the accuracy metric, multiple options could have a non-zero accuracy.

### 3.3 VQA Dataset Analysis

In this section, we provide an analysis of the questions and answers in the VQA train dataset. To gain an understanding of the types of questions asked and answers provided, we visualize the distribution of question types and answers. We also explore how often the questions may be answered without the image using just commonsense information. Finally, we analyze whether the information contained in an image caption is sufficient to answer the questions.

The dataset includes 614,163 questions and 7,984,119 answers (including answers provided by workers with and without looking at the image) for 204,721 images from
3.3.1 Questions

Types of Question. Given the structure of questions generated in the English language, we can cluster questions into different types based on the words that start the question. Fig. 5 shows the distribution of questions based on the first four words of the questions for both the real images (left) and abstract scenes (right). Interestingly, the distribution of questions is quite similar for both real images and abstract scenes. This helps demonstrate that the type of questions elicited by the abstract scenes is similar to those elicited by the real images. There exists a surprising variety of question types, including “What is...”, “Is there...”, “How many...”, and “Does the...”. Quantitatively, the percentage of questions for different types is shown in Table ???. Several example questions and answers are shown in Fig. 4. A particularly interesting type of question is the “What is...” questions, since they have a diverse set
of possible answers. See the appendix for visualizations for “What is...” questions.

**Lengths.** Fig. 6 shows the distribution of question lengths. We see that most questions range from four to ten words.

### 3.3.2 Answers

**Typical Answers.** Fig. 7 (top) shows the distribution of answers for several question types. We can see that a number of question types, such as “Is the...”, “Are...”, and “Does...” are typically answered using “yes” and “no” as answers. Other questions such as “What is...” and “What type...” have a rich diversity of responses. Other question types such as “What color...” or “Which...” have more specialized responses, such as colors, or “left” and “right”. See the appendix for a list of the most popular answers.

**Lengths.** Most answers consist of a single word, with the distribution of answers containing one, two, or three words, respectively being 89.32%, 6.91%, and 2.74% for real images and 90.51%, 5.89%, and 2.49% for abstract scenes. The brevity of answers is not surprising, since the questions tend to elicit specific information from the images. This is in contrast with image captions that generically describe
Figure 7: Distribution of answers per question type for a random sample of 60K questions for real images when subjects provide answers when given the image (top) and when not given the image (bottom).
the entire image and hence tend to be longer. The brevity of our answers makes automatic evaluation feasible. While it may be tempting to believe the brevity of the answers makes the problem easier, recall that they are human-provided open-ended answers to open-ended questions. The questions typically require complex reasoning to arrive at these deceptively simple answers (see Fig. 4). There are currently 23,234 unique one-word answers in our dataset for real images and 3,770 for abstract scenes.

‘Yes/No’ and ‘Number’ Answers. Many questions are answered using either “yes” or “no” (or sometimes “maybe”) – 38.37% and 40.66% of the questions on real images and abstract scenes respectively. Among these ‘yes/no’ questions, there is a bias towards “yes” – 58.83% and 55.86% of ‘yes/no’ answers are “yes” for real images and abstract scenes. Question types such as “How many...” are answered using numbers – 12.31% and 14.48% of the questions on real images and abstract scenes are ‘number’ questions. “2” is the most popular answer among the ‘number’ questions, making up 26.04% of the ‘number’ answers for real images and 39.85% for abstract scenes.

Subject Confidence. When the subjects answered the questions, we asked “Do you think you were able to answer the question correctly?” Fig. 8 shows the distribution of responses. A majority of the answers were labeled as confident for both real images and abstract scenes.

Inter-human Agreement. Does the self-judgment of confidence correspond to the answer agreement between subjects? Fig. 8 shows the percentage of questions in which (i) 7 or more, (ii) 3 – 7, or (iii) less than 3 subjects agree on the answers given their average confidence score (0 = not confident, 1 = confident). As expected, the agreement between subjects increases with confidence. However, even if all of the subjects are confident the answers may still vary. This is not surprising since some answers may vary, yet have very similar meaning, such as “happy” and “joyful”.

As shown in Table 3.3.3 (Question + Image), there is significant inter-human
**Figure 8:** Number of questions per average confidence score (0 = not confident, 1 = confident) for real images and abstract scenes (black lines). Percentage of questions where 7 or more answers are same, 3-7 are same, less than 3 are same (color bars).

<table>
<thead>
<tr>
<th>3-4 (15.3%)</th>
<th>5-8 (39.7%)</th>
<th>9-12 (28.4%)</th>
<th>13-17 (11.2%)</th>
<th>18+ (5.5%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is that a bird in the sky?</td>
<td>How many pizzas are shown?</td>
<td>Where was this picture taken?</td>
<td>Is he likely to get mugged if he walked down a dark alleyway like this?</td>
<td>What type of architecture is this?</td>
</tr>
<tr>
<td>What color is the shoe?</td>
<td>What are the sheep eating?</td>
<td>What ceremony does the cake commemorate?</td>
<td>Is this a vegetarian meal?</td>
<td>Is this a Flemish bricklaying pattern?</td>
</tr>
<tr>
<td>How many zebras are there?</td>
<td>What color is his hair?</td>
<td>Are these boats too tall to fit under the bridge?</td>
<td>What type of beverage is in the glass?</td>
<td>How many calories are in this pizza?</td>
</tr>
<tr>
<td>Is there food on the table?</td>
<td>What sport is being played?</td>
<td>What is the name of the white shape under the batter?</td>
<td>Can you name the performer in the purple costume?</td>
<td>What government document is needed to partake in this activity?</td>
</tr>
<tr>
<td>Is this man wearing shoes?</td>
<td>Name one ingredient in the skillet.</td>
<td>Is this at the stadium?</td>
<td>Besides these humans, what other animals eat here?</td>
<td>What is the make and model of this vehicle?</td>
</tr>
</tbody>
</table>

**Figure 9:** Example questions judged by Mturk workers to be answerable by different age groups. The percentage of questions falling into each age group is shown in parentheses.

agreement in the answers for both real images (83.30%) and abstract scenes (87.49%). Note that on average each question has 2.70 unique answers for real images and 2.39 for abstract scenes. The agreement is significantly higher (> 95%) for “yes/no” questions and lower for other questions (< 76%), possibly due to the fact that we perform exact string matching and do not account for synonyms, plurality, etc. Note that the automatic determination of synonyms is a difficult problem, since the level of answer granularity can vary across questions.
Is the Image Necessary? Clearly, some questions can sometimes be answered correctly using commonsense knowledge alone without the need for an image, e.g., “What is the color of the fire hydrant?”. We explore this issue by asking three subjects to answer the questions without seeing the image (see the examples in blue in Fig. 4). In Table 3.3.3 (Question), we show the percentage of questions for which the correct answer is provided over all questions, “yes/no” questions, and the other questions that are not “yes/no”. For “yes/no” questions, the human subjects respond better than chance. For other questions, humans are only correct about 21% of the time. This demonstrates that understanding the visual information is critical to VQA and that commonsense information alone is not sufficient.

To show the qualitative difference in answers provided with and without images, we show the distribution of answers for various question types in Fig. 7 (bottom). The distribution of colors, numbers, and even “yes/no” responses is surprisingly different for answers with and without images.

Which Questions Require Common Sense? In order to identify questions that require commonsense reasoning to answer, we conducted two AMT studies (on a subset 10K questions from the real images of VQA trainval) asking subjects –

1. Whether or not they believed a question required commonsense to answer the question, and

2. The youngest age group that they believe a person must be in order to be able to correctly answer the question – toddler (3-4), younger child (5-8), older child (9-12), teenager (13-17), adult (18+).

Each question was shown to 10 subjects. We found that for 47.43% of questions 3 or more subjects voted ‘yes’ to commonsense, (18.14%: 6 or more). In the ‘perceived human age required to answer question’ study, we found the following distribution of responses: toddler: 15.3%, younger child: 39.7%, older child: 28.4%, teenager: 11.2%,
adult: 5.5%. In Figure 9 we show several questions for which a majority of subjects picked the specified age range. Surprisingly the perceived age needed to answer the questions is fairly well distributed across the different age ranges. As expected the questions that were judged answerable by an adult (18+) generally need specialized knowledge, whereas those answerable by a toddler (3-4) are more generic.

We measure the degree of commonsense required to answer a question as the percentage of subjects (out of 10) who voted “yes” in our “whether or not a question requires commonsense” study. A fine-grained breakdown of average age and average degree of common sense (on a scale of 0 – 100) required to answer a question is shown in Table ???. The average age and the average degree of commonsense across all questions is 8.92 and 31.01% respectively.

It is important to distinguish between:

1. How old someone needs to be to be able to answer a question correctly, and
2. How old people think someone needs to be to be able to answer a question correctly.

Our age annotations capture the latter – perceptions of MTurk workers in an uncontrolled environment. As such, the relative ordering of question types in Table ?? is more important than absolute age numbers. The two rankings of questions in terms of common sense required according to the two studies were largely correlated (Pearson’s rank correlation: 0.58).

3.3.4 Captions vs. Questions

Do generic image captions provide enough information to answer the questions? Table 3.3.3 (Question + Caption) shows the percentage of questions answered correctly when human subjects are given the question and a human-provided caption describing the image, but not the image. As expected, the results are better than when humans are shown the questions alone. However, the accuracies are significantly
lower than when subjects are shown the actual image. This demonstrates that in order to answer the questions correctly, deeper image understanding (beyond what image captions typically capture) is necessary. In fact, we find that the distributions of nouns, verbs, and adjectives mentioned in captions is statistically significantly different from those mentioned in our questions + answers (Kolmogorov-Smirnov test, \( p < .001 \)) for both real images and abstract scenes. See the appendix for details.

### 3.4 VQA Baselines and Methods

In this section, we explore the difficulty of the VQA dataset for the MS COCO images using several baselines and novel methods. We train on VQA train+val. Unless stated otherwise, all human accuracies are on test-standard, machine accuracies are on test-dev, and results involving human captions (in gray font) are trained on train and tested on val (because captions are not available for test).

#### 3.4.1 Baselines

We implemented the following baselines:

1. **random**: We randomly choose an answer from the top 1K answers of the VQA
2. **prior ("yes"):** We always select the most popular answer ("yes") for both the open-ended and multiple-choice tasks. Note that "yes" is always one of the choices for the multiple-choice questions.

3. **per Q-type prior:** For the open-ended task, we pick the most popular answer per question type (see the appendix for details). For the multiple-choice task, we pick the answer (from the provided choices) that is most similar to the picked answer for the open-ended task using cosine similarity in Word2Vec[303] feature space.

4. **nearest neighbor:** Given a test image, question pair, we first find the $K$ nearest neighbor questions and associated images from the training set. See appendix for details on how neighbors are found. Next, for the open-ended task, we pick the most frequent ground truth answer from this set of nearest neighbor question, image pairs. Similar to the "per Q-type prior" baseline, for the multiple-choice task, we pick the answer (from the provided choices) that is most similar to the picked answer for the open-ended task using cosine similarity in Word2Vec[303] feature space.

3.4.2 Methods

For our methods, we develop a 2-channel vision (image) + language (question) model that culminates with a softmax over $K$ possible outputs. We choose the top $K = 1000$ most frequent answers as possible outputs. This set of answers covers 82.67% of the train+val answers. We describe the different components of our model below:

**Image Channel:** This channel provides an embedding for the image. We experiment with two embeddings –
Figure 10: Our best performing model (deeper LSTM Q + norm I). This model uses a two layer LSTM to encode the questions and the last hidden layer of VGGNet [408] to encode the images. The image features are then $\ell_2$ normalized. Both the question and image features are transformed to a common space and fused via element-wise multiplication, which is then passed through a fully connected layer followed by a softmax layer to obtain a distribution over answers.

1. **I**: The activations from the last hidden layer of VGGNet [408] are used as 4096-dim image embedding.

2. **norm I**: These are $\ell_2$ normalized activations from the last hidden layer of VGGNet [408].

**Question Channel**: This channel provides an embedding for the question. We experiment with three embeddings –

1. **Bag-of-Words Question (BoW Q)**: The top 1,000 words in the questions are used to create a bag-of-words representation. Since there is a strong correlation between the words that start a question and the answer (see Fig. 7), we find the top 10 first, second, and third words of the questions and create a 30 dimensional bag-of-words representation. These features are concatenated to get a 1,030-dim embedding for the question.

2. **LSTM Q**: An LSTM with one hidden layer is used to obtain 1024-dim embedding for the question. The embedding obtained from the LSTM is a concatenation of last cell state and last hidden state representations (each being
512-dim) from the hidden layer of the LSTM. Each question word is encoded
with 300-dim embedding by a fully-connected layer + tanh non-linearity which
is then fed to the LSTM. The input vocabulary to the embedding layer consists
of all the question words seen in the training dataset.

3. **deeper LSTM Q**: An LSTM with two hidden layers is used to obtain 2048-
dim embedding for the question. The embedding obtained from the LSTM
is a concatenation of last cell state and last hidden state representations (each
being 512-dim) from each of the two hidden layers of the LSTM. Hence 2 (hidden
layers) x 2 (cell state and hidden state) x 512 (dimensionality of each of the cell
states, as well as hidden states) in Fig. 10. This is followed by a fully-connected
layer + tanh non-linearity to transform 2048-dim embedding to 1024-dim. The
question words are encoded in the same way as in LSTM Q.

**Multi-Layer Perceptron (MLP)**: The image and question embeddings are
combined to obtain a single embedding.

1. For **BoW Q + I** method, we simply concatenate the BoW Q and I embeddings.
2. For **LSTM Q + I**, and **deeper LSTM Q + norm I** (Fig. 10) methods, the
image embedding is first transformed to 1024-dim by a fully-connected layer
+ tanh non-linearity to match the LSTM embedding of the question. The
transformed image and LSTM embeddings (being in a common space) are then
fused via element-wise multiplication.

This combined image + question embedding is then passed to an MLP – a fully con-
ected neural network classifier with 2 hidden layers and 1000 hidden units (dropout
0.5) in each layer with tanh non-linearity, followed by a softmax layer to obtain a dis-
tribution over $K$ answers. The entire model is learned end-to-end with a cross-entropy
loss. VGGNet parameters are frozen to those learned for ImageNet classification and
not fine-tuned in the image channel.

We also experimented with providing captions as input to our model. Similar to
Table 2: Accuracy of our methods for the open-ended and multiple-choice tasks on the VQA test-dev for real images. Q = Question, I = Image, C = Caption. (Caption and BoW Q + C results are on val). See text for details.

<table>
<thead>
<tr>
<th>Open-Ended</th>
<th>Multiple-Choice</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Yes/No Number Other</td>
<td>All Yes/No Number Other</td>
</tr>
<tr>
<td>prior (“yes”)</td>
<td>29.66 70.81 00.39 01.15</td>
</tr>
<tr>
<td>per Q-type prior</td>
<td>37.54 71.03 35.77 09.38</td>
</tr>
<tr>
<td>nearest neighbor</td>
<td>42.70 71.89 24.36 21.94</td>
</tr>
<tr>
<td>BoW Q</td>
<td>48.09 75.66 36.70 27.14</td>
</tr>
<tr>
<td>I</td>
<td>28.13 64.01 00.42 03.77</td>
</tr>
<tr>
<td>BoW Q + I</td>
<td>52.64 75.55 33.67 37.37</td>
</tr>
<tr>
<td>LSTM Q</td>
<td>48.76 78.20 35.68 26.59</td>
</tr>
<tr>
<td>LSTM Q + I</td>
<td>53.74 78.94 35.24 36.02</td>
</tr>
<tr>
<td>deeper LSTM Q</td>
<td>50.39 78.41 34.68 30.02</td>
</tr>
<tr>
<td>deeper LSTM Q + norm</td>
<td>57.75 80.50 36.77 43.08</td>
</tr>
</tbody>
</table>

Table 3.3.3, we assume that a human-generated caption is given as input. We use a bag-of-words representation containing the 1,000 most popular words in the captions as the caption embedding (Caption). For BoW Question + Caption (BoW Q + C) method, we simply concatenate the BoW Q and C embeddings.

For testing, we report the result on two different tasks: open-ended selects the answer with highest activation from all possible $K$ answers and multiple-choice picks the answer that has the highest activation from the potential answers.

### 3.4.3 Results

Table 2 shows the accuracy of our baselines and methods for both the open-ended and multiple-choice tasks on the VQA test-dev for real images.

As expected, the vision-alone model (I) that completely ignores the question performs rather poorly (open-ended: 28.13% / multiple-choice: 30.53%). In fact, on open-ended task, the vision-alone model (I) performs worse than the prior (“yes”) baseline, which ignores both the image and question (responding to every question with a “yes”).

Interestingly, the language-alone methods (per Q-type prior, BoW Q, LSTM Q)
that ignore the image perform surprisingly well, with BoW Q achieving 48.09% on open-ended (53.68% on multiple-choice) and LSTM Q achieving 48.76% on open-ended (54.75% on multiple-choice); both outperforming the nearest neighbor baseline (open-ended: 42.70%, multiple-choice: 48.49%). Our quantitative results and analyses suggest that this might be due to the language-model exploiting subtle statistical priors about the question types (e.g. “What color is the banana?” can be answered with “yellow” without looking at the image). For a detailed discussion of the subtle biases in the questions, please see [505].

The accuracy of our best model (deeper LSTM Q + norm I (Fig. 10), selected using VQA test-dev accuracies) on VQA test-standard is 58.16% (open-ended) / 63.09% (multiple-choice). We can see that our model is able to significantly outperform both the vision-alone and language-alone baselines. As a general trend, results on multiple-choice are better than open-ended. All methods are significantly worse than human performance.

Our VQA demo is available on CloudCV [20] – http://vqa.cloudcv.org/. This will be updated with newer models as we develop them.

To gain further insights into these results, we computed accuracies by question type in Table 3. Interestingly, for question types that require more reasoning, such as “Is the” or “How many”, the scene-level image features do not provide any additional information. However, for questions that can be answered using scene-level information, such as “What sport,” we do see an improvement. Similarly, for questions whose answer may be contained in a generic caption we see improvement, such as “What animal”. For all question types, the results are worse than human accuracies.

We also analyzed the accuracies of our best model (deeper LSTM Q + norm I) on a subset of questions with certain specific (ground truth) answers. In Fig. 11, we show the average accuracy of the model on questions with 50 most frequent ground truth answers on the VQA validation set (plot is sorted by accuracy, not frequency). We
can see that the model performs well for answers that are common visual objects such as “wii”, “tennis”, “bathroom” while the performance is somewhat underwhelming for counts (e.g., “2”, “1”, “3”), and particularly poor for higher counts (e.g., “5”, “6”, “10”, “8”, “7”).

In Fig. 12, we show the distribution of 50 most frequently predicted answers when the system is correct on the VQA validation set (plot is sorted by prediction frequency, not accuracy). In this analysis, “system is correct” implies that it has VQA accuracy 1.0 (see section 3.2 for accuracy metric). We can see that the frequent ground truth answers (e.g., “yes”, “no”, “2”, “white”, “red”, “blue”, “1”, “green”) are more frequently predicted than others when the model is correct.

**Table 3:** Open-ended test-dev results for different question types on real images (Q+C is reported on val). Machine performance is reported using the bag-of-words representation for questions. Questions types are determined by the one or two words that start the question. The percentage of questions for each type is shown in parentheses. Last and second last columns respectively show the average human age and average degree of commonsense required to answer the questions (as reported by AMT workers), respectively. See text for details.

<table>
<thead>
<tr>
<th>Question Type</th>
<th>Open-Ended K = 1000</th>
<th>Human To Be Able</th>
<th>Commonsense To Be Able</th>
</tr>
</thead>
<tbody>
<tr>
<td>what is (13.84)</td>
<td>23.57 34.28 43.88</td>
<td>16.86 73.68</td>
<td>09.07 27.52</td>
</tr>
<tr>
<td>what color (08.98)</td>
<td>33.37 43.53 48.61</td>
<td>28.71 86.06</td>
<td>06.60 13.22</td>
</tr>
<tr>
<td>what kind (02.49)</td>
<td>27.78 42.72 43.88</td>
<td>19.10 70.11</td>
<td>10.55 40.34</td>
</tr>
<tr>
<td>what are (02.32)</td>
<td>25.47 39.10 47.27</td>
<td>17.72 69.49</td>
<td>09.03 28.72</td>
</tr>
<tr>
<td>what type (01.78)</td>
<td>27.68 42.62 44.32</td>
<td>19.53 70.65</td>
<td>11.04 38.92</td>
</tr>
<tr>
<td>is the (10.16)</td>
<td>70.76 69.87 70.50</td>
<td>65.24 95.67</td>
<td>08.51 30.30</td>
</tr>
<tr>
<td>is this (08.26)</td>
<td>70.34 70.79 71.54</td>
<td>63.35 95.43</td>
<td>10.13 45.32</td>
</tr>
<tr>
<td>how many (10.28)</td>
<td>43.78 40.33 47.52</td>
<td>30.45 86.32</td>
<td>07.67 15.93</td>
</tr>
<tr>
<td>are (07.57)</td>
<td>73.96 73.58 72.43</td>
<td>67.10 95.24</td>
<td>08.65 30.63</td>
</tr>
<tr>
<td>does (02.75)</td>
<td>76.81 75.81 75.88</td>
<td>69.96 95.70</td>
<td>09.29 38.97</td>
</tr>
<tr>
<td>where (02.90)</td>
<td>16.21 23.49 29.47</td>
<td>11.09 43.56</td>
<td>09.54 36.51</td>
</tr>
<tr>
<td>is there (03.60)</td>
<td>86.50 86.37 85.88</td>
<td>72.48 96.43</td>
<td>08.25 19.88</td>
</tr>
<tr>
<td>is there (03.60)</td>
<td>86.50 86.37 85.88</td>
<td>72.48 96.43</td>
<td>08.25 19.88</td>
</tr>
<tr>
<td>why (01.20)</td>
<td>16.24 13.94 14.54</td>
<td>11.80 21.50</td>
<td>11.18 73.56</td>
</tr>
<tr>
<td>which (01.21)</td>
<td>29.50 34.83 40.84</td>
<td>25.64 67.44</td>
<td>09.27 30.00</td>
</tr>
<tr>
<td>do (01.15)</td>
<td>77.73 79.31 74.63</td>
<td>71.33 95.44</td>
<td>09.23 37.68</td>
</tr>
<tr>
<td>what does (01.12)</td>
<td>19.58 20.00 23.19</td>
<td>11.12 75.88</td>
<td>10.02 33.27</td>
</tr>
<tr>
<td>what time (00.67)</td>
<td>8.35 14.00 18.28</td>
<td>07.64 58.98</td>
<td>09.31 31.87</td>
</tr>
<tr>
<td>who (00.77)</td>
<td>19.75 20.43 27.28</td>
<td>14.69 56.93</td>
<td>09.49 43.82</td>
</tr>
<tr>
<td>what sport (00.81)</td>
<td>37.96 51.12 93.87</td>
<td>17.86 95.59</td>
<td>08.07 31.87</td>
</tr>
<tr>
<td>what animal (00.53)</td>
<td>23.12 59.70 71.02</td>
<td>17.67 92.51</td>
<td>06.75 18.04</td>
</tr>
<tr>
<td>what brand (00.36)</td>
<td>40.13 36.84 32.19</td>
<td>25.34 80.95</td>
<td>12.50 41.33</td>
</tr>
</tbody>
</table>

Finally, evaluating our best model (deeper LSTM Q + norm I) on the validation
questions for which we have age annotations (how old a human needs to be to answer the question correctly), we estimate that our model performs as well as a 4.74 year old child! The average age required on the same set of questions is 8.98. Evaluating the same model on the validation questions for which we have commonsense annotations (whether the question requires commonsense to answer it), we estimate that it has degree of commonsense of 17.35%. The average degree of commonsense required on same set of questions is 31.23%. Again, these estimates reflect the age and commonsense perceived by MTurk workers that would be required to answer the question. See the appendix for details.

We further analyzed the performance of the model for different age groups on the validation questions for which we have age annotations. In Fig. 13, we computed the average accuracy of the predictions made by the model for questions belonging to different age groups. Perhaps as expected, the accuracy of the model decreases as the age of the question increases (from 61.07% at 3−4 age group to 47.83% at 18+ age group).

In Fig. 14, we show the distribution of age of questions for different levels of accuracies achieved by our system on the validation questions for which we have age annotations. It is interesting to see that the relative proportions of different age groups is consistent across all accuracy bins with questions belonging to the age group 5-8 comprising the majority of the predictions which is expected because 5-8 is the most common age group in the dataset (see Fig. 9).

Table 4 shows the accuracy of different ablated versions of our best model (deeper LSTM Q + norm I) for both the open-ended and multiple-choice tasks on the VQA test-dev for real images. The different ablated versions are as follows –

1. **Without I Norm:** In this model, the activations from the last hidden layer of VGGNet [408] are not $\ell_2$-normalized. Comparing the accuracies in Table 4 and Table 2, we can see that $\ell_2$-normalization of image features boosts the
Figure 11: Pr (system is correct | answer) for 50 most frequent ground truth answers on the VQA validation set (plot is sorted by accuracy, not frequency). System refers to our best model (deeper LSTM Q + norm I).

Figure 12: Pr (answer | system is correct) for 50 most frequently predicted answers on the VQA validation set (plot is sorted by prediction frequency, not accuracy). System refers to our best model (deeper LSTM Q + norm I).

performance by 0.16% for open-ended task and by 0.24% for multiple-choice task.

2. **Concatenation:** In this model, the transformed image and LSTM embeddings are concatenated (instead of element-wise multiplied), resulting in doubling the number of parameters in the following fully-connected layer. Comparing the accuracies in Table 4 and Table 2, we can see that element-wise fusion performs better by 0.95% for open-ended task and by 1.24% for multiple-choice task.

3. **K = 500:** In this model, we use K = 500 most frequent answers as possible outputs. Comparing the accuracies in Table 4 and Table 2, we can see that K = 1000 performs better than K = 500 by 0.82% for open-ended task and by 1.92% for multiple-choice task.

4. **K = 2000:** In this model, we use K = 2000 most frequent answers as possible outputs. Comparing the accuracies in Table 4 and Table 2, we can see that K
Figure 13: \( \text{Pr}(\text{system is correct} \mid \text{age of question}) \) on the VQA validation set. System refers to our best model (deeper LSTM Q + norm I).

\[ \text{K} = 2000 \text{ performs better than } \text{K} = 1000 \text{ by 0.40\% for open-ended task and by 1.16\% for multiple-choice task.} \]

5. **Truncated Q Vocab @ 5:** In this model, the input vocabulary to the embedding layer (which encodes the question words) consists of only those question words which occur at least 5 times in the training dataset, thus reducing the vocabulary size from 14770 (when all question words are used) to 5134 (65.24\% reduction). Remaining question words are replaced with UNK (unknown) tokens. Comparing the accuracies in Table 4 and Table 2, we can see that truncating the question vocabulary @ 5 performs better than using all question words by 0.24\% for open-ended task and by 0.17\% for multiple-choice task.

6. **Truncated Q Vocab @ 11:** In this model, the input vocabulary to the embedding layer (which encodes the question words) consists of only those question words which occur at least 11 times in the training dataset, thus reducing the vocabulary size from 14770 (when all question words are used) to 3561 (75.89\%
Figure 14: \( Pr(\text{age of question} \mid \text{system is correct}) \) on the VQA validation set. System refers to our best model (deeper LSTM Q + norm I).

7. **Filtered Dataset:** We created a filtered version of the VQA train + val dataset in which we only keep the answers with subject confidence “yes”. Also, we keep only those questions for which at least 50% (5 out of 10) answers are annotated with subject confidence “yes”. The resulting filtered dataset consists of 344600 questions, compared to 369861 questions in the original dataset, leading to only 6.83% reduction in the size of the dataset. The filtered dataset has 8.77 answers per question on average. We did not filter the test set so that accuracies of the model trained on the filtered dataset can be compared with that of the model trained on the original dataset. The row “Filtered Dataset” in Table 4 shows the performance of the deeper LSTM Q + norm I model when trained on the filtered dataset. Comparing these accuracies with the corresponding accuracies in Table 2, we can see that the model trained on filtered version performs worse by 1.13% for open-ended task and by 1.88% for multiple-choice task.
Table 4: Accuracy of ablated versions of our best model (deeper LSTM Q + norm I) for the open-ended and multiple-choice tasks on the VQA test-dev for real images. Q = Question, I = Image. See text for details.

<table>
<thead>
<tr>
<th></th>
<th>Open-Ended</th>
<th>Multiple-Choice</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>All</td>
<td>Yes/No</td>
</tr>
<tr>
<td>Without I Norm</td>
<td>57.59</td>
<td>80.41</td>
</tr>
<tr>
<td>Concatenation</td>
<td>56.80</td>
<td>78.49</td>
</tr>
<tr>
<td>K = 500</td>
<td>56.93</td>
<td>80.61</td>
</tr>
<tr>
<td>K = 2000</td>
<td>58.15</td>
<td>80.61</td>
</tr>
<tr>
<td>Truncated Q Vocab @ 5</td>
<td>57.99</td>
<td>80.67</td>
</tr>
<tr>
<td>Truncated Q Vocab @ 11</td>
<td>57.81</td>
<td>80.42</td>
</tr>
<tr>
<td>Filtered Dataset</td>
<td>56.62</td>
<td>80.19</td>
</tr>
</tbody>
</table>

3.5 VQA Challenge and Workshop

We have set up an evaluation server\textsuperscript{3} where results may be uploaded for the test set and it returns an accuracy breakdown. We are organizing an annual challenge and workshop to facilitate systematic progress in this area; the first instance of the workshop was held at CVPR 2016\textsuperscript{4}. We suggest that papers reporting results on the VQA dataset –

1. Report test-standard accuracies, which can be calculated using either of the non-test-dev phases, i.e., “test2015” or “Challenge test2015” on the following links: [oe-real | oe-abstract | mc-real | mc-abstract].


For more details, please see the challenge page\textsuperscript{5}. Screenshots of leaderboards for open-ended-real and multiple-choice-real are shown in Fig. 15. We also compare the test-standard accuracies of our best model (deeper LSTM Q + norm I) for both open-ended and multiple-choice tasks (real images) with other entries (as of October 28, 2016) on the corresponding leaderboards in Table 5.

\textsuperscript{3}http://visualqa.org/challenge_2016.html
\textsuperscript{4}http://www.visualqa.org/workshop_2016.html
\textsuperscript{5}http://visualqa.org/challenge_2016.html
Table 5: Test-standard accuracy of our best model (deeper LSTM Q + norm I) compared to test-standard accuracies of other entries for the open-ended and multiple-choice tasks in the respective VQA Real Image Challenge leaderboards (as of October 28, 2016).

<table>
<thead>
<tr>
<th></th>
<th>Open-Ended</th>
<th>Multiple-Choice</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>All</td>
<td>Yes/No</td>
</tr>
<tr>
<td>snubi-naverlabs</td>
<td>60.60</td>
<td>82.23</td>
</tr>
<tr>
<td>MM_PaloAlto</td>
<td>60.36</td>
<td>80.43</td>
</tr>
<tr>
<td>LV-NUS</td>
<td>59.54</td>
<td>81.34</td>
</tr>
<tr>
<td>ACVT_Adelaide</td>
<td>59.44</td>
<td>81.07</td>
</tr>
<tr>
<td>global_vision</td>
<td>58.43</td>
<td>78.24</td>
</tr>
<tr>
<td>deeper LSTM Q + norm I</td>
<td>58.16</td>
<td>80.56</td>
</tr>
<tr>
<td>iBOWIMG</td>
<td>–</td>
<td>–</td>
</tr>
</tbody>
</table>

3.6 Conclusion and Discussion

In conclusion, we introduce the task of Visual Question Answering (VQA). Given an image and an open-ended, natural language question about the image, the task is to provide an accurate natural language answer. We provide a dataset containing over 250K images, 760K questions, and around 10M answers. We demonstrate the wide variety of questions and answers in our dataset, as well as the diverse set of AI capabilities in computer vision, natural language processing, and commonsense reasoning required to answer these questions accurately.

The questions we solicited from our human subjects were open-ended and not task-specific. For some application domains, it would be useful to collect task-specific questions. For instance, questions may be gathered from subjects who are visually impaired [51], or the questions could focus on one specific domain (say sports). Bigham et al. [51] created an application that allows the visually impaired to capture images and ask open-ended questions that are answered by human subjects. Interestingly, these questions can rarely be answered using generic captions. Training on task-specific datasets may help enable practical VQA applications.

We believe VQA has the distinctive advantage of pushing the frontiers on “AI-complete” problems, while being amenable to automatic evaluation. Given the recent
Figure 15: Leaderboard showing test-standard accuracies for VQA Real Image Challenge (Open-Ended) on left and leaderboard showing test-standard accuracies for VQA Real Image Challenge (Multiple-Choice) on right (snapshot from October 28, 2016).

progress in the community, we believe the time is ripe to take on such an endeavor.
CHAPTER IV

ANALYZING THE BEHAVIOR OF VISUAL QUESTION ANSWERING MODELS

4.1 Introduction

After the release of our VQA dataset, a flurry of recent deep-learning based models have been proposed for VQA [27, 84, 495, 485, 208, 24, 465, 217, 280, 25, 400, 227, 150, 321, 197, 480, 483, 510, 381]. Curiously, the performance of most methods is clustered around 60-70% (compared to human performance of 83% on open-ended task and 91% on multiple-choice task) with a mere 5% gap between the top-9 entries on the VQA challenge 2016.\(^1\) It seems clear that as a first step to understand these models, to meaningfully compare strengths and weaknesses of different models, to develop insights into their failure modes, and to identify the most fruitful directions for progress, it is crucial to develop techniques to understand the behavior of VQA models.

In this chapter, we develop novel techniques for characterizing the behavior of VQA models. As concrete instantiations, we analyze two VQA models ([279],[280]), one from each of the two major classes of VQA models – with-attention and without-attention. We also analyze the winning entry [150] of the VQA Challenge 2016.

4.2 Behavior Analyses

We analyze the behavior of VQA models along the following three dimensions –

**Generalization to novel instances:** We investigate whether the test instances that are incorrectly answered are the ones that are “novel” i.e., not similar to training

\(^1\)http://www.visualqa.org/challenge_2016.html
instances. The novelty of the test instances may be in two ways – 1) the test question-image (QI) pair is “novel”, i.e., too different from training QI pairs; and 2) the test QI pair is “familiar”, but the answer required at test time is “novel”, i.e., answers seen during training are different from what needs to be produced for the test QI pairs.

**Complete question understanding:** To investigate whether a VQA model is understanding the input question or not, we analyze whether the model ‘listens’ to only first few words of the question or the entire question, whether it ‘listens’ to only question (wh) words and nouns or all the words in the question.

**Complete image understanding:** The absence of a large gap between performance of language-alone and language + vision VQA models [27] provides evidence that current VQA models seem to be heavily reliant on the language model, perhaps not really understanding the image. In order to analyze this behavior, we investigate whether the predictions of the model change across images for a given question.

We present our behavioral analyses on the VQA dataset [27]. All the experimental results are reported on the VQA validation set using the following models trained on the VQA train set for the open-ended task –

**CNN + LSTM based model without-attention (CNN+LSTM):** We use the best performing model of [27] (code provided by [279]), which achieves an accuracy of 54.13% on the VQA validation set. It is a two channel model – one channel processes the image (using Convolutional Neural Network (CNN) to extract image features) and the other channel processes the question (using Long Short-Term Memory (LSTM) recurrent neural network to obtain question embedding). The image and question features obtained from the two channels are combined and passed through a fully connected (FC) layer to obtain a softmax distribution over the space of answers.

**CNN + LSTM based model with-attention (ATT):** We use the top-entry on the VQA challenge leaderboard (as of June 03, 2016) [280], which achieves an
accuracy of 57.02% on the VQA validation set. This model jointly reasons about image and question attention, in a hierarchical fashion. The attended image and question features obtained from different levels of the hierarchy are combined and passed through a FC layer to obtain a softmax distribution over the space of answers.

**VQA Challenge 2016 winning entry (MCB):** This is the multimodal compact bilinear (mcb) pooling model from [150] which won the real image track of the VQA Challenge 2016. This model achieves an accuracy of 60.36% on the VQA validation set. In this model, multimodal compact bilinear pooling is used to predict attention over image features and also to combine the attended image features with the question features. These combined features are passed through a FC layer to obtain a softmax distribution over the space of answers.

### 4.2.1 Generalization to novel instances

Do VQA models make mistakes because test instances are too different from training ones? To analyze the first type of novelty (the test QI pair is novel), we measure the correlation between test accuracy and distance of test QI pairs from its k nearest neighbor (k-NN) training QI pairs. For each test QI pair we find its k-NNs in the training set and compute the average distance between the test QI pair and its k-NNs. The k-NNs are computed in the space of combined image + question embedding (just before passing through FC layer) for all the three models (using euclidean distance metric for the CNN+LSTM model and cosine distance metric for the ATT and MCB models).

The correlation between accuracy and average distance is significant (-0.41 at k=50 for the CNN+LSTM model and -0.42 at k=15 for the ATT model). A high negative correlation value tells that the model is less likely to predict correct answers.

---

2 Code available at https://github.com/jiasenlu/HieCoAttenVQA
3 Code available at https://github.com/akirafukui/vqa-mcb
4 k=50 leads to highest correlation
5 k=15 leads to highest correlation
for test QI pairs which are not very similar to training QI pairs, suggesting that the model is not very good at generalizing to novel test QI pairs. The correlation between accuracy and average distance is not significant for the MCB model (-0.14 at k=1\textsuperscript{6}) suggesting that MCB is better at generalizing to novel test QI pairs.

We also found that 67.5\% of mistakes made by the CNN+LSTM model can be successfully predicted by checking distance of test QI pair from its k-NN training QI pairs (66.7\% for the ATT model, 55.08\% for the MCB model). Thus, this analysis not only exposes a reason for mistakes made by VQA models, but also allows us to build human-like models that can predict their own oncoming failures, and potentially refuse to answer questions that are ‘too different’ from ones seen in past.

To analyze the second type of novelty (the answer required at test time is not familiar), we compute the correlation between test accuracy and the average distance of the test ground truth (GT) answer with GT answers of its k-NN training QI pairs. The distance between answers is computed in the space of average Word2Vec [301] vectors of answers. This correlation turns out to be quite high (-0.62) for both CNN+LSTM and ATT models and significant (-0.47) for the MCB model. A high negative correlation value tells that the model tends to regurgitate answers seen during training.

These distance features are also good at predicting failures – 74.19\% of failures can be predicted by checking distance of test GT answer with GT answers of its k-NN training QI pairs for CNN+LSTM model (75.41\% for the ATT model, 70.17\% for the MCB model). Note that unlike the previous analysis, this analysis only explains failures but cannot be used to predict failures (since it uses GT labels). See Fig. 16 for qualitative examples.

From Fig. 16 (row1) we can see that the test QI pair is semantically quite different from its k-NN training QI pairs (\{1st, 2nd, 3rd\}-NN distances are \{15.05, 15.13, 47

\textsuperscript{6}k=1 leads to highest correlation
Figure 16: Examples from test set where the CNN+LSTM model makes mistakes and their corresponding nearest neighbor training instances. See appendix for more examples.

15.17}, which are higher than the corresponding distances averaged across all success cases: \{8.74, 9.23, 9.50,\}, explaining the mistake. Row2 shows an example where the model has seen the same question in the training set (test QI pair is semantically similar to training QI pairs) but, since it has not seen “green cone” for training instances (answers seen during training are different from what needs to be produced for the test QI pair), it is unable to answer the test QI pair correctly. This shows that current models lack compositionality: the ability to combine the concepts of “cone” and “green” (both of which have been seen in training set) to answer “green cone” for the test QI pair. This compositionality is desirable and central to intelligence.

4.2.2 Complete question understanding

We feed partial questions of increasing lengths (from 0-100% of question from left to right). We then compute what percentage of responses do not change when more and more words are fed.
Figure 17: X-axis shows length of partial question (in %) fed as input. Y-axis shows percentage of questions for which responses of these partial questions are the same as full questions and VQA accuracy of partial questions.

Fig. 17 shows the test accuracy and percentage of questions for which responses remain same (compared to entire question) as a function of partial question length. We can see that for 40% of the questions, the CNN+LSTM model seems to have converged on a predicted answer after ‘listening’ to just half the question. This shows that the model is listening to first few words of the question more than the words towards the end. Also, the model has 68% of the final accuracy (54%) when making predictions based on half the original question. When making predictions just based on the image, the accuracy of the model is 24%. The ATT model seems to have converged on a predicted answer after listening to just half the question more often (49% of the time), achieving 74% of the final accuracy (57%). The MCB model converges on a predicted answer after listening to just half the question 45% of the time, achieving 67% of the final accuracy (60%). See Fig. 18 for qualitative examples.

We also analyze the change in responses of the model’s predictions (see Fig. 19),
3.1.1.3 Attention-based models

The CONVATT model (Att) and the MCB model (MCB) are attention-based models. They encode the question and the image, then compute the attention weight for each region in the image and uses it as a weight for the image features. They then combine the weighted image features and the question embedding to generate a final output. The CONVATT model (Att) uses a convolutional layer to generate the attention weights, while the MCB model (MCB) uses a fully connected layer.

4.2.3 Complete image understanding

Does a VQA model really ‘look’ at the image? To analyze this, we compute the percentage of the time (say $X$) the response does not change across images (e.g., answer for all images is “2”) for a given question (e.g., “How many zebras?”) and plot histogram of $X$ across questions (see Fig. 20). We do this analysis for questions occurring for atleast 25 images in the VQA validation set, resulting in total 263 questions. The cumulative plot indicates that for 56% questions, the CNN+LSTM model outputs the same answer for at least half the images. This is fairly high, suggesting that the model is picking the same answer no matter what the image is. Promisingly, the ATT and MCB models (that do not work with a holistic entire-image representation and purportedly pay attention to specific spatial regions in an
image) produce the same response for at least half the images for fewer questions (42% for the ATT model, 40% for the MCB model).

Interestingly, the average accuracy (see the VQA accuracy plots in Fig. 20) for questions for which the models produce same response for >50% and <55% of the images is 56% for the CNN+LSTM model (60% for the ATT model, 73% for the MCB model) which is more than the respective average accuracy on the entire VQA validation set (54.13% for the CNN+LSTM model, 57.02% for the ATT model, 60.36% for the MCB model). Thus, producing the same response across images seems to be statistically favorable. Fig. 21 shows examples where the CNN+LSTM model predicts the same response across images for a given question. The first row shows examples where the model makes errors on several images by predicting the same answer for all images. The second row shows examples where the model is always correct even if it predicts the same answer across images. This is so because questions such as “What covers the ground?” are asked for an image in the VQA dataset only when ground is covered with snow (because subjects were looking at the image while asking questions about it). Thus, this analysis exposes label biases in the
Figure 20: Histogram of percentage of images for which model produces same answer for a given question and its comparison with test accuracy. The cumulative plot shows the % of questions for which model produces same answer for at least $x$ % of images.

dataset. Label biases (in particular, for “yes/no” questions) have also been reported in [505].

<table>
<thead>
<tr>
<th>Correct Response</th>
<th>Incorrect Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q: How many zebras</td>
<td>Predicted A: 2</td>
</tr>
<tr>
<td>Predicted A: 2</td>
<td>Predicted A: 2</td>
</tr>
<tr>
<td>Predicted A: 2</td>
<td>Predicted A: 2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>All Correct Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q: What covers the ground</td>
</tr>
<tr>
<td>Predicted A: snow</td>
</tr>
<tr>
<td>Predicted A: snow</td>
</tr>
<tr>
<td>Predicted A: snow</td>
</tr>
<tr>
<td>Predicted A: snow</td>
</tr>
<tr>
<td>Predicted A: snow</td>
</tr>
</tbody>
</table>

Figure 21: Examples where the predicted answers do not change across images for a given question. See appendix for more examples.

4.3 Conclusion

We develop novel techniques to characterize the behavior of VQA models, as a first step towards understanding these models, meaningfully comparing the strengths and
weaknesses of different models, developing insights into their failure modes, and identifying the most fruitful directions for progress. Our behavior analysis reveals that despite recent progress, today’s VQA models are “myopic” (tend to fail on sufficiently novel instances), often “jump to conclusions” (converge on a predicted answer after ‘listening’ to just half the question), and are “stubborn” (do not change their answers across images), with attention based models being less “stubborn” than non-attention based models.

As a final thought, we note that the somewhat pathological behaviors exposed in the paper are in some sense “correct” given the model architectures and the dataset being trained on. Ignoring optimization error, the maximum-likelihood training objective is clearly intended to capture statistics of the dataset. Our motive is simply to better understand current generation models via their behaviors, and use these observations to guide future choices – do we need novel model classes? or dataset with different biases? etc. Finally, it should be clear that our use of anthropomorphic adjectives such as “stubborn”, “myopic” etc. is purely for pedagogical reasons – to easily communicate our observations to our readers. No claims are being made about today’s VQA models being human-like.
CHAPTER V

OVERCOMING PRIORS IN VISUAL QUESTION ANSWERING

5.1 Visual Question Answering under Changing Priors (VQA-CP)

5.1.1 Introduction

In Chapter 4 we saw that today’s VQA models are heavily driven by superficial correlations in the training data and lack sufficient visual grounding. Similar findings have been reported in other works as well [9, 505, 168, 211]. It seems that when faced with a difficult learning problem, models typically resort to latching onto the language priors in the training data to the point of ignoring the image – e.g., overwhelmingly replying to ‘how many X?’ questions with ‘2’ (irrespective of X), ‘what color is . . . ?’ with ‘white’, ‘is the . . . ?’ with ‘yes’.

One reason for this emergent dissatisfactory behavior is the fundamentally problematic nature of IID train-test splits in the presence of strong priors. As a result, models that intrinsically memorize biases in the training data demonstrate acceptable performance on the test set. This is problematic for benchmarking progress in VQA because it becomes unclear what the source of the improvements is – if models have learned to ground concepts in images or they are driven by memorizing priors in training data.

To help disentangle these factors, we present new splits of the VQA v1 [27] and VQA v2 [168] datasets, called Visual Question Answering under Changing Priors (VQA-CP v1 and VQA-CP v2 respectively). These new splits are created by re-organizing the train and val splits of the respective VQA datasets in such a way
that the distribution of answers per question type ('how many', 'what color is', etc.) is by design different in the test split compared to the train split (Section 5.1.2). One important thing to note: we do not change the distribution of the underlying perceptual signals – the images – between train and test. Generalization across different domains of images (e.g. COCO images vs. webcam images) is an active research area and not the focus of this work. We change the distribution of answers for each question type between train and test. Our hypothesis is that it is reasonable to expect models that are answering questions for the ‘right reasons’ (image grounding) to recognize, for instance, ‘black’ color at test time even though ‘white’ is the most popular answer for ‘What color is the . . . ?’ questions in the train set.

To demonstrate the difficulty of our VQA-CP splits, we report the performance of several existing VQA models [279, 24, 495, 150] on these splits. Our key finding is that the performance of all tested existing models drops significantly when trained and evaluated on the new splits compared to the original splits (Section 5.1.3). This finding provides further confirmation and a novel insight to the growing evidence in literature on the behavior of VQA models [9, 505, 168, 211].

5.1.2 VQA-CP : Dataset Creation and Analysis

The VQA-CP v1 and VQA-CP v2 splits are created such that the distribution of answers per question type ('how many', 'what color is', etc.) is different in the test data compared to the training data. These splits are created by re-organizing the training and validation splits of the VQA v1 [27] and VQA v2 [168] datasets respectively 1, using the following procedure:

**Question Grouping:** Questions having the same question type (first few words of the question – ‘What color is the’, ‘What room is’, etc.) and the same ground truth answer are grouped together. For instance, {‘What color is the dog?’, ‘white’}

---

1We can not use the test splits from VQA datasets because creation of VQA-CP splits requires access to answer annotations, which are not publicly available on the test sets.
and \{‘What color is the plate?’, ‘white’\} are grouped together whereas \{‘What color is the dog?’, ‘black’\} is put in a different group. This grouping is done after merging the QA pairs from the VQA train and val splits. We use the question types provided in the VQA datasets.

**Greedily Re-splitting:** A greedy approach is used to redistribute data points (image, question, answer) to the VQA-CP train and test splits so as to maximize the coverage of the VQA-CP test concepts in the VQA-CP train split while making sure that questions with the same question type and the same ground truth answer are not repeated between test and train splits. In this procedure, we loop through all the groups created above, and in every iteration, we add the current group to the VQA-CP test split unless the group has already been assigned to the VQA-CP train split. We always maintain a set of concepts\(^2\) belonging to the groups in the VQA-CP test split that have not yet been covered by the groups in the VQA-CP train split. We then pick the group that covers majority of the concepts in the set, from the groups that have not yet been assigned to either split and add that group to the VQA-CP train split. We stop when the test split has about 1/3rd the dataset and add the remaining groups (not yet assigned to either split) to the train split.

The above approach results in 98.04% coverage of test question concepts (set of all unique words in questions after removing stop words – ‘is’, ‘are’, ‘the’, etc.) in the train split for VQA-CP v1 (99.01% for VQA-CP v2), and 95.07% coverage of test answers by the train split’s top 1000 answers for VQA-CP v1 (95.72% for VQA-CP v2). VQA-CP v1 train consists of \(~118K\) images, \(~245K\) questions and \(~2.5M\) answers (\(~121K\) images, \(~438K\) questions and \(~4.4M\) answers for VQA-CP v2 train). VQA-CP v1 test consists of \(~87K\) images, \(~125K\) questions and \(~1.3M\) answers (\(~98K\) images, \(~220K\) questions and \(~2.2M\) answers for VQA-CP v2 test).

\(^2\)For a given group, concepts are the set of all unique words present in the question type and the ground truth answer belonging to that group.
Figure 22: Distribution of answers per question type vary significantly between VQA-CP v1 train (left) and test (right) splits. For instance, ‘white’ and ‘red’ are commonly seen answers in train for ‘What color’, whereas ‘black’ is the most frequent answer in test. These have been computed for a random sample of 60K questions.

Fig. 22 shows the distribution of answers for several question types such as ‘what color’, ‘what sport’, ‘how many’, etc. for the train (left) and test (right) splits of the VQA-CP v1 dataset (see appendix for this analysis of the VQA-CP v2 dataset). We can see that the distributions of answers for a given question type is significantly different. For instance, ‘tennis’ is the most frequent answer for the question type ‘what sport’ in VQA-CP v1 train split whereas ‘skiing’ is the most frequent answer for the same question type in VQA-CP v1 test split. However, for VQA v1 dataset, the distribution for a given question type is similar across train and val splits [27] (for instance, ‘tennis’ is the most frequent answer for both the train and val splits). In the VQA-CP v1 splits, similar differences can be seen for other question types as
Table 6: We compare the performance of existing VQA models on VQA-CP v1 test splits (when trained on VQA-CP v1 train splits) to their performance on VQA v1 val splits (when trained on VQA v1 train splits). We find that the performance of all tested existing models degrades significantly in the new Changing Priors setting compared to the original VQA setting.

<table>
<thead>
<tr>
<th>Model</th>
<th>Dataset</th>
<th>Overall</th>
<th>Yes/No</th>
<th>Number</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>per Q-type prior [27]</td>
<td>VQA v1</td>
<td>35.13</td>
<td>71.31</td>
<td>31.93</td>
<td>08.86</td>
</tr>
<tr>
<td></td>
<td>VQA-CP v1</td>
<td>08.39</td>
<td>14.70</td>
<td>08.34</td>
<td>02.14</td>
</tr>
<tr>
<td>d-LSTM Q [27]</td>
<td>VQA v1</td>
<td>48.23</td>
<td>79.05</td>
<td>33.70</td>
<td>28.81</td>
</tr>
<tr>
<td></td>
<td>VQA-CP v1</td>
<td>20.16</td>
<td>35.72</td>
<td>11.07</td>
<td>08.34</td>
</tr>
<tr>
<td>d-LSTM Q + norm I [279]</td>
<td>VQA v1</td>
<td>54.40</td>
<td>79.82</td>
<td>33.87</td>
<td>40.54</td>
</tr>
<tr>
<td></td>
<td>VQA-CP v1</td>
<td>23.51</td>
<td>34.53</td>
<td>11.40</td>
<td>17.42</td>
</tr>
<tr>
<td>NMN [24]</td>
<td>VQA v1</td>
<td>54.83</td>
<td>80.39</td>
<td>33.45</td>
<td>41.07</td>
</tr>
<tr>
<td></td>
<td>VQA-CP v1</td>
<td>29.64</td>
<td>38.85</td>
<td>11.23</td>
<td>27.88</td>
</tr>
<tr>
<td>SAN [495]</td>
<td>VQA v1</td>
<td>55.86</td>
<td>78.54</td>
<td>33.46</td>
<td>44.51</td>
</tr>
<tr>
<td></td>
<td>VQA-CP v1</td>
<td>26.88</td>
<td>35.34</td>
<td>11.34</td>
<td>24.70</td>
</tr>
<tr>
<td>MCB [150]</td>
<td>VQA v1</td>
<td>60.97</td>
<td>81.62</td>
<td>34.56</td>
<td>52.16</td>
</tr>
<tr>
<td></td>
<td>VQA-CP v1</td>
<td>34.39</td>
<td>37.96</td>
<td>11.80</td>
<td>39.90</td>
</tr>
</tbody>
</table>

well – ‘are’, ‘which’.

5.1.3 Benchmarking VQA Models on VQA-CP

To demonstrate the difficulty of our VQA-CP splits, we report the performance of the following baselines and existing VQA models when trained on VQA-CP v1 and VQA-CP v2 train splits and evaluated on the corresponding test splits. We compare this with their performance when trained on VQA v1 and VQA v2 train splits and evaluated on the corresponding val splits. Results are presented in Tables 5.1.2 and 5.1.2.

per Q-type prior [27]: Predicting the most popular training answer for the corresponding question type (e.g., ‘tennis’ for ‘What sport . . .?’ questions). 3

Deeper LSTM Question (d-LSTM Q) [27]: Predicting the answer using question

3Note that, ideally the performance of this baseline on VQA-CP test set should be zero because the answers, given the question type, are different in test and train. But, due to some inter-human disagreement in the datasets, the performance is slightly higher (Tables 5.1.2 and 5.1.2).
Table 7: We compare the performance of existing VQA models on VQA-CP v2 test splits (when trained on VQA-CP v2 train splits) to their performance on VQA v2 val splits (when trained on VQA v2 train splits). We find that the performance of all tested existing models degrades significantly in the new Changing Priors setting compared to the original VQA setting.

<table>
<thead>
<tr>
<th>Model</th>
<th>Dataset</th>
<th>Overall</th>
<th>Yes/No</th>
<th>Number</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>per Q-type prior [27]</td>
<td>VQA v2</td>
<td>32.06</td>
<td>64.42</td>
<td>26.95</td>
<td>08.76</td>
</tr>
<tr>
<td></td>
<td>VQA-CP v2</td>
<td>08.76</td>
<td>19.36</td>
<td>11.70</td>
<td>02.39</td>
</tr>
<tr>
<td>d-LSTM Q [27]</td>
<td>VQA v2</td>
<td>43.01</td>
<td>67.95</td>
<td>30.97</td>
<td>27.20</td>
</tr>
<tr>
<td></td>
<td>VQA-CP v2</td>
<td>15.95</td>
<td>35.09</td>
<td>11.63</td>
<td>07.11</td>
</tr>
<tr>
<td>d-LSTM Q + norm I [279]</td>
<td>VQA v2</td>
<td>51.61</td>
<td>73.06</td>
<td>34.41</td>
<td>39.85</td>
</tr>
<tr>
<td></td>
<td>VQA-CP v2</td>
<td>19.73</td>
<td>34.25</td>
<td>11.39</td>
<td>14.41</td>
</tr>
<tr>
<td>NMN [24]</td>
<td>VQA v2</td>
<td>51.62</td>
<td>73.38</td>
<td>33.23</td>
<td>39.93</td>
</tr>
<tr>
<td></td>
<td>VQA-CP v2</td>
<td>27.47</td>
<td>38.94</td>
<td>11.92</td>
<td>25.72</td>
</tr>
<tr>
<td>SAN [495]</td>
<td>VQA v2</td>
<td>52.02</td>
<td>68.89</td>
<td>34.55</td>
<td>43.80</td>
</tr>
<tr>
<td></td>
<td>VQA-CP v2</td>
<td>24.96</td>
<td>38.35</td>
<td>11.14</td>
<td>21.74</td>
</tr>
<tr>
<td>MCB [150]</td>
<td>VQA v2</td>
<td>59.71</td>
<td>77.91</td>
<td>37.47</td>
<td>51.76</td>
</tr>
<tr>
<td></td>
<td>VQA-CP v2</td>
<td>36.33</td>
<td>41.01</td>
<td>11.96</td>
<td>40.57</td>
</tr>
</tbody>
</table>

alone (“blind” model).

Deeper LSTM Question + normalized Image (d-LSTM Q + norm I) [27]: The baseline VQA model.

Neural Module Networks (NMN) [24]: The model designed to be compositional in nature.

Stacked Attention Networks (SAN) [495]: One of the widely used models for VQA.

Multimodal Compact Bilinear Pooling (MCB) [150]: The winner of the VQA Challenge (on real image) 2016.

Brief descriptions of all of these models are in appendix.

From Tables 5.1.2 and 5.1.2, we can see that the performance of all tested existing VQA models drops significantly in the VQA-CP setting compared to the original VQA setting. Note that even though the NMN architecture is compositional by design, their performance degrades on the VQA-CP datasets. We posit this may
be because they use an additional LSTM encoding of the question to encode priors in the dataset. Also note that the d-LSTM Q + norm I model suffers the largest drop in overall performance compared to other VQA models, perhaps because other models have more powerful visual processing (for instance, attention on images). Another interesting observation from Tables 5.1.2 and 5.1.2 is that the ranking of the models based on overall performance changes from VQA to VQA-CP. For VQA, SAN outperforms NMN, whereas for VQA-CP, NMN outperforms SAN. For a brief discussion on trends for different question types, please see appendix.

5.1.4 Conclusion

In conclusion, we propose a new setting for VQA (VQA under Changing Priors (VQA-CP)) where, for every question type, train and test sets have different prior distributions of answers. We introduce novel splits of the existing VQA v1 and VQA v2 datasets to stress test models under changing priors. Quatitative evaluation of several existing VQA models on these new splits shows that the performance of all tested existing models drops significantly in the proposed Changing Priors setting compared to the existing setting where the train and test distributions of answers given the question type are similar. This finding provides further confirmation that today’s VQA models are largely driven by language priors in the training data and lack sufficient image grounding. Thus, the proposed splits can serve as benchmarks to evaluate the degree of visual groundedness in VQA models.

5.2 Grounded Visual Question Answering (GVQA)

5.2.1 Introduction

In this section, we propose a novel Grounded Visual Question Answering (GVQA) model that contains inductive biases and restrictions in the architecture specifically designed to prevent it from ‘cheating’ by primarily relying on priors in the training data (Section 5.2.2). GVQA is motivated by the intuition that questions in VQA
provide two key pieces of information:

(1) What should be recognized? Or what visual concepts in the image need to be reasoned about to answer the question (e.g., ‘What color is the plate?’ requires looking at the plate in the image),

(2) What should be said? Or what is the space of plausible answers (e.g., ‘What color ...?’ questions need to be answered with names of colors).

Our hypothesis is that models that do not explicitly differentiate between these two roles – which is the case for most existing models in literature – tend to confuse these two signals. They end up learning from question-answer pairs that a plausible color of a plate is white, and at test time, rely on this correlation more so than the specific plate in the image the question is about. GVQA explicitly disentangles the visual concept recognition from the answer space prediction.

GVQA is built off of an existing VQA model – Stacked Attention Networks (SAN) [495]. Our experiments demonstrate that GVQA significantly outperforms SAN on both VQA-CP v1 and VQA-CP v2 datasets (Section 5.2.3). Interestingly, it also outperforms more powerful VQA models such as Multimodal Compact Bilinear Pooling (MCB) [150] in several cases (Section 5.2.3). We also show that GVQA offers strengths complementary to SAN when trained and evaluated on the original VQA v1 and VQA v2 datasets (Section 5.2.5). Finally, GVQA is more transparent than existing VQA models, in that it produces interpretable intermediate outputs unlike most existing VQA models (Section 5.2.6).

5.2.2 GVQA model

We now introduce our Grounded Visual Question Answering model (GVQA). While previous VQA approaches directly map Image-Question tuples \((I, Q)\) to Answers \((A)\), GVQA breaks down the task of VQA into two steps: Look - locate the object / image patch needed to answer the question and recognize the visual concepts in the patch,
Glove Image (I)

Question (Q) 

Visual Concept Classifier (VCC)

Concepts grouped into clusters

Answer Cluster Predictor (ACP)

Concept Extractor (CE)

Answer Predictor (AP)

Visual Verifier (VV)

Figure 23: The proposed Grounded Visual Question Answering (GVQA) model.

and Answer - identify the space of plausible answers from the question and return the appropriate visual concept from the set of recognized visual concepts by taking into account which concepts are plausible. For instance, when GVQA is asked ‘What color is the dog?’, it identifies that the answer should be a color name, locates the patch in the image corresponding to dog, recognizes various visual concepts such as ‘black’, ‘dog’, ‘furry’, and finally outputs the concept ‘black’ because it is the recognized concept corresponding to color. Another novelty in GVQA is that it treats answering yes/no questions as a visual verification task, i.e., it verifies the visual presence/absence of the concept mentioned in the question. For instance, when GVQA is asked ‘Is the person wearing shorts?’, it identifies that the concept whose visual presence needs to be verified is ‘shorts’ and answers ‘yes’ or ‘no’ depending on whether it recognizes shorts or not in the image (specifically, on the patch corresponding to ‘person’).

GVQA is depicted in Figure 23. Given a question and an image, the question first goes through the Question Classifier and gets classified into yes/no or non yes/no. For non yes/no questions, the GVQA components that get activated are – 1) Visual
Concept Classifier (VCC) which takes as input the image features extracted from CNN and $Q_{main}$ given by the question Extractor, 2) Answer Cluster Predictor (ACP) whose input is the entire question. The outputs of VCC and ACP are fed to the Answer Predictor (AP) which produces the answer. For yes/no questions, the GVQA components that get activated are – 1) VCC (similarly to non yes/no), 2) Concept Extractor (CE) whose input is the entire question. The outputs of VCC and CE are fed to the Visual Verifier (VV) which predicts ‘yes’ or ‘no’. We present the details of each component below.

**Visual Concept Classifier (VCC)** is responsible for locating the image patch that is needed to answer the question, as well as producing a set of visual concepts relevant to the located patch. E.g., given ‘What is the color of the bus next to the car?’, the VCC is responsible for attending on the bus region and then outputting a set of concepts such as ‘bus’ and attributes such as its color, count, etc. It consists of a 2-hop attention module based off of Stacked Attention Networks ([495]) followed by a stack of binary concept classifiers. The image is fed to the attention module in the form of activations of the last pooling layer of VGG-Net [410]. To prevent the memorization of answer priors per question type, the question is first passed through a language Extractor, a simple rule that outputs the string (called $Q_{main}$) after removing the question type substring (eg. ‘What kind of’). $Q_{main}$ is embedded using an LSTM and then fed into the attention module. The multi hop attention produces a weighted linear combination of the image region features from VGG-Net, with weights corresponding to the degree of attention for that region. This is followed by a set of fully connected (FC) layers and a stack of $\sim$2000 binary concept classifiers that cover $\sim$95% of the concepts seen in train. VCC is trained with a binary logistic loss for every concept.

The set of VCC concepts is constructed by extracting objects and attributes, pertinent to the answer, from training QA pairs and retaining the most frequent ones.
Object concepts are then grouped into a single group where as attribute concepts are clustered into multiple small groups using K-means clustering in Glove embedding space [346], for a total of $C$ clusters. Concept clustering is required for the purpose of generating negative samples required to train the concept classifiers (for a concept classifier, positive samples are those which contain that concept either in the question or the answer). Since the question does not indicate objects and attributes absent in the image, negative data is generated using the following assumptions: (1) the attended image patch required to answer a question has at most one dominant object in it (2) every object has at most one dominant attribute from each attribute category (e.g., if the color of a bus is red, it can be used as a negative example for all other colors). Given these assumptions, when a concept in a cluster is treated as positive, all other concepts in that cluster are treated as negatives. Note that only a subset of all concept clusters are activated for each question during training, and only these activated clusters contribute to the loss.

**Question Classifier** classifies the input question $Q$ into 2 categories: Yes-No and non Yes-No using a Glove embedding layer, an LSTM and FC layers. Yes-No questions feed into the CE and the rest feed into the ACP.

**Answer Cluster Predictor (ACP)** identifies the type of the expected answer (e.g. object name, color, number, etc.). It is only activated for non yes/no questions. It consists of a Glove embedding layer and an LSTM, followed by FC layers that classify questions into one of the $C$ clusters. The clusters for ACP are created by K-means clustering on (1000) answer classes by embedding each answer in Glove space.\(^5\)

**Concept Extractor (CE)** extracts question concepts from yes/no questions

---

\(^4\)We use $C = 50$ because it gives better clusters than other values. Also, agglomerative clustering results in similar performance as K-means. More details in appendix.

\(^5\)We first create the clusters for ACP using the answer classes. We then create the clusters for VCC by assigning each VCC concept to one of these ACP clusters using Euclidean distance in Glove embedding space.
whose visual presence needs to be verified in the image, using a POS tag based
eextraction system\textsuperscript{6}. E.g., for ‘Is the cone green?’, we extract ‘green’. The extracted
concept is embedded in Glove space followed by FC layers to transform this embedding
to the same space as the VCC concepts so that they can be combined by VV. Please see the description of VV below.

**Answer Predictor (AP):** Given a set of visual concepts predicted by the VCC, and a concept category predicted by the ACP, the AP’s role is to predict the answer. ACP categories correspond to VCC concept clusters (see ACP’s and VCC’s output classes in Fig. 23. The colors denote the correspondence). Given this alignment, the output of the ACP can be easily mapped into a vector with the same dimensions as the VCC output by simply copying ACP dimensions into positions pertaining to the respective VCC cluster dimensions. The resulting ACP embedding is added element-wise to the VCC embedding followed by FC layers and a softmax activation, yielding a distribution over 998 VQA answer categories (top 1000 training answers minus ‘yes’ and ‘no’).

**Visual Verifier (VV):** Given a set of visual concepts predicted by the VCC and the embedding of the concept whose visual presence needs to be verified (given by CE), the VV’s role is to verify the presence/absence of the concept in VCC’s predictions. Specifically, the CE embedding is added element-wise to the VCC embedding followed by FC layers and a softmax activation, yielding a distribution over two categories – ‘yes’ and ‘no’.

**Model Training and Testing:** We first train VCC and ACP on the train split using the cluster labels (for ACP) and visual concept labels (for VCC)\textsuperscript{7}. The inputs to Answer Predictor (and Visual Verifier) are the predictions from VCC and ACP (CE

\textsuperscript{6}We use NLTK POS tagger. Spacy POS tagger results in similar performance. More details in appendix.

\textsuperscript{7}Note that we do not need additional image labels to train VCC, our labels are extracted automatically from the QA pairs. Same for ACP.
Table 8: Performance of GVQA (our model) compared to SAN on VQA-CP datasets. GVQA consistently outperforms SAN.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Model</th>
<th>Overall</th>
<th>Yes/No</th>
<th>Number</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>VQA-CP v1</td>
<td>GVQA (Ours)</td>
<td>39.23</td>
<td>64.72</td>
<td>11.87</td>
<td>24.86</td>
</tr>
<tr>
<td></td>
<td>SAN [495]</td>
<td>26.88</td>
<td>35.34</td>
<td>11.34</td>
<td>24.70</td>
</tr>
<tr>
<td>VQA-CP v2</td>
<td>GVQA (Ours)</td>
<td>31.30</td>
<td>57.99</td>
<td>13.68</td>
<td>22.14</td>
</tr>
<tr>
<td></td>
<td>SAN [495]</td>
<td>24.96</td>
<td>38.35</td>
<td>11.14</td>
<td>21.74</td>
</tr>
</tbody>
</table>

in the case of yes/no questions) on the training data. During training, we use ground truth labels for yes/no and non yes/no questions for the Question Classifier. During testing, we first run the Question Classifier to classify questions into yes/no and non yes/no. And feed the questions into their respective modules to obtain predictions on the test set. Please refer to appendix for implementation details.

5.2.3 Experiments on VQA-CP v1 and VQA-CP v2

Model accuracies: Table 5.2.3 shows the performance of our GVQA model in comparison to SAN (the model which GVQA is built off of) on VQA-CP v1 and VQA-CP v2 datasets using the VQA evaluation metric [27]. Accuracies are presented broken down into Yes/No, Number and Other categories. As it can be seen from Table 5.2.3, the proposed architectural improvements (in GVQA) over SAN show a significant boost in the overall performance for both the VQA-CP v1 (12.35%) and VQA-CP v2 (6.34%) datasets. It is worth noting that owing to the modular nature of the GVQA architecture, one may easily swap in other attention modules into the VCC. Interestingly, on the VQA-CP v1 dataset, GVQA also outperforms MCB [150] and NMN [24] (Tables 5.1.2 and 5.1.2) on the overall metric (mainly for yes/no questions), in spite of being built off of a relatively simpler attention module from SAN, and using relatively less powerful image features (VGG-16) as compared to ResNet-152 being used in MCB. On the VQA-CP v2 dataset, GVQA outperforms NMN in overall metric (as well as for number questions) and MCB for yes/no and number questions.
To check if our particular VQA-CP split was causing some irregularities in performance, we created four sets of VQA-CP v2 splits with different random seeds. This also led to a large portion of the dataset (84%) being covered across the test splits. The results show that GVQA consistently outperforms SAN across all four splits with average improvement being 7.14% (standard error: 1.36). Please see appendix for performance on each split.

**Performance of Model Components**

*Question Classifier:* On the VQA-CP v1 test set, the LSTM based question classifier obtains 99.84% accuracy. *ACP:* The Top-1 test accuracy is 54.06%, with 84.25% for questions whose answers are in attribute clusters and 43.17% for questions whose answers are in object clusters. The Top-3 accuracy rises to 65.33%. Note that these accuracies are computed using the automatically created clusters. *VCC:* The weighted mean test F1 score across all classifiers is 0.53. The individual concepts are weighted as per the number of positive samples, reflecting the coverage of that concept in the test set. Please refer to appendix for accuracies on the VQA-CP v2 dataset.

### 5.2.4 Role of GVQA Components

In order to evaluate the role of various GVQA components, we report the experimental results (on VQA-CP v1) by replacing each component in GVQA (denoted by "-<component>") with its traditional counterpart, i.e., modules used in traditional VQA models (denoted by "+<traditional counterpart>"). For instance, GVQA - CE + LSTM represents a model where CE in GVQA has been replaced with an LSTM. The results are presented in Table 5.2.4 along with the result of the full GVQA model for reference.

**GVQA - \(Q_\text{main} + Q_\text{full}\):** GVQA’s performance when the entire question (\(Q_\text{full}\)) is fed into VCC (as opposed to after removing the question type (\(Q_\text{main}\))) is 33.55% (overall), which is 5.68% (absolute) less than that with \(Q_\text{main}\). Note that even with
feeding the entire question, GVQA outperforms SAN, thus demonstrating that removing question type information helps but isn’t the main factor behind the better performance of GVQA. As an additional check, we trained a version of SAN where the input is $Q_{main}$ instead of $Q_{full}$. Results on VQA-CP v2 show that this version of SAN performs 1.36% better than the original SAN, however still 4.98% worse than GVQA (with $Q_{main}$). Please see appendix for detailed performance of this version of SAN.

**GVQA - CE + LSTM:** We replace CE with an LSTM (which is trained end-to-end with the Visual Verifier (VV) using VQA loss). The overall performance drops by 11.95%, with a drop of 28.76% for yes/no questions. This is an expected result, given that Table 5.2.3 shows that GVQA significantly outperforms SAN on yes/no questions and the CE is a crucial component of the yes/no pipeline.

**GVQA - ACP + LSTM:** We replace ACP with an LSTM (which is trained end-to-end with the Answer Predictor (AP) using VQA loss). The overall performance is similar to GVQA. But, the presence of ACP makes GVQA transparent and interpretable (see Section 5.2.6).

**GVQA - VCC loss:** We remove the VCC loss and treat the output layer of VCC as an intermediate layer whose activations are passed to the Answer Predictor (AP) and trained end-to-end with AP using VQA loss. The overall performance improves by 1.72% with biggest improvement in the performance on other questions (3.19%). This suggests that introducing the visual concept (semantic) loss in between the model pipeline hurts. Although removing VCC loss and training end-to-end with VQA loss achieves better performance, the model is no longer transparent (see Section 5.2.6). Using VCC loss or not is a design choice one would make based on the desired accuracy vs. interpretability trade off.

**GVQA - VCC loss - ACP + LSTM:** Replacing ACP with an LSTM on top of GVQA - VCC loss hurts the overall performance by 2.09% with biggest drop
Table 9: Experimental results when each component in GVQA (denoted by “-\text{<component>}>”) is replaced with its corresponding traditional counterpart (denoted by “ + \text{<traditional counterpart>}>”).

<table>
<thead>
<tr>
<th>Model</th>
<th>Overall</th>
<th>Yes/No</th>
<th>Number</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>GVQA - $Q_{main} + Q_{full}$</td>
<td>33.55</td>
<td>51.64</td>
<td>11.51</td>
<td>24.43</td>
</tr>
<tr>
<td>GVQA - CE + LSTM</td>
<td>27.28</td>
<td>35.96</td>
<td>11.88</td>
<td>24.85</td>
</tr>
<tr>
<td>GVQA - ACP + LSTM</td>
<td>39.40</td>
<td>64.72</td>
<td>11.73</td>
<td>25.33</td>
</tr>
<tr>
<td>GVQA - VCC_{loss}</td>
<td>40.95</td>
<td>65.50</td>
<td>12.32</td>
<td>28.05</td>
</tr>
<tr>
<td>GVQA - VCC_{loss} - ACP + LSTM</td>
<td>38.86</td>
<td>65.73</td>
<td>11.58</td>
<td>23.11</td>
</tr>
<tr>
<td>GVQA</td>
<td>39.23</td>
<td>64.72</td>
<td>11.87</td>
<td>24.86</td>
</tr>
</tbody>
</table>

Table 10: Results of GVQA and SAN on VQA v1 and VQA v2 when trained on the corresponding train splits.

<table>
<thead>
<tr>
<th>Model</th>
<th>VQA v1</th>
<th>VQA v2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle (GVQA, SAN)</td>
<td>63.77</td>
<td>61.96</td>
</tr>
<tr>
<td>Oracle (SAN, SAN)</td>
<td>60.85</td>
<td>56.68</td>
</tr>
<tr>
<td>Ensemble (GVQA, SAN)</td>
<td>56.91</td>
<td>52.96</td>
</tr>
<tr>
<td>Ensemble (SAN, SAN)</td>
<td>56.56</td>
<td>52.45</td>
</tr>
<tr>
<td>SAN</td>
<td>55.86</td>
<td>52.02</td>
</tr>
<tr>
<td>GVQA</td>
<td>51.12</td>
<td>48.24</td>
</tr>
</tbody>
</table>

(4.94%) for “other” questions (see GVQA - VCC_{loss} and GVQA - VCC_{loss} - ACP + LSTM rows in Table 5.2.4). This suggests that ACP helps significantly (as compared to an LSTM) in the absence of VCC loss (and it performs similar to an LSTM in the presence of VCC loss, as seen above). In addition, ACP adds interpretability to GVQA.

5.2.5 Experiments on VQA v1 and VQA v2

We also trained and evaluated GVQA on train and val splits of the VQA v1 [27] and VQA v2 [168] datasets (results in Table 5.2.5\(^8\)). On VQA v1, GVQA achieves 51.12% overall accuracy, which is 4.74% (absolute) less than SAN. This gap is not surprising because VQA v1 has well-established heavy language priors that existing

\(^8\)We present overall and yes/no accuracies only. Please refer to appendix for performance on number and other categories.
models (including SAN) can “memorize” from train set and exploit on the test set (since test set contains same priors as train set), whereas GVQA is designed not to. As vision improves, grounded models like GVQA may show improved performance over models that leverage priors from training data. Moreover, it is important to note that the gain (GVQA acc - SAN acc) on VQA-CP v1 (12.35% absolute) is much higher than the loss (SAN acc - GVQA acc) on VQA v1 (4.74% absolute).

On VQA v2, GVQA underperforms SAN by 3.78% overall, which is less than SAN acc - GVQA acc on VQA v1. And it outperforms SAN by 3.14% for yes/no questions. This shows that when the priors are weaker (in VQA v2 compared to those in VQA v1), the gap between GVQA and SAN’s performance decreases. We also trained and evaluated GVQA- VCC\textsubscript{loss} on both the VQA v1 and VQA v2 datasets and found that it performs worse than GVQA on VQA v1 and similar to GVQA on VQA v2. So in addition to interpretability, GVQA is overall better than GVQA- VCC\textsubscript{loss} on these original VQA splits.

In order to check whether GVQA has strengths complementary to SAN, we computed the oracle of SAN’s and GVQA’s performance – Oracle (GVQA, SAN), i.e., we pick the predictions of the model with higher accuracy for each test instance. As it can be seen from Table 5.2.5, the Oracle (GVQA, SAN)’s overall performance is 7.91% higher than that of SAN for VQA v1 (9.94% for VQA v2) suggesting that GVQA and SAN have complementary strengths. Also, note that Oracle (GVQA, SAN) is higher than Oracle (SAN, SAN) for both VQA v1 and VQA v2, suggesting that GVQA’s complementary strengths are more than that of another SAN model (with a different random initialization).

Inspired by this, we report the performance of the ensemble of GVQA and SAN Ensemble (GVQA, SAN) in Table 5.2.5, where the ensemble combines the outputs from the two models using product of confidences of each model. We can see that Ensemble (GVQA, SAN) outperforms Ensemble (SAN, SAN) by 0.35% overall for
VQA v1 (and by 0.51% for VQA v2). It is especially better for yes/no questions. We also found that the ensemble of GVQA- \( VCC_{\text{loss}} \) with SAN performs worse than Ensemble (SAN, SAN) for both the VQA datasets (refer to appendix for accuracies). Hence, GVQA is a better complement of SAN than GVQA- \( VCC_{\text{loss}} \), in addition to being more transparent.

5.2.6 Transparency

![Figure 24: Qualitative examples from GVQA. Left: We show top three answer cluster predictions (along with random concepts from each cluster) by ACP. Corresponding to each cluster predicted by ACP, we show the top visual concept predicted by VCC. Given these ACP and VCC predictions, the Answer Predictor (AP) predicts the correct answer ‘baseball’. Right: Smiling is the concept extracted by the CE whose visual presence in VCC’s predictions is verified by the Visual Verifier, resulting in ‘yes’ as the final answer.](image)

The architecture design of GVQA makes it more transparent than existing VQA models because it produces interpretable intermediate outputs (the outputs of VCC, ACP and the concept string extracted by the CE) unlike most existing VQA models.
What color are the bananas?

VCC says: bananas, green, many, food, 50
ACP says answer should be a color
GVQA answers green ✓
SAN answers yellow

What color are his pants?

VCC says: dirt, black, pants, 1, baseball, park
ACP says answer should be a color
GVQA answers black ❌
SAN answers blue

Figure 25: Left: GVQA’s prediction (‘green’) can be explained as follows – ACP predicts that the answer should be a color. Of the various visual concepts predicted by VCC, the only concept that is about color is green. Hence, GVQA’s output is ‘green’. SAN incorrectly predicts ‘yellow’. SAN’s architecture doesn’t facilitate producing an explanation of why it predicted what it predicted, unlike GVQA. Right: Both GVQA and SAN incorrectly answer the question. GVQA is incorrect perhaps because VCC predicts ‘black’, instead of ‘gray’. In order to dig further into why VCC’s prediction is incorrect, we can look at the attention map (in appendix), which shows that the attention is on the pants for the person’s left leg, but on the socks (black in color) for the person’s right leg. So, perhaps, VCC’s “black” prediction is based on the attention on the person’s right leg.

We show some example predictions from GVQA in Fig. 24. We can see that the intermediate outputs provide insights into why GVQA is predicting what it is predicting and hence enable a system designer to identify the causes of error. This is not easy to do in existing VQA models. Fig. 25 shows two other examples (one success and one failure) comparing and contrasting how GVQA’s intermediate outputs can help explain successes and failures (and thus, enabling targeted improvements) which is not possible to do for SAN and most other existing VQA models. See appendix for more such examples.
5.2.7 Conclusion

In this work, we proposed a novel Grounded Visual Question Answering model (GVQA) that contains inductive biases and restrictions in the architecture specifically designed to prevent the model from ‘cheating’ by primarily relying on priors in the training data. Specifically, GVQA explicitly disentangles the recognition of visual concepts present in the image from the identification of plausible answer space for a given question, enabling the model to more robustly generalize across different distributions of answers. GVQA is built off an existing VQA model – Stacked Attention Networks (SAN). Our experiments demonstrate that GVQA significantly outperforms SAN on both VQA-CP v1 and VQA-CP v2 datasets. Interestingly, it also outperforms more powerful VQA models such as Multimodal Compact Bilinear Pooling (MCB) in several cases. GVQA offers strengths complementary to SAN when trained and evaluated on the original VQA v1 and VQA v2 datasets. Finally, GVQA is more transparent and interpretable than existing VQA models.

GVQA is a first step towards building models which are visually grounded by design. Future work involves developing models that can utilize the best of both worlds (visual grounding and priors), such as, answering a question based on the knowledge about the priors of the world (sky is usually blue, grass is usually green) when the model’s confidence in the answer predicted as result of visual grounding is low.

5.3 Adversarial Regularization for Visual Question Answering

5.3.1 Introduction

In Section 5.2, we saw that GVQA is more robust to changing priors than existing VQA models. Although GVQA can be built on top of any existing VQA model, it does require non-trivial changes in the architecture. In this section, we propose
a simple drop-in regularizer for achieving robustness against changing priors. This regularizer can be added to any existing VQA model’s objective function, without requiring significant changes in the underlying VQA model’s architecture. Below we discuss the motivation and the intuition behind the proposed regularization scheme.

One intuitive measure of the strength of language priors in VQA is the performance of a ‘blind’ model that produces answers given only the question and not the associated image. In fact, this question-only model has become a standard and powerful baseline presented alongside VQA datasets [27, 167, 106, 218]. In this work, we codify this intuition, introducing a novel regularization scheme that sets a base VQA model against a question-only adversary to reduce the impact of language biases.

We consider unwanted language bias in VQA to be overly-specific relationships between questions and their likely answers learned from the training dataset – i.e. those that could enable a question-only model to achieve relatively high performance without ever seeing an image – and we explicitly optimize the question representation within a base VQA model to be uninformative to a question-only adversary model. In this adversarial regime, the question-only model is trained to answer as accurately as possible given the question encoding provided by the base VQA model; and simultaneously, the base VQA model is trained to adjust its question encoder (often implemented as a recurrent language model) to minimize the performance of the question-only model while maintaining its own VQA accuracy. Moreover, we leverage the question-only model to provide a differentiable notion of image grounding – the change in model confidence after considering the image – which we maximize explicitly for the VQA model. Thus, our objective consists of a question-only adversarial term and a difference of entropies term.

Our approach is largely model agnostic, end-to-end trainable, and simple to implement, consisting of a small, additional classification network built on the question representation of the base VQA model. We experiment on the VQA-CP dataset with
Figure 26: Given an arbitrary base VQA model (A), we introduce two regularizers. First, we build a question-only adversary (B) that takes the question embedding $q_i$ from the VQA model and is trained to output the correct answer from this information alone. For this network to succeed, $q_i$ must capture language biases from the dataset – the same biases that lead the base VQA model to ignore visual content. To reduce these biases, we set the base VQA model and the question-only adversary against each other, with the base VQA network modifying its question embedding to reduce question-only performance (shown here as gradient negation of the question-only model loss) Further, the question-only model allows estimation of the change in answer confidence given image (C), which we maximize explicitly.

multiple base VQA models, and find – 1) our approach provides consistent improvements over all baseline VQA models, 2) our approach outperforms the GVQA model significantly, 3) both question-only adversary and the difference of entropies components improve performance and their combination pushes this even further. On standard benchmarks [27, 167] where strong priors from training can be exploited on test set, our approach shows significantly smaller drops in accuracy compared to GVQA, with some settings facing only insignificant changes.

5.3.2 Reducing Language Bias Through Adversarial Regularization

Setting aside architectural specifics, the vast majority of VQA models operate on a set of similar design principles – first producing vector representations for the image and question and then combining them to predict the answer (often through complex attention mechanisms). However, when language biases are quite strong, the question feature may already be sufficiently discriminative and the model can learn to ignore
the visual signal without facing significant losses during training (e.g. “What color is the sky?” always mapping to “blue”). Such a model which fails to ground its answers in the image might be passable for benchmark datasets that carry similar biases; however, in the real-world, where brown grass and gray skies abound, its usefulness would be severely limited. In this section, we address this problem by explicitly reducing the discriminative power of the question feature – introducing a pair of adversarial regularizers that penalize the ability of a separate adversary network to confidently predict the answer from the question encoding alone.

**Preliminaries.** Given a dataset \( D = \{I_i, Q_i, a_i\}_{i=1}^N \) consisting of triplets of images \( I_i \in \mathcal{I} \), questions \( Q_i \in \mathcal{Q} \) and answers \( a_i \in \mathcal{A} \), the VQA task is to learn a mapping \( F : \mathcal{Q} \times \mathcal{I} \to [0, 1^{|\mathcal{A}|}] \) which produces an accurate distribution over the answer space given an input question-image pair.

Without loss of generality, we consider differentiable mappings that can be decomposed as an operation \( f \) over question and image encodings \( g : \mathcal{Q} \to \mathbb{R}^d \) and \( h : \mathcal{I} \to \mathbb{R}^k \) (as shown in Figure 26A). We write the prediction for instance \( i \) for this class of models as

\[
\begin{align*}
    v_i &= h(I_i), \quad q_i = g(Q_i) \\
    P(A | Q_i, I_i) &= f(v_i, q_i) \tag{1}
\end{align*}
\]

where we denote the image and question embeddings as \( v_i \) and \( q_i \) respectively.

Nearly all existing VQA models follow this pattern. The image encoder \( h(\cdot) \) is typically a fixed CNN pretrained on either classification or detection and the question encoder \( g(\cdot) \) is usually some form of word or character level RNN learned during training. Typically these models are trained with standard cross-entropy, optimizing parameters to minimize (2) over the ground truth data.

\[
\mathcal{L}_{VQA}(f, g, h) = \mathbb{E}_{\mathcal{I}, \mathcal{Q}, \mathcal{A}} \left[ - \log P_f(a_i|Q_i, I_i) \right] \approx -\frac{1}{N} \sum_{i=1}^N \log f(v_i, q_i)[a_i] \tag{2}
\]

**Question-Only Model.** One intuitive measure of the power of language priors in
VQA is the ability of a model to make low-error answer predictions from the question alone – in fact, some form of this ‘blind’ model has been frequently presented alongside VQA datasets for exactly this purpose [27, 167, 106, 218]. We formalize this question-only model as a mapping $f_Q$. As above, we assume $f_Q$ is differentiable and operates on learned question encodings such that $f_Q$ makes predictions

$$P_{f_Q}(A | Q_i) = f_Q(q_i), \quad q_i = g(Q_i).$$

(3)

We parameterize this model as a simple two-layer neural network but note that arbitrary choices can be made in this regard. As above, this model can be trained with cross-entropy, minimizing

$$\mathcal{L}_{QA}(f_Q, g) = \mathbb{E}_{Q,A} \left[ -\log P_{f_Q}(a_i | Q_i) \right] \approx -\frac{1}{N} \sum_{i=1}^{N} \log f_Q(q_i)[a_i].$$

(4)

5.3.2.1 Adversarial Regularization with a Question-Only Adversary

For any model of the form presented in (1), we can now introduce a simple adversarial regularizer that explicitly reduces the effect of language biases by modifying the question encoder to minimize the performance of this question-only adversary. Specifically, given a VQA model decomposed as $f, g, h$, we splice on the question-only model $f_Q$ such that $f_Q$ takes as input the encodings produced by $g(\cdot)$ (as in Figure 26), and establish opposing losses for the two networks which we detail below.

**Learning the Question-Only Adversary.** The question-only model $f_Q$ is trained to minimize the cross-entropy loss $\mathcal{L}_Q$ in (4); however, parameters in $g(\cdot)$ are not updated with respect to this loss – in effect, this forces $f_Q$ to perform as well as possible given the question encodings produced by the question encoder $g(\cdot)$ from the base VQA model.

**Adversarial Regularization for VQA.** As performance of the question-only model acts as a proxy for the language biases represented in the question encodings $q_i =$
\( g(Q_i) \), one approach to reduce bias representation is to adjust \( g(\cdot) \) such that the question-only model does poorly. As such, we can write this adversarial relationship between the question-only \( (f_Q) \) and base VQA models \( (f, g, h) \) as

\[
\min_{f, g, h} \max_{f_Q} \mathcal{L}_{VQA}(f, g, h) - \lambda \mathcal{L}_{QA}(f_Q, g) \quad (5)
\]

We note that in practice, training with this adversarial regularizer can be realized with a simple gradient negation of the question-only adversary’s loss as shown in Figure 26. Specifically, we back-propagate the negative of the gradient of \( \mathcal{L}_{Q}(f_Q, g) \) accumulated at \( q_i \) through the question encoder – updating the question encoder in a way that maximizes \( \mathcal{L}_{Q}(f_Q, g) \).

The regularization coefficient \( \lambda_Q \geq 0 \) in (5) controls the trade-off between VQA performance and language bias reduction. For low values of \( \lambda_Q \), little regularization occurs and the base model continues to learn language priors. On the other hand, large values of \( \lambda_Q \) force the model to remove all discriminative language biases, resulting in poor VQA performance for both the base VQA model and the question-only adversary – essentially stripping the question encoding of even basic question-type information \( \text{(e.g. failing to learn that “What color ... ?” questions require color answers).} \)

5.3.2.2 An Adversarial Difference of Entropies Regularizer

As the effect of this over-regularization for high-values of \( \lambda_Q \) highlights, the question-only adversary does not capture the full nuance of language bias in VQA. Given the question “What color is the sky?” it is reasonable to have a prior that the answer may be “blue”, but critically this belief should update depending on observations – i.e. the answer distribution should sharpen after viewing the image.

To capture this intuition, we add an additional term that aims to maximize the information gained about the answer from looking at the image. Specifically, we introduce another adversarial regularizer corresponding to the difference in entropies
between the base model prediction given the image and the question-only model which we write as

\[ L_H(f, g, h, f_Q) = E_{I,Q}[H(A | Q) - H(A | I, Q)] \]  

(6)

\[ = E_{q \sim P(Q)}[H(A | q)] - E_{q,v \sim P(Q,I)}[H(A | q, v)] \]  

(7)

\[ \approx \frac{1}{N} \sum_{i=1}^{N} \left( H(f_Q(q_i)) - H(f(v_i, q_i)) \right) \]  

(8)

We note that this regularizer resembles the conditional mutual information (CMI) between the answer and image given the question \( I(A; I|Q) \); however, \( f_Q(q) \) is not constrained to be the marginal of \( f(v, q) \) such that estimating the CMI in this way is ill-defined.

We can then update the adversarial relationship between \( f \) and \( f_Q \) from (5) with \( L_{MI} \), writing

\[ \min_{f, g, h} \max_{f_Q} L_{VQA}(f, g, h) - \lambda_Q L_{QA}(f_Q, g) - \lambda_H L_H(f, g, h, f_Q) \]  

(9)

where \( \lambda_H \geq 0 \) controls the strength of the difference of entropies regularizer. Note that while \( L_H \) is a function of \( f, g, h, \) and \( f_Q \), we only update the parameters of the question encoding \( g \) based on this loss. Otherwise, \( f_Q \) could learn to produce sharp output distributions from arbitrary question features to minimize \( L_H \). Likewise, \( f \) or \( h \) can easily adjust to produce arbitrarily peaky outputs, which we observe can lead to significant over-fitting.

As before, the question-only adversary \( f_Q \) in this setting must still perform as well as possible given the question embedding from \( g(\cdot) \), but this embedding is now additionally adjusted to maximize the entropy of \( f_Q \)’s output, while minimizing that of the VQA model. In the experiments that follow, we show that both of these adversarial regularizers improve performance on a language bias sensitive task. Further, we note that their benefits compound, with models combining both terms performing better across a wider range of regularization coefficients.
### 5.3.3 Experiments

**Implementation.** Our question-only adversary model is implemented as a 2-layer multi-layer perceptron with 256 hidden units and a ReLU activation that takes as input the question encoding from a base VQA network. The network’s output is a distribution over the candidate answers. We train the entire system (base VQA and question-only model) end-to-end with parameters initialized from scratch. We set batch size to 150, learning rate to 0.001, weight decay of 0.999 and use the Adam optimizer. The model takes \(\sim 8\) hours to train on a TITAN X for SAN (Torch, \(\sim 60\) epochs) and \(< 1\) hour for UpDown (PyTorch, \(\sim 40\) epochs). We use public codebases for both.

As discussed in Section 5.3.2, we update the parameters of the question encoding with respect to the VQA loss, the difference of entropies loss, and the negative of the question-only loss. The remaining VQA model parameters are trained with just the VQA loss. The question-only model is updated only by its VQA loss cross entropy loss term despite contributing to the difference of entropies loss.

**Models.** We evaluate the effect of our proposed regularization on the following base models:

- **Stacked Attention Network (SAN) [493]** – SAN encodes questions with a long short-term memory (LSTM) encoder and the image is encoded with a pretrained VGGNet [411]. The model performs two-hop question-based image attention and the final joint feature is passed to a 1000-way answer classifier. This model is trained with standard cross-entropy.

- **Bottom-Up and Top-Down Attention (UpDn) [21]** – Up-Down encodes questions with a gated recurrent unit (GRU) encoder and represents images as a set of bounding box features extracted from Faster R-CNN [371]. Soft-attention
over these regions is computed based on the question features and the attention-pooled feature is combined with the question as input to the classification layer. This model is trained directly on VQA score under a multi-label binary cross-entropy loss (see [21] for more details). We also apply this loss for the question-only model in our experiments, but compute a softmax over these outputs when computing entropies.

For both SAN\(^9\) and Up-Down\(^{10}\), we build on top of publicly available reimplementations. In the following results, we indicate the addition of our question-only adversarial regularization with \textbf{Q-Adv} and the difference of entropies term as \textbf{DoE}.

We also compare to the GVQA model built atop SAN. As we saw in Section 5.2, GVQA explicitly separates perception from question answering by introducing a Visual Concept Classifier (VCC) and an Answer Cluster Predictor (ACP). By design, this model isolates the answering module from the input question, mitigating the effect of language biases, but at a cost of relatively low standard VQA performance and multi-stage training.

**Datasets and Evaluation.** We train our models on the VQA-CP [13] train split and evaluate on the test set using the standard VQA evaluation metric [27]. For each model, we also report results when trained and evaluated on the standard VQA train and validation splits [27, 167] with the same regularization coefficients used for VQA-CP to compare with [13].

VQA-CP does not have a validation set and generating such a split is complicated by the need for it to contain priors different from both the training and test sets in order to be an accurate estimate of generalization under changing priors — an ill-defined notion for binary questions. As such, we set initial regularizer coefficients such that gradients at the question encoding are roughly equal in magnitude for all

\(^9\)SAN Codebase: https://github.com/abhshkdz/neural-vqa-attention

\(^{10}\)Up-Down Codebase: https://github.com/hengyuan-hu/bottom-up-attention-vqa
Table 11: Performance on VQA-CP v2 test and VQA v2 val. We significantly improve the accuracy of base models and achieve state-of-the-art performance on the VQA-CP dataset.

<table>
<thead>
<tr>
<th>Model</th>
<th>(\lambda_Q)</th>
<th>(\lambda_H)</th>
<th>VQA-CP v2 test</th>
<th>VQA v2 val</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Overall</td>
<td>Yes/No</td>
<td>Number</td>
</tr>
<tr>
<td>SAN [493]</td>
<td>-</td>
<td>-</td>
<td>24.96</td>
<td>38.35</td>
</tr>
<tr>
<td>SAN + Q-Adv</td>
<td>0.15</td>
<td>-</td>
<td>27.24</td>
<td>54.50</td>
</tr>
<tr>
<td>SAN + DoE</td>
<td>-</td>
<td>25</td>
<td>25.75</td>
<td>42.21</td>
</tr>
<tr>
<td>SAN + Q-Adv + DoE</td>
<td>0.15</td>
<td>25</td>
<td>33.29</td>
<td>56.65</td>
</tr>
<tr>
<td>UpDn [21]</td>
<td>-</td>
<td>-</td>
<td>39.74</td>
<td>42.27</td>
</tr>
<tr>
<td>UpDn + Q-Adv</td>
<td>0.005</td>
<td>-</td>
<td>40.08</td>
<td>42.34</td>
</tr>
<tr>
<td>UpDn + DoE</td>
<td>-</td>
<td>0.05</td>
<td>40.43</td>
<td>42.62</td>
</tr>
<tr>
<td>UpDn + Q-Adv + DoE</td>
<td>0.005</td>
<td>0.05</td>
<td>41.17</td>
<td>65.49</td>
</tr>
</tbody>
</table>

loss terms at the beginning of training and then explore a small region around this point. We report the best performing coefficients alongside our results and provide further analysis of the effect of these parameters in Section 5.3.4. Notably, we find these coefficients to be highly model dependent but generalize well between datasets and regularizer ablations. All models are trained until convergence as we have no validation set on which to base early-stopping.

5.3.4 Results

Table 11 presents our primary results on both the VQA-CP v2 and the VQA v2 datasets. Table 12 also shows limited results on the much more biased VQA v1 dataset [27] and its CP counterpart – VQA-CP v1 [13]. We make a number of observations below.

The proposed regularizers help, resulting in state-of-art performance on VQA-CP. For both SAN and UpDn models, adding the question-only adversary (Q-Adv) improves the performance of the respective base models (2.28% for SAN and 0.34% for UpDn) on the VQA-CP v2 dataset. Similarly, the difference of entropies (DoE) regularizer boosts the performance of both SAN and UpDn models, gaining improvements of 0.79% and 0.69% respectively. The combination of the Q-Adv and
Table 12: Performance on VQA-CP v1 test and VQA v1 val.

<table>
<thead>
<tr>
<th>Model</th>
<th>$\lambda_Q$</th>
<th>$\lambda_H$</th>
<th>VQA-CP v1 test</th>
<th>VQA v1 val</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Overall</td>
<td>Yes/No</td>
</tr>
<tr>
<td>GVQA [13]</td>
<td>-</td>
<td>-</td>
<td>39.23</td>
<td>64.72</td>
</tr>
<tr>
<td>SAN [493]</td>
<td>-</td>
<td>-</td>
<td>26.88</td>
<td>35.34</td>
</tr>
<tr>
<td>Ours</td>
<td>0.15</td>
<td>-</td>
<td>28.02</td>
<td>35.70</td>
</tr>
<tr>
<td>Ours</td>
<td>-</td>
<td>25</td>
<td>27.83</td>
<td>36.33</td>
</tr>
<tr>
<td>Ours</td>
<td>0.15</td>
<td>25</td>
<td><strong>43.43</strong></td>
<td><strong>74.16</strong></td>
</tr>
</tbody>
</table>

DoE regularizers further boosts the performance, resulting in 8.33% improvement over SAN and 1.43% over UpDn. Comparing our SAN + Q-Adv + DoE model to GVQA which is also built on top of SAN, we outperform GVQA significantly (1.99%). Our UpDn + Q-Only + DoE model also sets a new state-of-the-art on VQA-CP v2, improving over GVQA by 9.87% (although it is important to note the more powerful base architecture already outperforms GVQA by 8.44%).

Similar trends repeat for VQA-CP v1 as well. With the question-only regularizer improving SAN by 1.14%, DoE by 0.95%, and their combination by over 16.55% – outperforming GVQA by 4.2% and again setting state-of-the-art. We note that these larger gains are in part due to the increased language biases present in the VQA-CP v1 dataset.

Moreover, we find the question-only network performs increasingly poorly as our models perform better on VQA-CP – indicating that optimization is going well and that the intuition behind our regularizers seems well-founded.

The proposed regularizers do not hurt significantly on VQA v2. When trained and tested on the VQA v2 dataset (right side of Table 11), the addition of the proposed regularizers results in a insignificant drop in the performance for SAN (0.1%) and a minor drop in performance for UpDn (0.73%) compared to prior work. This is in contrast to GVQA, whose performance drops by 4.17% for SAN on VQA v2 (note that GVQA is built off of SAN).

The more the biases, the higher the gain on VQA-CP, and the higher the
**loss on VQA.** VQA v1 has significantly more bias than VQA v2 and consequentially VQA-CP v1 has a sharper change between training and test. As such, we observe the proposed regularizers improve over the base model significantly more in VQA-CP v1 (16.55% for SAN) than in VQA-CP v2 (8.33% for SAN). For the same reasons, the proposed regularizers hurt a bit more on VQA v1 (3.71% for SAN compared to 0.1% on VQA v2), where strong language biases can be leveraged to boost performance. However, this drop in the performance on VQA v1 is still significantly less than that with GVQA (4.74%).

**UpDn [21] is less driven by biases than SAN.** The drop in the performance of UpDn from VQA v2 to VQA-CP v2 is 23.74% which is significantly less than that of SAN (27.45%). This shows that UpDn may be less driven by biases than SAN. And hence, the gains in UpDn (1.43%) due to the proposed regularizers are less than those in SAN (8.33%).

**Our approach results in less biased output distributions.** Figure 28 shows answer frequency distributions for VQA v2 train, SAN, our SAN+Q-Adv+DoE model (marked Ours), and VQA v2 test for three questions: “What color is the dress she/he is wearing?” “What sport ...?” “What color is the fire hydrant?” It is quite clear that while neither of the SAN based models completely match the test distribution, the base SAN model aligns significantly more with the training distribution – even amplifying the bias for ‘blue’ in the first question despite very few answers being ‘blue’ in test.

**Difference of entropies (DoE) stabilizes training with the question-only adversary.** Figure 27 shows VQA-CP v2 test performance of the SAN model, for a range of question-only regularizer coefficients $\lambda_Q$. We can see that when the DoE term is not used (orange line), performance begins to drop after approximately 0.2 and by 0.35 has deteriorated significantly. At these higher values, nearly all discriminative information in the question encoding is lost – with the VQA model sacrificing its own
Figure 27: Maximizing difference of entropies (DoE) along with the question-only adversarial regularization for the SAN model, not only improves results on changing priors, but also stabilizes training.

Figure 28: Answer distribution for SAN+Q-Adv+DoE mimic the prior less for questions with high language bias.
performance to lower that of the question-only model. However, we observe that for reasonable values of $\lambda_H$, the strength of the question-only adversary can be varied over a much wider range with less dramatic losses (blue curve in Figure 27). We observe a similar trend when keeping $\lambda_Q$ constant and sweeping over $\lambda_H$, wherein a dramatic improvement is observed when moving to non-zero $\lambda_H$ and then a slow decay for large values of $\lambda_H$. Unlike the question-only adversary, the DoE regularizer simultaneously seeks to sharpen the VQA models posterior while weakening the question-only prior.

**Question-only performance:** We study the performance of the question-only model after being trained on VQA-CP v2 using our regularizers. We compare to a question-only model trained without these regularizers, i.e. a model trained to predict the correct answer given the question-encoding learned by the base VQA model. We find this Q-only(SAN) model achieves 24.84% on the VQA-CP v2 training set compared to 13.85% for our SAN+Q-only+DoE model, demonstrating that our approach has effectively restricted the discriminative information in the question encoding.

**Proposed model shows complementary strengths with the base model:** To study whether our models learn complementary strengths to the base VQA models, we experiment with ensembles of both models. First, we consider oracle ensembles where the best model output for each data point is considered for evaluation. This is an upper bound on ensemble performance that relies on knowing ground truth. We find that the Oracle(Ours, SAN) ensemble outperforms two separately trained SAN models Oracle(SAN, SAN), by 1.48% for VQA v1 and by 3.46% for VQA v2—significantly lower gains than with Oracle(GVQA, SAN) which improves by 5.28%. It is notable however that the architecture of GVQA is significantly different from the base SAN model and hence is expected to exhibit different error patterns and a higher Oracle accuracy. To take a more attainable view, we also computed a standard ensemble Ensemble(Ours, SAN) and compared to an Ensemble(SAN, SAN) model,
outperforming it by 1.24% for VQA v2 but falling short by 0.15% for VQA v1. In contrast, Ensemble(GVQA, SAN) improves VQA v2 performance by only 0.54%.

5.3.5 Conclusion

We propose a novel adversarial regularization scheme for reducing the memorization of dataset biases in VQA based on a question-only adversary and the difference of model confidences after processing the image. Experiments on the VQA-CP dataset, show that this technique allows existing VQA models to significantly improve performance in the midst of changing priors. Consequently, we achieve state-of-the-art performance on VQA-CP. Our approach can be implemented as a simple, drop-in module on top of existing VQA models and easily trained end-to-end from scratch.
CHAPTER VI

CONCLUSION

In this dissertation, I introduce and study a multi-modal Artificial Intelligence (AI) task called Visual Question Answering (VQA) – given an image and a natural language question about the image (e.g., ‘What kind of store is this?’, ‘Is it safe to cross the street?’), the machine’s task is to automatically produce an accurate natural language answer (‘bakery’, ‘yes’). Specifically, my colleagues and I introduced the task of free-form and open-ended Visual Question Answering (VQA). We collected a large scale dataset (>0.25M images, >0.76M questions, ∼10M answers) and made it publicly available (www.visualqa.org). This dataset, together with the development of baseline models and organization of annual challenges and workshops by us, led to remarkable improvements in the state-of-art on VQA. As part of my dissertation, I also developed novel techniques to characterize the behavior of VQA models. And finally, I addressed the issue of VQA models being driven by superficial correlations in training data and lacking sufficient image grounding by – 1) proposing a new evaluation protocol to evaluate the degree of visual groundedness in VQA models, 2) proposing a novel Grounded VQA (GVQA) model that contains inductive biases and restrictions in the architecture specifically designed to prevent the model from ‘cheating’ by primarily relying on priors in the training data, 3) proposing a novel adversarial regularization scheme that can be added to any existing VQA model’s objective function, without significantly changing the underlying VQA model’s architecture.

Future Work Directions: VQA and Beyond

VQA. Despite tremendous progress in VQA, there are some specific types of questions in VQA where the community has not made enough progress (mentioned below).
Some of these are highlighted below:

- **Counting:** The performance of state-of-art VQA models on counting questions (e.g., ‘How many people are standing in the queue?’; ‘How many slices of pizza are there?’) is only \( \sim 45\% \) (compared to the human performance of \( \sim 83\% \) and overall (across all questions) performance of state-of-art models of \( \sim 71\% \)). Clearly, the act of counting itself is not challenging – what is challenging is to parse the language, identify the referring expressions, grounding the referring expressions into visual concepts (e.g., detecting each individual slice of pizza, detecting each person who is standing and in the queue) – all of these are studied today as separate tasks in the computer vision and NLP community. I think studying unified VQA models that include these components as modules could be a step towards improving counting performance of VQA models.

- **Optical Character Recognition (OCR):** Another class of questions where the community has not made enough progress is all questions that require reading text photographed in images (e.g., ‘What does the street sign say?’, ‘What is the name of the building?’). Answering such questions requires the ability to do Optical Character Recognition (OCR), which I believe current VQA models lack because they do not get enough training signal from the downstream VQA loss to be able to learn OCR. Also, most of the existing VQA models predict answers by doing classification over a fixed set of \( K \) (typically 1000 - 3000) answers. Hence these models will not be able to correctly answer such OCR type of questions if the correct word / phrase does not lie in the list of those \( K \) answers. I believe building VQA models that use existing OCR techniques as modules and that have the ability to predict answers not seen during training could be a good first step towards making progress in this direction. Recently, with the release of the TextVQA dataset [412] and the organization of the TextVQA challenge (https://textvqa.org/challenge), the community
has already started making progress in this direction, but there is still a lot of room for improvement.

- **Knowledge Based Reasoning:** We have not made much progress on questions that require knowledge based reasoning and common sense (e.g., ‘Does this person have 20/20 vision?’; ‘Is this food healthy?’). Such questions require an agent to understand what ‘20/20’ vision means and what types of food items are healthy, in addition to understanding the visual content – recognizing that the person is wearing spectacles and that it is a fast food item. I believe a limiting factor in this area is lack of existence of a large-scale and open-ended Knowledge Based (KB) VQA dataset. Creating a much larger and open-ended KB-VQA dataset has the potential to push the progress in this direction.

**Beyond: From Vision and Language to Actions.** Most of my past work has been towards building agents that can ‘see’ and ‘talk’. However, for a lot of practical applications (e.g., physical agents navigating inside our houses executing natural language commands) we need agents that can not only ‘see’ and ‘talk’ but can also take actions. Below are some directions towards generalizing vision and language agents to be able to take actions.

In this space of building agents that can ‘see’, ‘talk’ and ‘act’, one bold initiative which was well ahead of its time was the SHRDLU [477] project, studied by Terry Winograd in 1972 – an agent that operates on a table top scene consisting of several blocks such as cuboid, cone, containers etc.; there is a teacher which instructs the agent what to do (e.g., ‘pick up a red block’) and the agent either executes an action or asks a question (if the instruction is not clear) (e.g., ‘By “It”, I assume you mean the block which is taller than the one I am holding.’) (Fig. 29).

However, SHRDLU was a hand-engineered rule-based system. I think building a learning based SHRDLU agent can be a first step towards building agents that can ‘see’, ‘talk’ and ‘act’.
As a baby step in this direction, in a recent work [19], I worked on the following - how can we train agents to follow language instructions grounded in visual data (e.g., ‘Add a red sphere’, ‘Add a large cylinder’) and execute actions to generate scenes that are consistent with the given instruction (Fig. 30). Using reinforced adversarial learning framework [154], we have taken the first step towards training agents that can follow simple instructions (as mentioned above).

More generally, in the long term, I look forward to interactive agents that can, for instance, edit images based on natural language queries such as ‘Change the background to winter.’, AI assistants such as Alexa that can not only process language commands but can also situate itself in the its surrounding environment and can answer questions such as ‘Alexa, is my laptop in my bedroom?’, and finally agents that can move around our houses and execute natural language commands such as ‘Could you please get my laptop from upstairs?’.

Figure 29: The table-top setup and an example dialog from the SHRDLU [477] project (studied by Terry Winograd in 1972).
Figure 30: Given an instruction (‘There is a small sphere’), the task for an agent is to execute actions to create scenes that are consistent with the given instruction (i.e., each such scene consists of a small sphere).
APPENDIX A

APPENDIX FOR VISUAL QUESTION ANSWERING

In this appendix, we provide:

1. - Additional analysis comparing captions and Q&A data
2. - Qualitative visualizations for “What is” questions
3. - Human accuracy on multiple-choice questions
4. - Details on VQA baselines
5. - “Age” and “Commonsense” of our model
6. - Details on the abstract scene dataset
7. - User interfaces used to collect the dataset
8. - List of the top answers in the dataset
9. - Additional examples from the VQA dataset

A.1 Captions vs. Questions

Do questions and answers provide further information about the visual world beyond that captured by captions? One method for determining whether the information captured by questions & answers is different from the information captured by captions is to measure some of the differences in the word distributions from the two datasets. We cast this comparison in terms of nouns, verbs, and adjectives by extracting all words from the caption data (MS COCO captions for real images and captions collected by us for abstract scenes) using the Stanford part-of-speech (POS)\(^1\) tagger [437]. We normalize the word frequencies from captions, questions, and answers per image, and

\(^1\)Noun tags begin with NN, verb tags begin with VB, adjective tags begin with JJ, and prepositions are tagged as IN.
compare captions vs. questions and answers combined. Using a Kolmogorov-Smirnov test to determine whether the underlying distributions of the two datasets differ, we find a significant difference for all three parts of speech \( (p < .001) \) for both real images and abstract scenes. This helps motivate the VQA task as a way to learn information about visual scenes; although both captions and questions & answers provide information about the visual world, they do it from different perspectives, with different underlying biases [165], and can function as complementary to one another.

We illustrate the similarities and differences between the word distributions in captions vs. questions & answers as Venn-style word clouds [100] with size indicating the normalized count – Fig. 32 (nouns), Fig. 33 (verbs), and Fig. 34 (adjectives) for real images and Fig. 35 (nouns), Fig. 36 (verbs), and Fig. 37 (adjectives) for abstract scenes.\(^2\) The left side shows the top words in questions & answers, the right the top words in captions, and the center the words common to both, with size indicating the harmonic mean of the counts.

We see that adjectives in captions capture some clearly visual properties discussed in previous work on vision to language [311], such as material and pattern, while the questions & answers have more adjectives that capture what is usual (e.g., “dominant”, “approximate”, “higher”) and other kinds of commonsense properties (e.g., “edible”, “possible”, “unsafe”, “acceptable”). Interestingly, we see that question & answer nouns capture information about “ethnicity” and “hairstyle”, while caption nouns capture information about pluralized visible objects (e.g., “cellphones”, “daughters”) and groups (e.g., “trio”, “some”), among other differences. “Man” and “people” are common in both captions and questions & answers.

One key piece to understanding the visual world is understanding spatial relationships, and so we additionally extract spatial prepositions and plot their proportions in the captions vs. the questions & answers data in Fig. 31 (left) for real images and

\(^2\)Visualization created using http://worditout.com/.
Figure 31: Proportions of spatial prepositions in the captions and question & answers for real images (left) and abstract scenes (right).

Fig. 31 (right) for abstract scenes. We see that questions & answers have a higher proportion of specific spatial relations (*i.e.*, “in”, “on”) compared to captions, which have a higher proportion of general spatial relations (*i.e.*, “with”, “near”).
Figure 33: Venn-style word clouds [100] for verbs with size indicating the normalized count for real images.

Figure 34: Venn-style word clouds [100] for adjectives with size indicating the normalized count for real images.
Figure 35: Venn-style word clouds \([100]\) for nouns with size indicating the normalized count for abstract scenes.

Figure 36: Venn-style word clouds \([100]\) for verbs with size indicating the normalized count for abstract scenes.

Figure 37: Venn-style word clouds \([100]\) for adjectives with size indicating the normalized count for abstract scenes.
Figure 38: Distribution of questions starting with “What is” by their first five words for a random sample of 60K questions for real images (left) and all questions for abstract scenes (right). The ordering of the words starts towards the center and radiates outwards. The arc length is proportional to the number of questions containing the word. White areas are words with contributions too small to show.

A.2 “What is” Analysis

In Fig. 38, we show the distribution of questions starting with “What is” by their first five words for both real images and abstract scenes. Note the diversity of objects referenced in the questions, as well as, the relations between objects, such as “holding” and “sitting on”. In Fig. 39, we show the distribution of answers for “What is” questions ending in different words. For instance, questions ending in “eating” have answers such as “pizza”, “watermelon” and “hot dog”. Notice the diversity in answers for some questions, such as those that end with “for?” or “picture?”. Other questions result in intuitive responses, such as “holding?” and the response “umbrella”.

A.3 Multiple-Choice Human Accuracy

To compute human accuracy for multiple-choice questions, we collected three human answers per question on a random subset of 3,000 questions for both real images and abstract scenes. In Table A.3, we show the human accuracies for multiple choice
Figure 39: Distribution of answers for questions starting with “What is” for a random sample of 60K questions for real images (top) and all questions for abstract scenes (bottom). Each column corresponds to questions ending in different words, such as “doing?” “on?” etc.
Table 13: For each of the two datasets, real and abstract, first two rows are the human accuracies for multiple-choice questions when subjects were shown both the image and the question. Majority vote means we consider the answer picked by majority of the three subjects to be the predicted answer by humans and compute accuracy of that answer for each question. Average means we compute the accuracy of each of the answers picked by the subjects and record their average for each question. The last row is the inter-human agreement for open-ended answers task when subjects were shown both the image and the question. All accuracies are evaluated on a random subset of 3000 questions.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Accuracy Metric</th>
<th>All</th>
<th>Yes/No</th>
<th>Number</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real</td>
<td>MC majority vote</td>
<td>91.54</td>
<td>97.40</td>
<td>86.97</td>
<td>87.91</td>
</tr>
<tr>
<td></td>
<td>MC average</td>
<td>88.53</td>
<td>94.40</td>
<td>84.99</td>
<td>84.64</td>
</tr>
<tr>
<td></td>
<td>Open-Ended</td>
<td>80.62</td>
<td>94.78</td>
<td>78.46</td>
<td>69.69</td>
</tr>
<tr>
<td>Abstract</td>
<td>MC majority vote</td>
<td>93.57</td>
<td>97.78</td>
<td>96.71</td>
<td>88.73</td>
</tr>
<tr>
<td></td>
<td>MC average</td>
<td>90.40</td>
<td>94.59</td>
<td>94.36</td>
<td>85.32</td>
</tr>
<tr>
<td></td>
<td>Open-Ended</td>
<td>85.66</td>
<td>95.32</td>
<td>94.17</td>
<td>74.12</td>
</tr>
</tbody>
</table>

questions. Table A.3 also shows the inter-human agreement for open-ended answer task. In comparison to open-ended answer, the multiple-choice accuracies are more or less same for “yes/no” questions and significantly better (≈ 15% increase for real images and ≈ 11% increase for abstract scenes) for “other” questions. Since “other” questions may be ambiguous, the increase in accuracy using multiple choice is not surprising.

A.4 Details on VQA baselines

“per Q-type prior” baseline. We decide on different question types based on first few words of questions in the real images training set and ensure that each question type has at least 30 questions in the training dataset. The most popular answer for each question type is also computed on real images training set.

“nearest neighbor” baseline. For every question in the VQA test-standard set, we find its \(k\) nearest neighbor questions in the training set using cosine similarity in Skip-Thought [230] feature space. We also experimented with bag of words and
Word2Vec [303] feature spaces but we obtained the best performance with Skip-Thought. In this set of \( k \) questions and their associated images, we find the image which is most similar to the query image using cosine similarity in fc7 feature space. We use the fc7 features from the caffenet model in BVLC Caffe [207]. The most common ground truth answer of this most similar image and question pair is the predicted answer for the query image and question pair. We pick \( k = 4 \) on the test-dev set.

**A.5 “Age” and “Commonsense” of our model**

We estimate the age and degree of commonsense of our best model (deeper LSTM Q + norm I), selected using VQA test-dev accuracies). To estimate the age, we compute a weighted average of the average age per question, weighted by the accuracy of the model’s predicted answer for that question, on the subset of questions in the VQA validation set for which we have age annotations (how old a human needs to be to answer the question correctly). To estimate the degree of commonsense, we compute a weighted average of the average degree of commonsense per question, weighted by the accuracy of the model’s predicted answer for that question, on the subset of questions in the VQA validation set for which we have commonsense annotations (whether the question requires commonsense to answer it).

**A.6 Abstract Scenes Dataset**

In Fig. 40 (left), we show a subset of the objects that are present in the abstract scenes dataset. For more examples of the scenes generated, please see Fig. 45. The user interface used to create the scenes is shown in Fig. 40 (right). Subjects used a drag-and-drop interface to create the scenes. Each object could be flipped horizontally and scaled. The scale of the object determined the rendering order of the objects. Many objects have different attributes corresponding to different poses or types. Most animals have five different discrete poses. Humans have eight discrete expressions and
their poses may be continuously adjusted using a “paperdoll” model [29].

![Image of objects and AMT interface](image)

**Figure 40**: Left: A small subset of the objects present in the abstract scene dataset. Right: The AMT interface for collecting abstract scenes. The light green circles indicate where users can select to manipulate a person’s pose. Different objects may be added to the scene using the folders to the right.

### A.7 User Interfaces

In Fig. 41, we show the AMT interface that we used to collect questions for images. Note that we tell the workers that the robot already knows the answer to the previously asked question(s), inspiring them to ask different kinds of questions, thereby increasing the diversity of our dataset.

Fig. 42 shows the AMT interface used for collecting answers to the previously collected questions when subjects were shown the corresponding images. Fig. 43 shows the interface that was used to collect answers to questions when subjects were not shown the corresponding image (i.e., to help in gathering incorrect, but plausible, answers for the multiple-choice task and to assess how accurately the questions can be answered using common sense knowledge alone).
Stump a smart robot! Ask a question about this scene that a human can answer, but a smart robot probably can’t!

Updated instructions: Please read carefully.

We have built a smart robot. It understands a lot about scenes. It can recognize and name all the objects, it knows where the objects are, it can recognize the scene type (e.g., kitchen, beach), people’s expressions and poses, and properties of objects (e.g., the color of objects, their texture). Your task is to stump this smart robot! In particular, it already knows answers to some questions about this scene. We will tell you what these questions are.

Ask a question about this scene that this smart robot probably cannot answer, but any human can easily answer while looking at the scene in the image.

IMPORTANT: The question should be about this scene. That is, the human should need the image to be able to answer the question — the human should not be able to answer the question without looking at the image.

Your work will get rejected if you do not follow the instructions below:

• Do not ask questions that are similar to the ones listed below each image. As mentioned, the robot already knows the answers to those questions for the scene in this image. Please ask about something different.

• Do not repeat questions. Do not ask the same questions or the same questions with minor variations over and over again across images. Think of a new question each time specific to the scene in each image.

• Each question should be a single question. Do not ask questions that have multiple parts or multiple sub-questions in them.

• Do not ask generic questions that can be asked of many other scenes. Ask questions specific to the scene in each image.

Below is a list of questions the smart robot can already answer. Please ask a different question about this scene that a human can answer “if” looking at the scene in the image (and not otherwise), but would stump this smart robot:

Q1: What is unusual about this mustache? (The robot already knows the answer to this question.)
Q2: What is her facial expression? (The robot already knows the answer to this question.)
Q3: Write your question, different from the questions above, here to stump this smart robot.

Figure 41: Our AMT interface for collecting the third question for an image, when subjects were shown previous questions that were collected and were asked to ask a question different from previous questions.
Figure 42: The AMT interface used to collect answers to a question when subjects were shown the image while answering the question.

Figure 43: The AMT interface used to collect answers to a question when subjects were not shown the image while answering the question using only commonsense to collect the plausible, but incorrect, multiple-choice answers.
A.8 Answer Distribution

The top 250 answers in our real images dataset along with their counts and percentage counts are given below. The answers have been presented in different colors to show the different Part-of-Speech (POS) tagging of the answers with the following color code: yes/no, noun, verb, adjective, adverb, and numeral.

“yes” (566613, 22.82%), “no” (381307, 15.35%), “2” (80031, 3.22%), “1” (46537, 1.87%), “white” (41753, 1.68%), “3” (41334, 1.66%), “red” (33834, 1.36%), “blue” (28881, 1.16%), “4” (27174, 1.09%), “green” (22453, 0.9%), “black” (21852, 0.88%), “yellow” (17312, 0.7%), “brown” (14488, 0.58%), “5” (14373, 0.58%), “tennis” (10941, 0.44%), “baseball” (10299, 0.41%), “6” (10103, 0.41%), “orange” (9136, 0.37%), “0” (8812, 0.35%), “bathroom” (8473, 0.34%), “wood” (8219, 0.33%), “right” (8209, 0.33%), “left” (8058, 0.32%), “frisbee” (7671, 0.31%), “pink” (7519, 0.3%), “gray” (7385, 0.3%), “pizza” (6892, 0.28%), “7” (6005, 0.24%), “kitchen” (5926, 0.24%), “8” (5592, 0.23%), “cat” (5514, 0.22%), “skiing” (5189, 0.21%), “skateboarding” (5122, 0.21%), “dog” (5092, 0.21%), “snow” (4867, 0.2%), “black and white” (4852, 0.2%), “skateboard” (4697, 0.19%), “surfing” (4544, 0.18%), “water” (4513, 0.18%), “giraffe” (4027, 0.16%), “grass” (3979, 0.16%), “surfboard” (3934, 0.16%), “wii” (3898, 0.16%), “kite” (3852, 0.16%), “10” (3756, 0.15%), “purple” (3722, 0.15%), “elephant” (3646, 0.15%), “broccoli” (3604, 0.15%), “man” (3590, 0.14%), “winter” (3490, 0.14%), “stop” (3413, 0.14%), “train” (3226, 0.13%), “9” (3217, 0.13%), “apple” (3189, 0.13%), “silver” (3186, 0.13%), “horse” (3159, 0.13%), “banana” (3151, 0.13%), “umbrella” (3139, 0.13%), “eating” (3117, 0.13%), “sheep” (2927, 0.12%), “bear” (2803, 0.11%), “phone” (2772, 0.11%), “12” (2633, 0.11%), “motorcycle” (2608, 0.11%), “cake” (2602, 0.1%), “wine” (2574, 0.1%), “beach” (2536, 0.1%), “soccer” (2504, 0.1%), “sunny” (2475, 0.1%), “zebra” (2403, 0.1%), “tan” (2402, 0.1%), “brick” (2395, 0.1%), “female” (2372, 0.1%), “bananas” (2350, 0.09%), “table” (2331, 0.09%), “laptop” (2316, 0.09%), “hat” (2277, 0.09%), “bench” (2259,
“flowers” (2219, 0.09%), “woman” (2197, 0.09%), “male” (2170, 0.09%), “cow” (2084, 0.08%), “food” (2083, 0.08%), “living room” (2022, 0.08%), “bus” (2011, 0.08%), “snowboarding” (1990, 0.08%), “kites” (1979, 0.08%), “cell phone” (1943, 0.08%), “helmet” (1885, 0.08%), “maybe” (1853, 0.07%), “outside” (1846, 0.07%), “hot dog” (1809, 0.07%), “night” (1805, 0.07%), “trees” (1785, 0.07%), “11” (1753, 0.07%), “bird” (1739, 0.07%), “down” (1732, 0.07%), “bed” (1587, 0.06%), “camera” (1560, 0.06%), “tree” (1547, 0.06%), “christmas” (1544, 0.06%), “fence” (1543, 0.06%), “nothing” (1538, 0.06%), “unknown” (1532, 0.06%), “tennis racket” (1525, 0.06%), “red and white” (1518, 0.06%), “bedroom” (1500, 0.06%), “bat” (1494, 0.06%), “glasses” (1491, 0.06%), “tile” (1487, 0.06%), “metal” (1470, 0.06%), “blue and white” (1440, 0.06%), “fork” (1439, 0.06%), “plane” (1439, 0.06%), “airport” (1422, 0.06%), “cloudy” (1413, 0.06%), “15” (1407, 0.06%), “up” (1399, 0.06%), “blonde” (1398, 0.06%), “day” (1396, 0.06%), “teddy bear” (1386, 0.06%), “glass” (1379, 0.06%), “20” (1365, 0.05%), “beer” (1345, 0.05%), “car” (1331, 0.05%), “sitting” (1328, 0.05%), “boat” (1326, 0.05%), “standing” (1326, 0.05%), “clear” (1318, 0.05%), “13” (1318, 0.05%), “nike” (1293, 0.05%), “sand” (1282, 0.05%), “open” (1279, 0.05%), “cows” (1271, 0.05%), “bike” (1267, 0.05%), “chocolate” (1266, 0.05%), “donut” (1263, 0.05%), “airplane” (1247, 0.05%), “birthday” (1241, 0.05%), “carrots” (1239, 0.05%), “skis” (1220, 0.05%), “girl” (1220, 0.05%), “many” (1211, 0.05%), “zoo” (1204, 0.05%), “suitcase” (1199, 0.05%), “old” (1180, 0.05%), “chair” (1174, 0.05%), “beige” (1170, 0.05%), “ball” (1169, 0.05%), “ocean” (1168, 0.05%), “sandwich” (1168, 0.05%), “tie” (1166, 0.05%), “horses” (1163, 0.05%), “palm” (1163, 0.05%), “stripes” (1155, 0.05%), “fall” (1146, 0.05%), “cheese” (1142, 0.05%), “scissors” (1134, 0.05%), “round” (1125, 0.05%), “chinese” (1123, 0.05%), “knife” (1120, 0.05%), “14” (1110, 0.04%), “toilet” (1099, 0.04%), “don’t know” (1085, 0.04%), “snowboard” (1083, 0.04%), “truck” (1076, 0.04%), “boy” (1070, 0.04%), “coffee” (1070, 0.04%), “cold” (1064, 0.04%), “fruit” (1064, 0.04%), “walking” (1053, 0.04%)
A.9 Additional Examples

To provide insight into the dataset, we provide additional dataset examples (random selection) in Fig. 44, Fig. 45, and Fig. 46.
Figure 44: Random examples of questions (black), (a subset of the) answers given when looking at the image (green), and answers given when not looking at the image (blue) for numerous representative examples of the real image dataset.
Figure 45: Random examples of questions (black), (a subset of the) answers given when looking at the image (green), and answers given when not looking at the image (blue) for numerous representative examples of the abstract scene dataset.
Figure 46: Random examples of multiple-choice questions for numerous representative examples of the real and abstract scene dataset.
APPENDIX B

APPENDIX FOR ANALYZING THE BEHAVIOR OF VQA MODELS

In this appendix, we provide:

1. - Behavioral analysis for question-only and image-only VQA models.
2. - Scatter plot of average distance of test instances from nearest neighbor training instances w.r.t. VQA accuracy.
3. - Additional qualitative examples for “generalization to novel test instances”.
4. - The analyses on “complete question understanding” for different question types.
5. - Additional qualitative examples for “complete question understanding”.
6. - The analyses on “complete image understanding” for different question types.
7. - Additional qualitative examples for “complete image understanding”.

B.1 Behavioral analysis for question-only and image-only VQA models

We evaluated the performance of both CNN+LSTM and ATT models by just feeding in the question (and mean image embedding) and by just feeding in the image (and mean question embedding). We computed the percentage of responses that change on feeding the question as well, compared to only feeding in the image and the percentage of responses that change on feeding the image as well, compared to only feeding in the question. We found that the responses changed much more (about 40% more) on addition of the question than they did on addition of the image. So this suggests that the VQA models are heavily driven by question rather than the
B.2 Scatter plot of average distance of test instances from nearest neighbor training instances w.r.t. VQA accuracy

Figure 47: Test accuracy vs. average distance of the test points from k-NN training points for the CNN+LSTM model.

Fig. 47 shows the variation of accuracy of test point w.r.t their average distance from k-NN training points for the CNN+LSTM model. Each point in the plot represents average statistics (accuracy and average distance) for a random subset of 25 test points. We can see that for the test points with low accuracy, the average distance is higher compared to test points with high accuracy. The correlation between accuracy and average distance is significant (-0.41 at $k = 50$).\(^1\)

\(^1\) $k = 50$ leads to highest correlation
B.3 Additional qualitative examples for “generalization to novel test instances”

Fig. 48 shows test QI pairs for which the CNN+LSTM model produces the correct response and their nearest neighbor QI pairs from training set. It can be seen that the nearest neighbor QI pairs from the training set are similar to the test QI pair. In addition, the GT labels in the training set are similar to the test GT label.

Fig. 49 shows test QI pairs for which the CNN+LSTM model produces incorrect response and their nearest neighbor QI pairs from training set. Some of the mistakes are probably because the test QI pair does not have similar QI pairs in the training set (rows 2, 4 and 5) while other mistakes are probably because the GT labels in the training set are not similar to the GT test label (rows 1 and 3).

B.4 Analyses on “complete question understanding” for different question types

We show the breakdown of our analyses from chapter 4 – (i) whether the model ‘listens’ to the entire question; and (ii) which POS tags matter the most – over the three major categories of questions – “yes/no”, “number” and “other” as categorized in [27]. “yes/no” are questions whose answers are either “yes” or “no”, “number” are questions whose answers are numbers (e.g., “Q: How many zebras are there?”, “A: 2”), “other” are rest of the questions.

For “yes/no” questions, the ATT model seems particularly ‘jumpy’ – converging on a predicted answer listening to only the first few words of the question (see Fig. 50). Surprisingly, the accuracy is also as much as the final accuracy (after listening to entire question) when making predictions based on first few words of the question. In contrast, the CNN+LSTM model converges on a predicted answer later, after listening to atleast 35% of the question, achieving as much as the final accuracy after convergence. For “number” and “other” questions, both ATT and CNN+LSTM...
model show similar trends (see Fig. 51 for “number” and Fig. 52 for “other”).

It is interesting to note that VQA models are most sensitive to adjectives for “yes/no” questions (compared to wh-words for all questions) (see Fig. 53). This is probably because often the “yes/no” questions are about attributes of objects (e.g., “Is the cup empty?”). For “number” questions, the CNN+LSTM model is most sensitive to adjectives whereas the ATT model is most sensitive to wh-words (see Fig. 54). For “other” questions, both the models are most sensitive to “nouns” (see Fig. 55).

**B.5 Additional qualitative examples for “complete question understanding”**

Fig. 56 shows examples where the CNN+LSTM model converges on a predicted answer without listening to the entire question. On doing so, the model gets the answer correct for some QI pairs (first three rows) and incorrect for others (last two rows).

**B.6 Analyses on “complete image understanding” for different question types**

Fig. 57, Fig. 58 and Fig. 59 show the breakdown of percentage of questions for which the model produces same answer across images for “yes/no”, “number” and “other” respectively. The ATT model seems to be more “stubborn” (does not change its answers across images) for “yes/no” questions compared to the CNN+LSTM model, and less “stubborn” for “number” questions compared to the CNN+LSTM model.

**B.7 Additional qualitative examples for “complete image understanding”**

Fig. 60 shows examples where the CNN+LSTM model produces the same answer for at least half the images for a given question and the accuracy achieved by the model for such QI pairs.
**Figure 48:** Test QI pairs for which the CNN+LSTM model produces the correct response and their nearest neighbor QI pairs from training set.
<table>
<thead>
<tr>
<th>Test Sample</th>
<th>Nearest Neighbor Training Samples</th>
</tr>
</thead>
</table>
| Q: What kind of food is this?  | Predicted: A: dessert  
GT A: dessert  
Accuracy: 0.9 |
| Q: What is red and driving down the road? | Predicted: A: car  
GT A: yes  
Accuracy: 0.9 |
| Q: What breed of horse is this? | Predicted: A: mix and white  
GT A: chestnut  
Accuracy: 0.9 |
| Q: Is this Miley Cyrus? | Predicted: A: yes  
GT A: no  
Accuracy: 0.9 |
GT A: Florida  
Accuracy: 0.9 |

**Figure 49:** Test QI pairs for which the CNN+LSTM model produces incorrect response and their nearest neighbor QI pairs from training set.
**Figure 50:** X-axis shows length of partial “yes/no” question (in %) fed as input. Y-axis shows percentage of “yes/no” questions for which responses of these partial “yes/no” questions are the same as full “yes/no” questions and VQA accuracy of partial “yes/no” questions.

**Figure 51:** X-axis shows length of partial “number” question (in %) fed as input. Y-axis shows percentage of “number” questions for which responses of these partial “number” questions are the same as full “number” questions and VQA accuracy of partial “number” questions.
Figure 52: X-axis shows length of partial “other” question (in %) fed as input. Y-axis shows percentage of “other” questions for which responses of these partial “other” questions are the same as full “other” questions and VQA accuracy of partial “other” questions.

Figure 53: Percentage of “yes/no” questions for which responses remain same (compared to entire “yes/no” question) as a function of POS tags dropped from the “yes/no” question.
Figure 54: Percentage of “number” questions for which responses remain same (compared to entire “number” question) as a function of POS tags dropped from the “number” question.

Figure 55: Percentage of “other” questions for which responses remain same (compared to entire “other” question) as a function of POS tags dropped from the “other” question.
Figure 56: Examples where the CNN+LSTM model converges on a predicted answer without listening to the entire question.
Figure 57: Histogram of percentage of images for which model produces same answer for a given “yes/no” question. The cumulative plot shows the % of “yes/no” questions for which model produces same answer for \textit{at least} $x$ % of images.

Figure 58: Histogram of percentage of images for which model produces same answer for a given “number” question. The cumulative plot shows the % of “number” questions for which model produces same answer for \textit{at least} $x$ % of images.
Figure 59: Histogram of percentage of images for which model produces same answer for a given “other” question. The cumulative plot shows the % of “other” questions for which model produces same answer for \textit{at least} x % of images.
Figure 60: Examples where the CNN+LSTM model produces the same answer for at least half the images for each of the questions shown above. “Q” denotes the question for which model produces same response for at least half the images, “A” denotes the answer predicted by the model (which is same for at least half the images), “Number of Images” denotes the number of images for which the question is repeated in the VQA validation set and “Average Accuracy” is the VQA accuracy for these QI pairs (with same question but different images).
APPENDIX FOR OVERCOMING PRIORS IN VQA

C.1 Visual Question Answering under Changing Priors (VQA-CP)

In this appendix, we provide:

1. Additional analysis of VQA-CP splits
2. Details of benchmarking VQA models on VQA-CP

C.1.1 Additional analysis of VQA-CP splits

Fig. 61 shows the distribution of answers for several question types such as ‘what color’, ‘what sport’, ‘how many’, etc. for the train (left) and test (right) splits of the VQA-CP v2 dataset (the distribution of answers for VQA-CP v1 is presented in Section 5.1.2). We can see that the distributions of answers for a given question type is significantly different for train and test. For instance, ‘tennis’ is the most frequent answer for the question type ‘what sport’ in VQA-CP v2 train split whereas ‘baseball’ is the most frequent answer for the same question type in VQA-CP v2 test split. Similar differences can be seen for other question types as well – ‘does’, ‘which’.

C.1.2 Details of benchmarking VQA models on VQA-CP

Below we provide brief descriptions of all the existing VQA models used for benchmarking on VQA-CP splits:

**Deeper LSTM Question (d-LSTM Q) [27]**: Predicting the answer using question alone (“blind” model). It encodes the question using an LSTM and passes the encoding through a Multi-Layered Perceptron (MLP) to classify into answers.
Figure 61: Distribution of answers per question type vary significantly between VQA-CP v2 train (left) and test (right) splits. For instance, ‘white’ and ‘black’ are commonly seen answers in train for ‘What color’, where as ‘red’ is the most frequent answer in test. These have been computed for a random sample of 60K questions.

**Deeper LSTM Question + normalized Image (d-LSTM Q + norm I)** [27]:
The baseline VQA model. This model consists of a Multi-Layered Perceptron (MLP) fed in by normalized image embeddings (produced by VGG-Net [410]) and question embeddings (produced by a 2 layered LSTM). The MLP produces a distribution over top 1000 answers.

**Neural Module Networks (NMN)** [24]: The model designed to be compositional in nature. The model consists of composable modules where each module has a specific role (such as detecting a dog in the image, counting the number of dogs
in the image, etc.). Given an image and the natural language question about the image, NMN decomposes the question into its linguistic substructures using a parser to determine the structure of the network required to answer the question.

**Stacked Attention Networks (SAN)** [495]: One of the widely used models for VQA. Given an image and question, SAN uses the question to attend over the image, using a multi-hop architecture.¹

**Multimodal Compact Bilinear Pooling (MCB)** [150]: The winner of the VQA Challenge (on real images) 2016. MCB uses multimodal compact bilinear pooling to predict attention over image features and also to combine the attended image features with the question features.

**Question-type trends of model performance on VQA-CP**: Examining the accuracies of the above VQA models for different question types shows that the performance drop from VQA to VQA-CP is larger for some question types than the others. For VQA-CP v1, all the models show a significant drop (~70%) for ‘is there a’ questions (such as ‘Is there a flowering tree in the scene?’). For such questions in the VQA-CP v1 test split, the correct answer is ‘yes’ whereas the prior answer for questions starting with ‘Is there a’ in VQA-CP v1 train split is ‘no’. So, models tend to answer the VQA-CP v1 test questions with ‘no’ driven by the prior in the training data. Some other examples of question types in VQA-CP v1 resulting in significant drop in performance (more than 10%) for all the models are – ‘is this an’, ‘do you’, ‘are there’, ‘how many people are’, ‘what color is the’, ‘what sport is’, ‘what room is’, etc. Examples of question types in VQA-CP v2 resulting in more than 10% drop in performance for all the models are – ‘is it’, ‘is he’, ‘are there’, ‘how many people are in’, ‘what color is the’, ‘what animal is’, ‘what is in the’, etc.

¹We use a torch implementation of SAN, available at https://github.com/abhshkdz/neural-vqa-attention, for our experiments.
C.2 Grounded Visual Question Answering (GVQA)

In this appendix, we provide:

1. - Implementation details of GVQA
2. - Additional splits of VQA-CP v2
3. - Performance of model components on VQA-CP v2
4. - Performance of SAN with $Q_{main}$
5. - Performance of GVQA - VCC$_{loss}$ on VQA v1 and VQA v2
6. - Additional qualitative examples

C.2.1 Implementation details of GVQA

For the Question Classifier, we use a single layer LSTM with 512d hidden state and train it using the binary cross-entropy loss. For the Answer Cluster Predictor (ACP), we use a single layer LSTM with 256d hidden state and train it using the cross-entropy loss (cross-entropy over 50 classes, corresponding to 50 answer clusters). For the Visual Concept Classifier (VCC), we use a single layer LSTM with 512d hidden state to encode $Q_{main}$, the VGG-Net [410] to extract the activations of the last pooling layer (514 x 14 x 14) and the 2-hop attention architecture from SAN [495]. We use the binary cross-entropy loss to train each classifier in the VCC. For a given training instance, only a subset of all concept clusters are activated, and only these activated clusters contribute to the loss.

For the Question classifier, the ACP and the VCC, we use the rmsprop optimizer with a base learning rate of 3e-4. For the Answer Predictor (AP) and the Visual Verifier (VV), we use the Adam optimizer with a base learning rate of 3e-3 and 3e-4 respectively. All the implementation is using the torch deep learning framework [97].

Effect of number of clusters, clustering algorithm, POS tagger: As mentioned in Section 5.2.2, we used 50 clusters and K-means clustering algorithm for clustering the answer classes for the Answer Cluster Predictor (ACP). We tried 25
and 100 clusters as well and found that changing the number of clusters in K-means from 50 to 25 results in 1.05% drop, from 50 to 100 results in 0.76% drop in the overall VQA accuracy for the VQA-CP v2 dataset. We also tried Agglomerative clustering (instead of K-means) and found that it results in 0.42% drop in the overall VQA accuracy on the VQA-CP v2 dataset. Finally, we tried using Spacy POS tagger (instead of NLTK) for the Concept Extractor (CE) and found that it results in 0.02% improvement in the overall VQA accuracy on the VQA-CP v2 dataset.

### C.2.2 Additional splits of VQA-CP v2

<table>
<thead>
<tr>
<th>Model</th>
<th>Split1</th>
<th>Split2</th>
<th>Split3</th>
<th>Split4</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAN</td>
<td>24.96</td>
<td>26.07</td>
<td>22.69</td>
<td>24.19</td>
<td>24.48</td>
</tr>
<tr>
<td></td>
<td>31.30</td>
<td>32.40</td>
<td>33.78</td>
<td>28.99</td>
<td>31.62</td>
</tr>
<tr>
<td>GVQA</td>
<td>24.96</td>
<td>26.07</td>
<td>22.69</td>
<td>24.19</td>
<td>24.48</td>
</tr>
<tr>
<td></td>
<td>31.30</td>
<td>32.40</td>
<td>33.78</td>
<td>28.99</td>
<td>31.62</td>
</tr>
</tbody>
</table>

*Figure 62:* Performance of SAN and GVQA for different VQA-CP v2 splits. GVQA consistently outperforms SAN across all splits.

As mentioned in Section 5.2.3, to check if our particular VQA-CP split was causing some irregularities in performance, we created three additional sets of VQA-CP v2 splits with different random seeds. We evaluated both SAN and GVQA on all four splits (please see Fig. 62). We can see that GVQA consistently outperforms SAN across all four splits with average improvement being 7.14% (standard error: 1.36).

### C.2.3 Performance of model components on VQA-CP v2

*Question Classifier:* On the VQA-CP v2 test set, the LSTM based question classifier obtains 99.30% accuracy. *ACP:* The Top-1 test accuracy is 51.33%, with 80.12% for questions whose answers are in attribute clusters and 39.21% for questions whose answers are in object clusters. The Top-3 accuracy rises to 63.22%. Note that these accuracies are computed using the automatically created clusters. *VCC:* The weighted mean test F1 score across all classifiers is 0.53. The individual concepts are weighted as per the number of positive samples, reflecting the coverage of that concept in the test set.


C.2.4 Performance of SAN with $Q_{\text{main}}$

Table 14: Performance of SAN - $Q_{\text{full}} + Q_{\text{main}}$ compared to SAN and GVQA (our model) on VQA-CP v2 dataset. GVQA outperforms both SAN and SAN - $Q_{\text{full}} + Q_{\text{main}}$.

<table>
<thead>
<tr>
<th>Model</th>
<th>Overall</th>
<th>Yes/No</th>
<th>Number</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAN [495]</td>
<td>24.96</td>
<td>38.35</td>
<td>11.14</td>
<td>21.74</td>
</tr>
<tr>
<td>SAN - $Q_{\text{full}} + Q_{\text{main}}$</td>
<td>26.32</td>
<td>44.73</td>
<td>09.46</td>
<td>21.29</td>
</tr>
<tr>
<td>GVQA (Ours)</td>
<td>31.30</td>
<td>57.99</td>
<td>13.68</td>
<td>22.14</td>
</tr>
</tbody>
</table>

As mentioned in Section 5.2.4, as an additional check, we trained a version of SAN where the input is $Q_{\text{main}}$ instead of $Q_{\text{full}}$. Table C.2.4 shows the results of this version of SAN (SAN - $Q_{\text{full}} + Q_{\text{main}}$) along with those of SAN and GVQA on VQA-CP v2. We can see that this version of SAN performs 1.36\% (overall) better than the original SAN, however still 4.98\% (overall) worse than GVQA (with $Q_{\text{main}}$).

C.2.5 Performance of GVQA - VCC$_{\text{loss}}$ on VQA v1 and VQA v2

Table 15: Results of GVQA, GVQA - VCC$_{\text{loss}}$ and SAN on VQA v1 val split when trained on the VQA v1 train split. Please see text for more details.

<table>
<thead>
<tr>
<th>Model</th>
<th>VQA v1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Overall</td>
</tr>
<tr>
<td>SAN</td>
<td>55.86</td>
</tr>
<tr>
<td>GVQA - VCC$_{\text{loss}}$</td>
<td>48.51</td>
</tr>
<tr>
<td>GVQA</td>
<td>51.12</td>
</tr>
<tr>
<td>Ensemble (SAN, SAN)</td>
<td>56.56</td>
</tr>
<tr>
<td>Ensemble ((GVQA - VCC$_{\text{loss}}$, SAN)</td>
<td>56.44</td>
</tr>
<tr>
<td>Ensemble (GVQA, SAN)</td>
<td>56.91</td>
</tr>
<tr>
<td>Oracle (SAN, SAN)</td>
<td>60.85</td>
</tr>
<tr>
<td>Oracle ((GVQA - VCC$_{\text{loss}}$, SAN)</td>
<td>64.47</td>
</tr>
<tr>
<td>Oracle (GVQA, SAN)</td>
<td>63.77</td>
</tr>
</tbody>
</table>

Table C.2.5 and Table C.2.5 present the full results (i.e., broken down into Yes/No, Number and Other) of three models – GVQA, GVQA- VCC$_{\text{loss}}$ and SAN, along with their ensembles and Oracle performances. We can see that GVQA- VCC$_{\text{loss}}$ performs
Table 16: Results of GVQA, GVQA - VCC\textsubscript{loss} and SAN on VQA v2 val split when trained on the VQA v2 train split. Please see text for more details.

<table>
<thead>
<tr>
<th>Model</th>
<th>Overall</th>
<th>Yes/No</th>
<th>Number</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAN</td>
<td>52.02</td>
<td>68.89</td>
<td>34.55</td>
<td>43.80</td>
</tr>
<tr>
<td>GVQA - VCC\textsubscript{loss}</td>
<td>48.34</td>
<td>66.38</td>
<td>31.61</td>
<td>39.05</td>
</tr>
<tr>
<td>GVQA</td>
<td>48.24</td>
<td>72.03</td>
<td>31.17</td>
<td>34.65</td>
</tr>
<tr>
<td>Ensemble (SAN, SAN)</td>
<td>52.45</td>
<td>69.17</td>
<td>34.78</td>
<td>44.41</td>
</tr>
<tr>
<td>Ensemble ((GVQA - VCC\textsubscript{loss}), SAN)</td>
<td>51.79</td>
<td>68.59</td>
<td>34.44</td>
<td>43.61</td>
</tr>
<tr>
<td>Ensemble (GVQA, SAN)</td>
<td>52.96</td>
<td>72.72</td>
<td>34.19</td>
<td>42.90</td>
</tr>
<tr>
<td>Oracle (SAN, SAN)</td>
<td>56.68</td>
<td>74.37</td>
<td>40.08</td>
<td>47.61</td>
</tr>
<tr>
<td>Oracle ((GVQA - VCC\textsubscript{loss}), SAN)</td>
<td>61.93</td>
<td>85.13</td>
<td>43.51</td>
<td>49.16</td>
</tr>
<tr>
<td>Oracle (GVQA, SAN)</td>
<td>61.96</td>
<td>85.65</td>
<td>43.76</td>
<td>48.75</td>
</tr>
</tbody>
</table>

worse than GVQA on VQA v1 and similar to GVQA on VQA v2. So in addition to interpretability, GVQA is overall better than GVQA- VCC\textsubscript{loss} on these original VQA splits. Another observation about GVQA- VCC\textsubscript{loss} is that the Oracle ((GVQA- VCC\textsubscript{loss}), SAN)’s overall performance is 8.61% higher than that of SAN for VQA v1 (9.91% for VQA v2), suggesting that GVQA- VCC\textsubscript{loss} has strengths complementary to SAN (just like GVQA). Note that Oracle ((GVQA- VCC\textsubscript{loss}), SAN) is higher than Oracle (SAN, SAN) for both VQA v1 and VQA v2, suggesting that GVQA- VCC\textsubscript{loss}’s complementary strengths are more than that of another SAN model (with a different random initialization). Inspired by this, we report the performance of the ensemble of GVQA- VCC\textsubscript{loss} and SAN ((GVQA- VCC\textsubscript{loss}) + SAN) in Table C.2.5 and Table C.2.5, where the ensemble combines the outputs from the two models using product of confidences of each model. Unlike GVQA + SAN, (GVQA- VCC\textsubscript{loss}) + SAN does not outperform SAN + SAN (worse by 0.12% overall for VQA v1 and by 0.66% overall for VQA v2). Hence, GVQA is a better complement of SAN than GVQA- VCC\textsubscript{loss}, in addition to being more transparent.
C.2.6 Additional qualitative examples

Fig. 63 shows the VCC’s attention map for the example shown in Fig. 25 (right). Please refer to Fig. 25 for more details.

Fig. 64 and Fig. 65 show some qualitative examples from the VQA-CP v2 test set along with GVQA’s and SAN’s predicted answers. Also shown are the intermediate outputs from GVQA which provide insights into why GVQA is predicting what it is predicting and hence enable a system designer to identify the causes of error. This is not easy to do in existing VQA models such as SAN.
**Figure 64: Transparency of GVQA.** For each of the above examples, GVQA’s intermediate predictions can help explain why it predicted what it predicted. **Top-left:** VCC predicts the following visual concepts – blue, person, skiing and jacket. ACP predicts the cluster corresponding to colors. Finally, GVQA predicts ‘blue’ as the answer. So, we can see why GVQA predicts ‘blue’ – because, of all the visual concepts predicted by VCC, only ‘blue’ represents a color. Looking at the attention maps can further indicate why GVQA is “seeing” blue (because it is “looking” at the jacket as well, unlike SAN which is only “looking” at the pants). SAN’s prediction is ‘orange’ and unlike GVQA, SAN’s architecture does not facilitate producing such an explanation, which makes it difficult to understand why it is saying what it is saying. **Top-right:** Both GVQA and SAN are “looking” at the regions covered with snow, but GVQA correctly predicts ‘winter’, whereas SAN incorrectly predicts ‘summer’ which is unclear why. **Bottom-left:** The Concept Extractor (CE) predicts ‘happy’ whose visual presence is verified by VCC which is “looking” at the region corresponding to the kid’s face. **Bottom-right:** GVQA focuses on a larger part of the scene and correctly recognizes it as ‘bathroom’.
Figure 65: Transparency of GVQA. For the above examples, both GVQA and SAN incorrectly answer the question. However, GVQA’s intermediate predictions can help explain why it is incorrect. **Top-left:** For GVQA, VCC’s predictions indicate that it is perhaps “looking” at the field, which can be further verified by the attention map. SAN’s attention map suggests that it is “looking” at the ball but still does not explain why it is predicting ‘soccer’. Perhaps, it is confusing the ball with a soccer ball. **Top-right:** The attention maps from GVQA and SAN look similar to each other. However, looking at ACP’s and VCC’s prediction (for GVQA) suggest that it is indeed “seeing” ‘pasta’ (the correct answer), but still predicting ‘carrots’ because the ACP is incorrectly predicting the cluster corresponding to vegetables instead of the cluster corresponding to pasta. **Bottom:** GVQA is “looking” at the smartphone (unlike SAN), but yet incorrectly answers ‘no’, because the VCC does not recognize the phone as a smartphone. It however correctly predicts ‘phone’, ‘electronic’, ‘black’ and ‘right’.
REFERENCES


[2] “Personal communication,”


135


140
[100] COPPERSMITH, G. and KELLY, E., “Dynamic wordclouds and vennclouds for exploratory data analysis,” in ACL Workshop on Interactive Language Learning and Visualization, 2014. xiv, 94, 95, 96, 97


[145] Flickr, “Wayan Vota. Photo used under Creative Commons.”


152


[369] Ren, M., Kiros, R., and Zemel, R., “Exploring models and data for image question answering,” in *NIPS*, 2015. 9


