Assessing the Robustness of Visual Question Answering Models

Jia-Hong Huang, Modar Alfadly, Bernard Ghanem, Marcel Worring

Abstract Deep neural networks have been playing an essential role in the task of Visual Question Answering (VQA). Until recently, their accuracy has been the main focus of research. Now there is a trend toward assessing the robustness of these models against adversarial attacks by evaluating the accuracy of these models under increasing levels of noisiness in the inputs of VQA models. In VQA, the attack can target the image and/or the proposed query question, dubbed main question, and yet there is a lack of proper analysis of this aspect of VQA. In this work, we propose a new method that uses semantically related questions, dubbed basic questions, acting as noise to evaluate the robustness of VQA models. We hypothesize that as the similarity of a basic question to the main question decreases, the level of noise increases. To generate a reasonable noise level for a given main question, we rank a pool of basic questions based on their similarity with this main question. We cast this ranking problem as a LASSO optimization problem. We also propose a novel robustness measure $R$ score and two large-scale basic question datasets in order to standardize robustness analysis of VQA models. The experimental results demonstrate that the proposed evaluation method is able to effectively analyze the robustness of VQA models. To foster the VQA research, we will publish our proposed datasets.

1 Introduction

Visual Question Answering (VQA) is one of the most challenging computer vision tasks in which an algorithm is given a natural language question about an image and is tasked with producing a natural language answer for that question-image pair. Recently, various VQA models Antol et al (2015); Andreas et al (2016b); Malinowski et al (2015); Noh et al (2016a); Wu et al (2016); Lu et al (2016); Ben-younes et al (2017); Fukui et al (2016); Kim et al (2017); Malinowski and Fritz (2014b); Geman et al (2015); Agrawal et al (2018); Vedantam et al (2019); Chen et al (2020); Sheng et al (2021); Kolling et al (2022) have been proposed to tackle this problem, and their main performance measure is accuracy.

To find a robustness measure, we note the ultimate goal for VQA models is to perform as humans do for the same task. Now, if a human is presented with a ques-
tion or the same question which is accompanied by some highly similar questions, s/he tends to give the same or a very similar answer in both cases. Evidence of this has been reported in psychology Rips (1994). In our work, we call an input question the main question and define a basic question as a question semantically similar to the given main question. When we add or replace some words or phrases by semantically similar entities to the main question, the VQA model should output the same or a very similar answer. This is illustrated in Figure 1. We can consider these added entities as small perturbations or noise to the input. The model is robust if it produces the same answer. Because robustness analysis requires studying the accuracy of VQA models under different noise levels, we need to know how to quantify the level of noise for the given question. We hypothesize that a basic question with larger similarity score to the main question is considered to inject a smaller amount of noise if it is added to the main question and vice versa. Inspired by the above reasoning, we propose a novel method for measuring the robustness of VQA models. Figure 2 depicts the structure of our method. It contains two modules, a VQA model and a Noise Generator. The Noise Generator takes a plain text main question (MQ) and a plain text basic question dataset (BQD) as input. It starts by ranking the basic questions in BQD by their similarity to MQ using a text similarity ranking method. To measure the robustness of this VQA model, the accuracy with and without the generated noise for different noise levels is compared. We propose a robustness measure $R_{score}$ to quantify performance.

For the question ranking method, given a main question and a basic question, we can have different measures that quantify the similarity of those questions and produce a score. These different similarities lead to a different ranking. Commonly used text similarity metrics, such as BLEU (BiLingual Evaluation Understudy) Papineni et al (2002), are based on computing the overlapping of two texts. However, these metrics cannot capture the semantic meaning of text very well. So, question rankings based on the commonly used text similarity metrics are not accurate.

To improve the question ranking quality, we propose a new method formulated using LASSO optimization and compare it to other rankings produced by the commonly used textual similarity measures. Then, we do perform this comparison to rank our proposed BQDs, General Basic Question Dataset (GBQD) and Yes/No Basic Question Dataset (YNBQD). Furthermore, we evaluate the robustness of six pretrained state-of-the-art VQA models Antol et al (2015); Lu et al (2016); Ben-younes et al (2017); Kim et al (2017). Finally, we conduct extensive experiments to compare our proposed LASSO ranking method with the other metrics in BQD ranking.

Note that since the basic question (BQ) rankings based on those commonly used textual similarity measures are not effective, the noise level is not controllable based on those measures. However, our proposed LASSO basic question ranking method is effective. It is capable of quantifying and controlling the strength of the injected noise level. In this paper, our main contributions are summarized as follows:

- We introduce two large-scale basic questions datasets and make available two datasets for VQA robustness evaluation.
• We propose a novel method to measure the robustness of VQA models and test it on six different state-of-the-art VQA models.
• We propose a new LASSO-based text similarity ranking method and show that it outperforms seven popular similarity metrics.

The rest of our paper is organized as follows. In section 2, we review several related works. In section 3, we discuss the details of our proposed method and demonstrate how to use it for measuring the robustness of VQA models. Furthermore, in sections 4 and 5, we present the various analyses on our proposed General Basic Question Dataset (GBQD) and Yes/No Basic Question Dataset (YNBQD) Huang et al (2019). Finally, in section 6, we compare the performance of the state-of-the-art VQA models in terms of robustness and accuracy.

Relations to our previous work
This paper is an improved work based on our previous conference paper accepted by the Thirty-Third AAAI Conference on Artificial Intelligence (AAAI-2019) as an oral paper Huang et al (2019). Compared to this work, the improvements are summarized as follows. First, we propose a framework, referring to Figure 7, and a threshold-based criterion, referring to Algorithm 1, to exploit BQs to analyze the most robust HieCoAtt VQA model Lu et al (2016). Second, we show that the step of question sentences preprocessing is necessary for our proposed LASSO ranking method, and it guarantees that the proposed method works correctly. Third, we conduct an extended experiment on YNBQD. The current paper is a complete restructured and rewritten version.

2 Related Work
Over the past few years, VQA has emerged as an interesting and intelligent task which has drawn lots of attention from the research community with a variety of approaches Malinowski and Fritz (2014a); Andreas et al (2016b); Noh et al (2016b); Malinowski et al (2015); Zhang et al (2016); Kiros et al (2014); Zhu et al (2016); Andreas et al (2016a); Lu et al (2016); Li and Jia (2016); Xiong et al (2016); Malinowski et al (2017); Agrawal et al (2018); Vedantam et al (2019); Chen et al (2020); Sheng et al (2021); Kolling et al (2022). The above works involve different fields including natural language processing (NLP), computer vision, and machine learning. In the following subsections, we discuss numerous bodies of work including the sentence evaluation metrics, models’ accuracy and robustness, and datasets, related to our paper.

Sentence Evaluation Metrics
Sentence evaluation metrics have been widely used in several areas such as video/image captioning Yu et al (2016); Huang et al (2021e, 2022, 2021b,c,d) and text summarization Barzilay and Elhadad (1999). In this work, we exploit the commonly used metrics to measure the similarity between BQ and MQ. BLEU (BiLingual Evaluation Understudy) Papineni et al (2002) is one of the most popular metrics in machine translation based on precision. Yet, its effectiveness is questioned by some works such as Elliott and Keller (2013); Kulkarni et al (2011). METEOR Banerjee and Lavie (2005) is based on the harmonic mean of unigram precision and recall, and it can handle the stemming and synonym matching, which is designated to fix problems found with BLEU and produces a better correlation with translations by human experts. Regarding the difference between METEOR and BLEU, METEOR evaluates the correlation at the sentence and segment level whereas BLEU looks for correlations at the corpus level. ROUGE (Recall Oriented Understudy of Gisting Evaluation) Lin (2004) is another popular recall-based met-
ric in the text summarization community, and it tends to reward the longer sentences with the higher recall. CIDEr Vedantam et al (2015), a consensus-based metric, rewards a sentence for being similar to the majority of descriptions written by the human expert and this metric is mostly used in the image captioning community. It extends the existing metrics with $tf-idf$ weights of $n$-grams between candidate sentence and reference sentence. Sometimes, unnecessary parts of the sentence are also weighted and this leads to ineffective scores. So, CIDEr is an inefficient metric for natural language sentence evaluation in some sense. In our experiments, we take all of the metrics above and our proposed LASSO ranking approach to rank BQs and compare their BQ ranking performance.

**Evaluating Image Captioning**

Some commonly used techniques, such as encoding and decoding, in the image captioning task Xu et al (2015); Karpathy and Fei-Fei (2015); Vinyals et al (2015); Fang et al (2015) are also used in the VQA task. In Fang et al (2015), the authors try to use a language model to combine a set of possible words detected in several regions of the input image, and then generate some description for the image. The authors of Vinyals et al (2015) exploit a convolutional neural networks model to extract the high-level image features, and then give an LSTM unit these features as the first input. In Xu et al (2015), the authors propose an algorithm to generate a word at each time step by paying attention to local image regions related to the predicted word at the current time step. In Karpathy and Fei-Fei (2015), the authors propose a deep neural networks model to learn how to embed the language and visual information into a common multimodal space. To the best of our knowledge, the existing image captioning algorithms only can generate rough and short descriptions for a given image, and those descriptions tend to be grammatically similar to the ones in the training set. Also, although BLEU is commonly used to evaluate the result of the image captioning task, it isn’t the most proper metric to evaluate the quality of the image captioning result because of its innate property.

**Evaluating Visual Question Answering**

In VQA, we have two types of inputs with different modalities including the question sentence and image, so VQA is a multimodal task. In Kiros et al (2014); Ben-younes et al (2017); Fukui et al (2016); Kim et al (2017); Lin et al (2015), the authors have tried to focus on modeling the interactions between two different embedding spaces. The authors of Kiros et al (2014); Lin et al (2015) have shown that the bilinear interaction between two embedding spaces is very successful in deep learning for fine-grained classification and multimodal language modeling. In Fukui et al (2016), the authors propose a method, Multimodal Compact Bilinear (MCB) pooling, to compute an outer product between visual and textual features. The authors of Kim et al (2017) propose a tensor-based method, Multimodal Low-rank Bilinear (MLB) pooling, to parameterize the full bilinear interactions between image and question sentence embedding spaces. In Ben-younes et al (2017), the authors propose another method to efficiently parameterize the bilinear interactions between textual and visual representations, and they also show that MCB and MLB are special cases of their proposed method. In Ren et al (2015a), the authors exploit Recurrent Neural Networks (RNN) and Convolutional Neural Networks (CNN) to build a question generation algorithm, but it sometimes generates questions with invalid grammar. The authors of Malinowski et al (2015); Gao et al (2015); Malinowski et al (2017) exploit RNN to combine the word and image features for the VQA task. In Ma et al (2016), the authors have tried to exploit convolutions to group the neighboring features of word and image. Gated Recurrent Unit (GRU) Chung et al (2014) is another variant of RNN, and the authors of Noh et al (2016b) use it to encode an input question. Additionally, they introduce a dynamic parameter layer in their CNN model, and the weights of the model are adaptively predicted by the embedded question features. The above VQA methods are all based on accuracy-based datasets. To the best of our knowledge, there is no existing VQA method evaluated by a robustness-based dataset since that kind of dataset does not exist.

**Robustness of Neural Network Models**

Recently, the authors of Fawzi et al (2017); Carlini and Wagner (2017); Xu et al (2009); Kafle and Kanan (2017b,a); Huang et al (2019, 2017, 2018); Huang (2017); Hu et al (2019); Huck Yang et al (2018); Liu et al (2018); Yang et al (2018); Di Sipio et al (2022) have tried to discuss the robustness issue of deep learning models from the image, Fawzi et al (2017); Carlini and Wagner (2017) or text Huang et al (2019) point of view. In Fawzi et al (2017); Carlini and Wagner (2017), the authors analyze the robustness of learning models by adding some noise or perturbations into images and observe how the predicted result will be affected. The authors of Moosavi-Dezfooli et al (2018) provide theoretical evidence on the existence of a strong relation between small curvature and large robustness. Moreover, they propose an efficient regularizer that encourages small curvatures and also show that the regularizer leads to a significant boost in robustness of neural networks. To the best of our knowledge, most of the existing works play with adding noise to the image input. In this work, we play with noise added to the text input. We consider the BQs of a given MQ is a kind of noise of the given MQ. Then, we exploit the BQs to do the robustness analysis of VQA models.

**Datasets for Visual Question Answering**

Recently, many accuracy-based VQA datasets have been proposed. To the best of our knowledge, DAQUAR (DATaset for Ques tion Answering on Real-world images) dataset Malinowski and Fritz (2014a) is the first
proposed dataset, which contains about 12.5 thousand manually annotated question-answer pairs on about 1449 indoor scenes Silberman et al (2012). A question in the original DAQUAR dataset only has a single ground truth answer. The authors of Malinowski et al (2017) collect additional answers for each question to extend the DAQUAR. After the introduction of DAQUAR, three other VQA datasets based on MS-COCO Lin et al (2014) have been proposed, namely Ren et al (2015b); Antol et al (2015); Gao et al (2015). The authors of Ren et al (2015b) have transformed existing annotations for the image caption generation task into question-answer pairs based on a syntactic parser Klein and Manning (2003) and a set of hand-designed rules. In Antol et al (2015), the authors have proposed another popular dataset, called VQA. It contains around 614000 questions concerning the visual content of 205000 real-world images. Also, it has 150000 questions based on 50000 abstract scenes. Additionally, the authors of the VQA dataset provide 10 answers for each image. The VQA test set answers are not released because of the VQA challenge workshop. Finally, the authors of Gao et al (2015) have annotated about 158000 images with 316000 Chinese question-answer pairs with the corresponding English translations. In Yu et al (2015), the authors try to simplify the evaluation of the performance of VQA models by introducing Visual Madlibs, a multiple choice question answering (QA) by filling the blanks task. In the task, a VQA model has to choose one out of four provided answers based on a given image and the prompt. Formulating VQA task in this way wipes out ambiguities in answer candidates. A simple accuracy metric is used to measure the performance of different VQA models. However, VQA models require holistic reasoning based on the given images in this task. It remains challenging for machines, despite the simple evaluation. In Malinowski and Fritz (2014a,b, 2015), the automatic and simple performance evaluation metrics have been a part of building the VQA dataset. The authors of the Visual7W dataset Zhu et al (2016) have built question-answer pairs based on the Visual Genome dataset Krishna et al (2017), and it contains around 330000 natural language questions. In contrast to the other datasets such as VQA or DAQUAR, the Visual Genome dataset focuses on the so-called six Ws, namely what, where, when, who, why, and how, which can be answered with a text-based sentence. Additionally, Visual7W extends question and answer pairs with extra groundings of the correspondences, and it not only includes natural language answers but also answers requiring locating the object. Then, the Visual7W contains multiple-choice answers similar to Visual Madlibs Yu et al (2015). In Nag Chowdhury et al (2016), the authors have proposed Xplore-M-Ego, which is a dataset of images with natural language queries, a media retrieval system, and collective memories. Their work focuses on a user-centric, dynamic scenario, where the given answers are conditioned not only on questions, but also on the geographical position of the questioner. There is another task, called video question answering, which is related to VQA. It needs to understand long term relations in the video. In Zhu et al (2015), the authors have proposed a task which needs to fill in blanks in captions associated with videos. The task requires inferring the past, describing the present and predicting the future in a diverse set of video descriptions data ranging from movies Zhu et al (2015); Rohrbach et al (2015); Tapaswi et al (2016) and cooking videos Regneri et al (2013) to web videos Ji et al (2019). However, the above datasets are accuracy-based and they cannot be used in the evaluation of the robustness of VQA models. In this work, we propose GBQD and YNBQD robustness-based datasets.

3 Methodology

In this section, we introduce our proposed method. We start with a discussion on how to embed questions and use different metrics to generate BQs. Then, we discuss how to analyze the robustness of six pretrained state-of-the-art VQA models by BQ. The overall method is illustrated in Figure 2. It consists of two main components, dubbed the VQA module and Noise Generator respectively. The VQA module contains the model we want to do robustness analysis on, while the Noise Generator utilizes eight ranking methods, namely BLEU-1, BLEU-2, BLEU-3, BLEU-4, ROUGE, CIDEr, METEOR, and our proposed LASSO ranking method, to generate noise for a given main question. According to our hypothesis mentioned in the Introduction, a set of effectively ranked BQs based on some ranking method should have a decreasing accuracy. Let us first introduce some basic notations for our method.

Question Encoding

The first step in our method is the embedding of the question sentences. Let \( w_1, \ldots, w_N \) be the words in question \( q \), with \( w_i \) denoting the \( t \)-th word for \( q \) and \( x_i \) denoting the \( t \)-th word embedding for \( q \). Word2Vec Mikolov et al (2013), GloVe Pennington et al (2014) and Skip-thoughts Kiros et al (2015) are popular text encoders Huang and Worring (2020); Huang et al (2021a). Since we define a BQ as a question semantically similar to the given MQ, we need an encoder that can better capture the semantic meaning of a sentence. Among these encoders, Skip-thoughts focuses on the semantic meaning of the whole sentence, capturing relations between words. So, we use Skip-thoughts to embed the questions in this paper. The Skip-thoughts model exploits an RNN encoder with GRU Chung et al (2014) activations, which maps an English sentence, \( i.e., q_i \), into a feature vector \( v \in \mathbb{R}^{4800} \). We encode all the training and validation questions of the VQA dataset Antol et al (2015) into the columns of \( A \), a matrix of Skip-
thoughts embedded basic question candidates. We use \( b \) to denote a Skip-thoughts encoded main question.

The question encoder at each time step generates a hidden state \( h^t \). It can be considered as the representation of the sequence \( \{ w^1, ..., w^t \} \). So, the hidden state \( h^N \) represents the whole sequence \( \{ w^1, ..., w^1, ..., w^N \} \), i.e., a question sentence in our case. For convenience, here we drop the index \( i \) and iterate the following sequential equations to encode a question:

\[
\begin{align*}
    r^t &= \sigma(U_r h^{t-1} + W_r x^t) \\
    z^t &= \sigma(U_z h^{t-1} + W_z x^t) \\
    \tilde{h}^t &= \tanh(U(r^t \odot h^{t-1}) + W x^t) \\
    h^t &= z^t \odot \tilde{h}^t + (1 - z^t) \odot h^{t-1},
\end{align*}
\]

where \( U_r, U_z, W_r, W_z, U \) and \( W \) are the matrices of weight parameters. \( h^t \) is the state update at time step \( t \), \( r^t \) is the reset gate, \( \odot \) denotes an element-wise product, \( z^t \) is the update gate, and \( h^1 = 0 \) as \( t = 0 \). These two gates take values between zero and one. Finally, \( \sigma \) denotes the activation function.

**Level-controllable Noise Generator**

Based on the assumption mentioned in our Introduction, level-controllable noise, i.e., BQ, generation will involve similarity-based ranking. As we have mentioned in the Introduction, the existing textual similarity measures, such as BLEU, CIDEr, METEOR, and ROUGE, cannot effectively capture the semantic similarity. In this work, we propose a new optimization-based ranking method to address this issue. The problem of generating BQs that are similar to an MQ can be cast as a LASSO optimization problem. By embedding all the main questions and the basic question candidates using Skip-thoughts, LASSO modelling helps us to determine a sparse number of basic questions suited to represent the given main question. The LASSO model is expressed by the following optimization:

\[
\min_x \frac{1}{2} ||Ax - b||^2_2 + \lambda ||x||_1,
\]

where \( \lambda \) is a tradeoff parameter which controls the quality of BQs.

To develop our basic question dataset (BQD), we combine the unique questions in the training and validation datasets of the most popular VQA dataset Antol et al. (2015) and we use the testing dataset as our main question candidates. Also, we need to do “question sentences preprocessing”, in particular, making sure that none of the main questions is contained in our basic question dataset, as otherwise, LASSO modelling cannot give a useful ranking. Otherwise and because we are encouraging sparsity, the ranking will neglect all other questions and give them a similarity score of zero.

**BQ Generation by LASSO-based Ranking Method**

In this subsection, we describe how to use the LASSO-based ranking method to generate the basic questions of a given main question (refer to Figure 2). Now, we are ready to deal with our LASSO optimization problem to get the sparse solution \( x \). One can consider the elements of \( x \) to be the similarity score between the main question \( b \) and the corresponding BQ in \( A \). The first embedded BQ candidate is the first column of \( A \) and the corresponding similarity score is the first element of \( x \) and so on. Furthermore, we collect the top-k BQs of each given MQ based on the ranking of scores in \( x \). Intuitively, if a BQ has a higher similarity score to a given query question, it implies that this BQ is more similar to the given MQ and vice versa. Additionally, because most of the VQA models have the highest accuracy performance in answering yes/no questions, we argue that yes/no questions are the simplest questions for VQA models in the sense of accuracy. Hence, we also create a Yes/No Basic Question dataset based on the aforementioned basic question generation approach.

**Details of the Proposed Basic Question Dataset**

The size of the basic questions dataset has a great impact on the noise generation method. Intuitively, the more questions you have, the more chance it has to contain similar questions to any given main question. In our work, based on the LASSO-based ranking method, we propose two large-scale basic question datasets, General Basic Question Dataset and Yes/No Basic Question Dataset. Note that, in our dataset collections, we set \( k = 21 \) because after top-21 the similarity scores of BQs are negligible. As such, we get the ranked BQs of 244,302 testing question candidates. The proposed General and Yes/No BQ datasets, with the format \{Image, MQ, 21 (BQ + corresponding similarity score)\}, contain 81,434 images from the testing images of MS COCO dataset Lin et al. (2014) and 244,302 main questions from the testing questions of VQA dataset (open-ended task) Antol et al. (2015). Furthermore, our General and Yes/No basic questions are extracted from the validation and training questions of VQA dataset (open-ended task) and the corresponding similarity scores of General and Yes/No BQ are generated by our LASSO ranking approach. That is to say, in our GBQD and YNBQD, there are 5,130,342 (General BQ + corresponding similarity score) tuples and 5,130,342 (Yes/No BQ + corresponding similarity score) tuples.

**Robustness Analysis by General and Yes/No Basic Questions**

To measure the robustness of any VQA model, we measure how its accuracy changes when its input is cor-
ruptured with noise. The noise can be completely random, structured and/or semantically related to the final task. Since the input in VQA is an MQ-image pair, the noise can be injected into both. The noise to the question should have some contextual semantics for the measure to be informative, instead of introducing misspellings or changing or dropping random words. Here we propose a novel robustness measure for VQA by introducing semantically relevant noise to the questions where we are able to control the level of noise.

The authors of VQA dataset Antol et al (2015) provide the open-ended and multiple-choice tasks for evaluation. For the multiple-choice task, an answer should be selected from 18 answer candidates. However, the answer of the open-ended task can be any phrase or word. For both tasks, the answers are evaluated by accuracy, which is considered to reflect human consensus. We measure accuracy as defined in Antol et al (2015) accuracy, which is considered to reflect human consensus.

We encode all the training and validation questions using the Skip-thought Vector Kiros et al (2015). Regarding our LASSO modeling and because the quality of BQ is mainly affected by the parameter λ, we choose λ = 10−6, for the better quality, to generate our GBQD and YNBQD. 

4 Experiments

In this section, we explain our implementation details and the experiments we conducted to validate and analyze our proposed method.

Dataset.

We conduct the experiments on GBQD, YNBQD and VQA dataset Antol et al (2015). The VQA dataset is based on the MS COCO dataset Lin et al (2014), and it includes 248,349 training, 121,512 validation and 244,302 testing questions. Each question in VQA dataset is associated with 10 answers annotated by different people from AMT (Amazon Mechanical Turk). About 90% of answers only have a single word and 98% of answers have no more than three words. Regarding our General and Yes/No Basic Questions Datasets, because the similarity scores are negligible after top 21 ranked BQs, we only collect the top 21 ranked General and Yes/No BQs and put them into our GBQD and YNBQD. Because most of the pretrained state-of-the-art VQA models are trained under the condition that the maximum number...
| BQ ID | Similarity Score | BQ                                      |
|-------|------------------|-----------------------------------------|
| 01    | 0.295            | How old is the truck?                   |
| 02    | 0.240            | How old is this car?                    |
| 03    | 0.142            | How old is the vehicle?                 |
| 04    | 0.120            | What number is the car?                 |
| 05    | 0.093            | What color is the car?                  |
| 06    | 0.063            | How old is the bedroom?                 |
| 07    | 0.063            | What year is the car?                   |
| 08    | 0.037            | Where is the old car?                   |
| 09    | 0.033            | How old is the seat?                    |
| 10    | 0.032            | How old is the car?                     |
| 11    | 0.028            | What make is the blue car?              |
| 12    | 0.028            | How old is the golden retriever?        |
| 13    | 0.024            | What is beneath the car?                |
| 14    | 0.022            | Is the car behind him a police car?     |
| 15    | 0.020            | How old is the pilot?                   |
| 16    | 0.017            | How old are you?                        |
| 17    | 0.016            | How old is the laptop?                  |
| 18    | 0.016            | How old is the television?              |
| 19    | 0.015            | What make is the main car?              |
| 20    | 0.015            | What type and model is the car?         |
| 21    | 0.015            | What is lifting the car?                |

(a) “MQ: How old is the car?” and image “(a)” in Figure 4.

| BQ ID | Similarity Score | BQ                                      |
|-------|------------------|-----------------------------------------|
| 01    | 0.281            | Where is the cat sitting on?            |
| 02    | 0.108            | What is this cat sitting on?            |
| 03    | 0.055            | What is cat sitting on?                 |
| 04    | 0.053            | What is the cat on the left sitting on? |
| 05    | 0.050            | What is the giraffe sitting on?         |
| 06    | 0.047            | What is the cat sitting in the car?     |
| 07    | 0.046            | That is the black cat sitting on?       |
| 08    | 0.042            | What is the front cat sitting on?       |
| 09    | 0.041            | What is the cat perched on?             |
| 10    | 0.041            | What’s the cat sitting on?              |
| 11    | 0.037            | What is the cat leaning on?             |
| 12    | 0.035            | What object is the cat sitting on?      |
| 13    | 0.029            | What is the doll sitting on?            |
| 14    | 0.023            | How is the cat standing?                |
| 15    | 0.022            | What is the cat setting on?             |
| 16    | 0.022            | What is the cat walking on?             |
| 17    | 0.021            | What is the iPhone sitting on?          |
| 18    | 0.021            | What is the cat napping on?             |
| 19    | 0.020            | What is the dog sitting at?             |
| 20    | 0.018            | What is the birds sitting on?           |
| 21    | 0.018            | What is the sitting on?                 |

(b) “MQ: What is the cat sitting on?” and image “(b)” in Figure 4.

Table 1: “MQ: How old is the car?” and image “(a)” corresponds to Figure 4-(a). “MQ: What is the cat sitting on?” and image “(b)” corresponds to Figure 4-(b).

of input words is 26, we divide the 21 top ranked BQs, i.e., $21 = 3 \times 7$, into 7 consecutive partitions to do the robustness analysis, referring to Table 2 for GBQD and Table 3 for YNBQD. Note that, under the above setting, the total number of words for each MQ with 3 BQs is equal to or less than 26 words.

**BQ Generation by Popular Text Evaluation Metrics.**

In this subsection, we discuss the non-\textit{LASSO}-based ranking methods to generate the basic questions of a given main question. We compare the performance of \textit{LASSO}-based ranking method with non-\textit{LASSO}-based ranking methods including seven popular sentence evaluation metrics Papineni et al (2002); Vedantam et al (2015); Lin (2004); Banerjee and Lavie (2005), namely BLEU-1, BLEU-2, BLEU-3, BLEU-4, ROUGE, CIDEr and METEOR that are also used to measure the similarity score between MQ and BQs. Similar to the setup for building the General Basic Question Dataset
Table 2: The table shows the six state-of-the-art pretrained VQA models evaluation results on the GBQD and VQA dataset. “−” indicates the results are not available, “−std” represents the accuracy of VQA model evaluated on the complete testing set of GBQD and VQA dataset and “dev” indicates the accuracy of VQA model evaluated on the partial testing set of GBQD and VQA dataset. In addition, $diff = Original_{dev} - X_{dev}$, where $X$ is equal to the “First”, “Second”, etc.

Table 3: The table shows the six state-of-the-art pretrained VQA models evaluation results on the YNBDQ and VQA dataset. “−” indicates the results are not available, “−std” represents the accuracy of VQA model evaluated on the complete testing set of YNBDQ and VQA dataset and “dev” indicates the accuracy of VQA model evaluated on the partial testing set of YNBDQ and VQA dataset. In addition, $diff = Original_{dev} - X_{dev}$, where $X$ is equal to the “First”, “Second”, etc.
Table 4: This table shows the robustness scores, $R_{\text{score}}$, of six state-of-the-art VQA models based on GBQD ($R_{\text{score1}}$), YNBQD ($R_{\text{score2}}$) and VQA Antol et al (2015) dataset. LQI denotes LSTM Q+I, HAV denotes HieCoAtt (Alt,VGG19), HAR denotes HieCoAtt (Alt,Resnet200), MU denotes MUTAN without Attention, MUA denotes MUTAN with Attention and MLB denotes MLB with Attention. The $R_{\text{score}}$ parameters are $(t, m) = (0.05, 20)$.

| Model | LQI | HAV | HAR | MU | MUA | MLB |
|-------|-----|-----|-----|----|-----|-----|
| $R_{\text{score1}}$ | 0.19 | 0.48 | 0.45 | 0.30 | 0.34 | 0.36 |
| $R_{\text{score2}}$ | 0.08 | 0.48 | 0.53 | 0.30 | 0.23 | 0.37 |

(i) Are the rankings of BQs effective? We take the top 21 ranked BQs and divide them into 7 consecutive partitions and each partition contains 3 top ranked BQs. Figure 5-(a)-1 shows that the accuracy decreases from the first partition to the seventh partition. Also, according to Figure 5-(a)-2, the accuracy decrement increases from the first partition to the seventh. The above two trends imply the similarity of BQs to the given MQ decreases from the first partition to the seventh (i.e., the noise level increases). Specifically, the level of noise increases from the first partition to the seventh because our assumption is that a BQ with smaller similarity score to the given MQ indicates that this BQ introduces more noise to the given MQ and vice versa. Note that when we replace the GBQD by YNBQD and do the same experiment (refer to Figure 5-(b)-1 and Figure 5-(b)-2), the trends are similar to those in GBQD. Based on Figure 5, we conclude that the rankings by LASSO ranking method are effective. However, based on Figure 6, we discover that the accuracy of these 7 similarity metrics, $\{\text{BLEU1...4, ROUGE, CIDEr, METEOR}\}$, are less monotonous and much more random from the first partition to the seventh partition. In other words, the level of noise is changing randomly from the first partition to the seventh partition. In fact, the accuracy in these results is very low compared to the original accuracy, referring to Table 2. This means that the added BQs based on the 7 similarity metrics represent much more noise than the ones ranked by our LASSO ranking method. Obviously, this will significantly harm the accuracy of the state-of-the-art VQA models. According to the above, we see that the rankings by these 7 sentence similarity metrics are not effective in this context.

(ii) Which VQA model is the most robust? We divide current VQA models into two categories, attention-based and non-attention-based. Referring to Table 4, HAV, HAR, MUA and MLB are attention-based models whereas LQI and MU are not. Generally speaking and according to Table 4, the attention-based VQA models are more robust than non-attention-based ones. However, when we consider MU and MUA in Table 4 ($R_{\text{score2}}$), the non-attention-based model (MU) is more robust than the attention-based model (MUA). Note that the difference between MU and MUA is only the attention mechanism. Yet, in Table 4 ($R_{\text{score1}}$), MUA is more robust than MU. It implies that the variety of BQ candidates affects the robustness of attention-based VQA models in some cases. Finally, based on Table 4, we conclude that HieCoAtt Lu et al (2016) is the most robust VQA model. Since the HieCoAtt model with co-attention mechanism which repeatedly exploits the text and image information to guide each other, it...
Fig. 5: The figure shows the “accuracy” and “accuracy decrement” of the six state-of-the-art pretrained VQA models evaluated on GBQD, YNBQD and VQA Antol et al (2015) datasets. These results are based on our proposed LASSO BQ ranking method. Note that we divide the top 21 ranked GBQs into 7 partitions where each partition contains 3 ranked GBQs; this is in reference to (a)-1 and (a)-2. We also divide the top 21 ranked YNBQs into 7 partitions and each partition contains 3 ranked YNBQs; this is in reference to (b)-1 and (b)-2. BQs are acting as noise, so the partitions represent the noises ranked from the least noisy to the noisiest. That is, in this figure the first partition is the least noisy partition and so on. Because the plots are monotonously decreasing in accuracy, or, equivalently, monotonously increasing in accuracy decrement, the ranking is effective. In this figure, “First top 3” represents the first partition, “Second top 3” represents the second partition and so on.

Fig. 6: This figure shows the accuracy of six state-of-the-art pretrained VQA models evaluated on the GBQD and VQA dataset by different BQ ranking methods, BLEU-1, BLEU-2, BLEU-3, BLEU-4, ROUGE, CIDEr and METEOR. In (a), the grey shade denotes BLEU-1, blue shade denotes BLEU-2, orange shade denotes BLEU-3, purple shade denotes BLEU-4 and green shade denotes ROUGE. In this figure, the definition of partitions are same as Figure 5. The original accuracy of the six VQA models can be referred to Table 2-(a), Table 2-(b), etc. To make the figure clear, we plot the results of CIDEr and METEOR in (b) and (c), respectively. Based on this figure and Figure 5 in our paper, our LASSO ranking method performance is better than those seven ranking methods.

makes VQA models more robust Lu et al (2016); Huang et al (2019). Based on our experimental result, we know that HieCoAtt is the most robust VQA model, and this motivates us to conduct the extended experiments for this model.

(iii) Can basic questions directly help the accuracy of the HieCoAtt model? According to Table 4, we know that HieCoAtt is the most robust VQA model. Also, it was the previous state-of-the-art VQA model in the sense of accuracy Lu et al (2016). The above reasons motivate us to conduct the extended experiment and analysis of this model. We claim that if the quality of BQs is good enough, then using direct concatenation of MQ and BQs helps the accuracy of
**Fig. 7:** Visual Question Answering by Basic Questions (VQABQ) pipeline. Note that in Module 1 all of the training and validation questions are only encoded by Skip-Thought Question Encoder once for generating the Basic Question Matrix. That is, the next input of Skip-Thought Question Encoder is only a new main question. Module 2 is a VQA model which we want to test, and it is the HieCoAtt VQA model in our case. Regarding the input question of the HieCoAtt model, it is the direct concatenation of a given main question with the corresponding selected basic questions based on the Threshold-based Criterion. “D” denotes the direct concatenation of basic questions.

| score1 | score2/score1 | score3/score2 |
|--------|--------------|--------------|
| avg 0.33 | 0.61         | 0.73         |
| std 0.20 | 0.27         | 0.21         |

Table 5: In this table, “avg” denotes average and “std” denotes standard deviation.

| Opend-Ended Case (Total: 244362 questions) |
|------------------------------------------|
| 0 BQ (96.84%)                           |
| 1 BQ (3.07%)                            |
| 2 BQ (0.09%)                            |
| 3 BQ (0.00%)                            |
| # Q 236570                              |
| 7012 211                                |
| 9                                         |

Table 6: The table shows how many BQs are appended. “X BQ” means X BQs are appended by MQ, where X = 0, 1, 2, 3, and “# Q” denote number of questions.

The HieCoAtt VQA model. To justify the claim, we propose a framework, Visual Question Answering by Basic Questions (VQABQ), to exploit selected BQs to analyze the HieCoAtt VQA model, referring to Figure 7. We select BQs with a good quality based on a threshold-based criterion, referring to Algorithm 1. In our proposed BQD, each MQ has 21 corresponding BQs with scores and these scores are all between [0 – 1] with the following order:

\[ \text{score}1 \geq \text{score}2 \geq \ldots \geq \text{score}21, \]

where we further define three thresholds, s1, s2 and s3, for the selection process. For convenience, we only take the top 3 ranked BQs to do the selection. Then, we compute the averages (avg) and standard deviations (std) for score1, score2/score1, and score3/score2, respectively (refer to Table 5). We use \( \text{avg} \pm \text{std} \) to be the initial estimation of the above three thresholds. We discover that when \( s1 = 0.60, s2 = 0.58, \) and \( s3 = 0.41 \), we will get the BQs which best help the accuracy of the HieCoAtt VQA model in case of the MQ-BQs direct concatenation method.

According to Table 6, about 96.84% testing questions (MQs) cannot find the proper BQs to improve the accuracy of the HieCoAtt model by the MQ-BQs direct concatenation method. Although we only have around 3.16% MQs benefit from the BQs, our method still makes the performance of the HieCoAtt model competitive, accuracy increasing from 60.32% to 60.34%, referring to Table 7. In other words, the number of questions answered correctly by our proposed method is around 49 questions more than the original HieCoAtt VQA model Lu et al (2016). It implies that if we have a good enough basic question dataset, then it helps us increase more accuracy. Accordingly, based on our experimental results, we believe that BQs with good enough quality help the accuracy of the HieCoAtt VQA model by using the direct concatenation method.

(iv) Is question sentences preprocessing necessary? We claim that question sentences preprocessing is necessary for our proposed LASSO ranking method. For convenience, we exploit the same HieCoAtt model to show the claim. In the previous Methodology section, we do the question sentences preprocessing before the sentences embedding. If we do not have the step of question sentences preprocessing, the LASSO ranking method will generate some random ranking result. For convenience, we take the same HieCoAtt VQA model to demonstrate what the random ranking is. As shown

### Algorithm 1  MQ-BQs Concatenation Algorithm

1: Note that s1, s2, s3 are thresholds we can choose.
2: procedure MQ-BQs concatenation
3: if score1 > s1 then
4: appending the given MQ and BQ1 with the largest score
5: if score2/score1 > s2 then
6: appending the given MQ, BQ1, and BQ2 with the second large score
7: if score3/score2 > s3 then
8: appending the given MQ, BQ1, BQ2, and BQ3 with the third large score

Table 7: Evaluation results of HieCoAtt (Alt,VGG19) model improved by Algorithm 1. Note that the original accuracy of HieCoAtt (Alt,VGG19) VQA model for “test-dev-acc” is 60.48 and for “test-std-acc” is 60.32.
Table 8: The HieCoAtt (Alt, VGG19) model evaluation results on BQD and VQA dataset Antol et al (2015) without question sentences preprocessing. “-” indicates the results are not available. “-std” means that the VQA model is evaluated by the complete testing set of BQD and VQA dataset, and “-dev” means that the VQA model is evaluated by the partial testing set of BQD and VQA dataset. In addition, \( \text{diff} = \text{Original}_{\text{dev}} - \text{X}_{\text{dev}} \), where \( X \) is equal to “First”, “Second”, “Fourth”.

| Task Type       | Open-Ended  |
|-----------------|-------------|
| Method          | HieCoAtt (Alt, VGG19) |
| Test Set        | dev - All  |
| Partition       | Original - All | Original-standard |
|                  | Original - dev | Original-standard |

|                      | Original-dev | Original-standard |
|----------------------|--------------|-------------------|
| First-dev            | 51.77        | 51.95             |
| Second-dev           | 58.65        | 38.22             |
| Third-dev            | 59.70        | 79.95             |
| Fourth-dev           | 51.81        | -                 |
| Fifth-dev            | -            | -                 |
| Sixth-dev            | -            | -                 |
| Seventh-dev          | -            | -                 |
| Original-dev         | -            | -                 |
| Original-standard    | -            | -                 |

Fig. 8: This figure demonstrates what is the ranking result of jumping randomly. For convenience, we only take the most robust VQA model, HieCoAtt, to demonstrate the random jump. If we do not have question sentences preprocessing, then the proposed \textit{LASSO} ranking method is ineffective. That is, if we have done the question sentences preprocessing, the trend in this figure should be similar to Figure 5-(a)-1 and Figure 5-(b)-1. In this figure, “MQ only” represents the original query question and “First top 3” represents the first partition, “Second top 3” represents the second partition and so on. For the detailed numbers, please refer to Table 8.

in Figure 8, the ranking result is jumping randomly because of not doing the question sentences preprocessing. If the proposed method works correctly, the trend of Figure 8 should be monotone like trends in Figure 5.

(v) \textbf{What are the pros and cons of each metric?}

To compare with our proposed \textit{LASSO} basic question ranking method, we also conduct the basic question ranking experiments using the seven aforementioned text similarity metrics on the same basic question candidate dataset. Although the ranking performance of these metrics is less than satisfactory, various works Xu et al (2015); Mostafazadeh et al (2016); Karpathy and Fei-Fei (2015); Vinyals et al (2015); Fang et al (2015) still use them for sentence evaluation because of their simple implementation. As for our \textit{LASSO} ranking method, the ranking performance is quite effective, despite its simplicity. Note that, in practice, we will directly use our proposed datasets to test the robustness of VQA models without running the \textit{LASSO} ranking method again, so the computational complexity of \textit{LASSO} ranking method is not an issue in this case.

(vi) \textbf{Is the ranking in semantic meaning effective?}

In the \textit{LASSO} BQ ranking method, the semantic meaning of a question cannot be ranked very accurately but it still works quite well. This is primarily due to the state-of-the-art question encoder, Skip-thoughts Kiros et al (2015). It cannot completely capture the semantic meaning of the question and embed it into vector format. We believe that if more semantic encoders are developed in the future, the \textit{LASSO} ranking method can readily make use of them to produce more semantically driven ranking. Although the semantic meaning ranking by \textit{LASSO} ranking method is not very accurate, it is still acceptable. We provide some BQ ranking results using our \textit{LASSO} ranking method in Figure 4 and Table 1.

(vii) \textbf{What affects the quality of BQs?}

In our model, \( \lambda \) is one of the most important factors that can affect the quality of BQs. Through our experiments, we find that \( \lambda \in [10^{-6}, 10^{-5}] \) yields satisfactory ranking performance. One can refer to Figure 5 to get an understanding of the satisfactory ranking performance. We provide some ranking examples based on \textit{LASSO} ranking method in Table 1 to show the quality of BQs when \( \lambda = 10^{-6} \).

(viii) \textbf{Extended experiments on YNBQD dataset.}

Although we have done the basic question ranking experiments by the seven different text similarity metrics, \( \textit{BLEU}_1..._4, \textit{ROUGE}, \textit{CIDEr}, \textit{METEOR} \) on GBQD, we haven’t done such ranking experiments by those metrics on YNBQD. So, we explain the experimental details in the following. We conduct the extended experiments on our proposed YNBQD dataset by the above seven different text similarity metrics. In Figure 9, the definition of partitions are the same as Figure 5. The original accuracy of the six VQA models is given in Table 3-(a), Table 3-(b), etc. For convenience, we plot the results of
Fig. 9: This figure shows the accuracy of six state-of-the-art pretrained VQA models evaluated on the YNBQD and VQA Antol et al (2015) dataset by different BQ ranking methods, BLEU-1, BLEU-2, BLEU-3, BLEU-4, ROUGE, CIDEr and METEOR. The result in this figure is consistent with the result in Figure 6. Note that in Figure 9-(a), the grey shade denotes BLEU-1, blue shade denotes BLEU-2, orange shade denotes BLEU-3, purple shade denotes BLEU-4 and green shade denotes ROUGE. For more detailed explanation, please refer to the Extended experiments on YNBQD dataset subsection.

CIDEr and METEOR in Figure 9-(b) and Figure 9-(c), respectively. Based on Figure 9, Figure 6, and Figure 5, we conclude that the proposed LASSO ranking method performance is better than those seven ranking methods on both YNBQD and GBQD datasets. For the detail numbers of all the experiment, please refer to Table 2, 3, ..., 22.

5 Discussion

In this section, we present state-of-the-art VQA models among our six tested VQA models, Antol et al (2015); Lu et al (2016); Ben-younes et al (2017); Kim et al (2017), in different senses.

In the sense of robustness.

According to Table 4, we observe that “HieCoAtt (Alt,VGG19)” model has the highest $R_{score1}$, 0.48. Furthermore, “HieCoAtt (Alt,Resnet200)” has the highest $R_{score2}$, 0.53. Therefore, for GBQD, “HieCoAtt (Alt,VGG19)” model is the state-of-the-art VQA model among our six tested VQA models in the sense of robustness. However, for YNBQD, “HieCoAtt (Alt,Resnet200)” model is the state-of-the-art VQA model among our six tested VQA models in the sense of robustness. Additionally, “LSTM Q+I” model has the lowest $R_{score1}$ and $R_{score2}$. Generally speaking, we can say that the attention-based VQA model is more robust than the non-attention-based one.

In the sense of accuracy.

According to Table 2, we discover that “MUTAN with Attention” model in Table 2-(d) has the highest accuracy, 65.77, and “LSTM Q+I” has the lowest accuracy, 58.18. Therefore, “MUTAN with Attention” model is the state-of-the-art VQA model among our six tested VQA models in the sense of accuracy. Also, these results imply that the attention-based VQA model has higher accuracy than the non-attention-based one.

6 Conclusion

In this work, we propose a novel method comprised of a number of components namely, large-scale General Basic Question Dataset, Yes/No Basic Question Dataset and robustness measure ($R_{score}$) for measuring the robustness of VQA models.

Our method contains two main modules, VQA module and Noise Generator. The former one is able to rank the given BQs and the latter one is able to take the query, basic questions and an image as input and then output the natural language answer of the given query question about the image. The goal of the proposed method is to serve as a benchmark to help the community in building more accurate and robust VQA models.

Moreover, based on our proposed General and Yes/No Basic Question Datasets and $R_{score}$, we show that our LASSO BQ ranking method has the better ranking performance among most of the popular text evaluation metrics. Finally, we have some new methods to evaluate the robustness of VQA models, so how to build a robust and accurate VQA model will be interesting future work.

A Appendices

Detailed experimental results are presented in Table 9, 10, ..., 22.
### Table 9: The table shows the six state-of-the-art pretrained VQA models evaluation results on the GBQD and VQA dataset. "=" indicates the results are not available. "std" represents the accuracy of VQA model evaluated on the complete testing set of GBQD and VQA dataset and "dev" indicates the accuracy of VQA model evaluated on the partial testing set of GBQD and VQA dataset. In addition, \( diff = Original_{dev} - Original_{std} \), where \( X \) is equal to the "First", "Second", etc.

| Task Type | Method                          | Open-Ended (BLEU-1) | Open-Ended (BLEU-2) | Open-Ended (BLEU-3) |
|-----------|--------------------------------|---------------------|---------------------|---------------------|
|           | Dev                            | All                 | Dev                 | All                 |
|           | First-std                       | 48.33               | 48.50               | 49.01               |
|           | Second-std                      | 48.07               | 48.31               | 49.01               |
|           | Third-std                       | 48.30               | 48.47               | 49.38               |
|           | Fourth-std                      | 48.87               | 48.95               | 49.23               |
|           | Fifth-std                       | 48.97               | 49.03               | 50.06               |
|           | Sixth-std                       | 49.00               | 49.20               | 50.18               |
|           | Seventh-std                     | 49.12               | 49.23               | 50.28               |

### Table 10: The table shows the six state-of-the-art pretrained VQA models evaluation results on the GBQD and VQA dataset. "=\) indicates the results are not available. "std" represents the accuracy of VQA model evaluated on the complete testing set of GBQD and VQA dataset and "dev\) indicates the accuracy of VQA model evaluated on the partial testing set of GBQD and VQA dataset. In addition, \( diff = Original_{dev} - Original_{std} \), where \( X \) is equal to the "First", "Second", etc.

| Task Type | Method                          | Open-Ended (BLEU-1) | Open-Ended (BLEU-2) | Open-Ended (BLEU-3) |
|-----------|--------------------------------|---------------------|---------------------|---------------------|
|           | Dev                            | All                 | Dev                 | All                 |
|           | First-std                       | 48.33               | 48.50               | 49.01               |
|           | Second-std                      | 48.07               | 48.31               | 49.01               |
|           | Third-std                       | 48.30               | 48.47               | 49.38               |
|           | Fourth-std                      | 48.87               | 48.95               | 49.23               |
|           | Fifth-std                       | 48.97               | 49.03               | 50.06               |
|           | Sixth-std                       | 49.00               | 49.20               | 50.18               |
|           | Seventh-std                     | 49.12               | 49.23               | 50.28               |

### Assessing the Robustness of Visual Question Answering Models

Table 9 shows the six state-of-the-art pretrained VQA models evaluation results on the GBQD and VQA dataset. In addition, \( diff = Original_{dev} - Original_{std} \), where \( X \) is equal to the "First", "Second", etc.
Table 11: The table shows the six state-of-the-art pretrained VQA models evaluation results on the GBQD and VQA dataset. “−” indicates the results are not available. “std” represents the accuracy of VQA model evaluated on the complete testing set of GBQD and VQA dataset and “dev” indicates the accuracy of VQA model evaluated on the partial testing set of GBQD and VQA dataset. In addition, \( d_{\text{diff}} = \text{Original}_{\text{dev}} - \text{X}_{\text{dev}} \), where \( X \) is the “First”, “Second”, etc.

Table 12: The table shows the six state-of-the-art pretrained VQA models evaluation results on the GBQD and VQA dataset. “−” indicates the results are not available. “std” represents the accuracy of VQA model evaluated on the complete testing set of GBQD and VQA dataset and “dev” indicates the accuracy of VQA model evaluated on the partial testing set of GBQD and VQA dataset. In addition, \( d_{\text{diff}} = \text{Original}_{\text{dev}} - \text{X}_{\text{dev}} \), where \( X \) is equal to the “First”, “Second”, etc.
Table 13: The table shows the six state-of-the-art pretrained VQA models evaluation results on the GBQD and VQA dataset. "−" indicates the results are not available, "std" represents the accuracy of VQA model evaluated on the complete testing set of GBQD and VQA dataset and "dev" indicates the accuracy of VQA model evaluated on the partial testing set of GBQD and VQA dataset. In addition, \(diff = \text{Original}_{\text{dev}} - \text{X}_{\text{dev}}\), where \(X\) is equal to the "First", "Second", etc.

Table 14: The table shows the six state-of-the-art pretrained VQA models evaluation results on the GBQD and VQA dataset. "−" indicates the results are not available, "std" represents the accuracy of VQA model evaluated on the complete testing set of GBQD and VQA dataset and "dev" indicates the accuracy of VQA model evaluated on the partial testing set of GBQD and VQA dataset. In addition, \(diff = \text{Original}_{\text{dev}} - \text{X}_{\text{dev}}\), where \(X\) is equal to the "First", "Second", etc.
Table 15: The table shows the six state-of-the-art pretrained VQA models evaluation results on the GBQD and VQA dataset. "-" indicates the results are not available, "-std" represents the accuracy of VQA model evaluated on the complete testing set of GBQD and VQA dataset and "dev" indicates the accuracy of VQA model evaluated on the partial testing set of GBQD and VQA dataset. In addition, $\text{diff} = \text{Original-dev} - \text{X-devAHT}$, where $X$ is equal to the “First,” “Second,” etc.

Table 16: The table shows the six state-of-the-art pretrained VQA models evaluation results on the YNBQD and VQA dataset. "-" indicates the results are not available, "-std" represents the accuracy of VQA model evaluated on the complete testing set of YNBQD and VQA dataset and "dev" indicates the accuracy of VQA model evaluated on the partial testing set of YNBQD and VQA dataset. In addition, $\text{diff} = \text{Original-devAHT} - \text{X-devAHT}$, where $X$ is equal to the “First,” “Second,” etc.
Table 17: The table shows the six state-of-the-art pretrained VQA models evaluation results on the YNBQD and VQA dataset. “–” indicates the results are not available, “std” represents the accuracy of VQA model evaluated on the complete testing set of YNBQD and VQA dataset and “–dev” indicates the accuracy of VQA model evaluated on the partial testing set of YNBQD and VQA dataset. In addition, \( \text{diff} = \text{Original}_{\text{dev}} - X_{\text{dev}} \), where \( X \) is equal to the “First”, “Second”, etc.

| Task Type | Method | Open-Ended (BLEU-2) | Open-Ended (BLEU-3) | Open-Ended (BLEU-3) |
|-----------|--------|---------------------|---------------------|---------------------|
| First-dev | HieCoAtt (Alt, VGG19) | 47.29 | 36.44 | 81.47 |
| Second-dev | HieCoAtt (Alt, VGG19) | 47.32 | 36.48 | 81.50 |
| Third-dev | HieCoAtt (Alt, VGG19) | 47.35 | 36.52 | 81.53 |
| Fourth-dev | HieCoAtt (Alt, VGG19) | 47.37 | 36.56 | 81.56 |
| Fifth-dev | HieCoAtt (Alt, VGG19) | 47.40 | 36.60 | 81.59 |
| Sixth-dev | HieCoAtt (Alt, VGG19) | 47.43 | 36.64 | 81.62 |

| Task Type | Method | Open-Ended (BLEU-2) | Open-Ended (BLEU-3) | Open-Ended (BLEU-3) |
|-----------|--------|---------------------|---------------------|---------------------|
| First-dev | HieCoAtt (Alt, ResNet200) | 47.30 | 36.56 | 81.49 |
| Second-dev | HieCoAtt (Alt, ResNet200) | 47.33 | 36.60 | 81.52 |
| Third-dev | HieCoAtt (Alt, ResNet200) | 47.36 | 36.64 | 81.55 |
| Fourth-dev | HieCoAtt (Alt, ResNet200) | 47.39 | 36.68 | 81.58 |
| Fifth-dev | HieCoAtt (Alt, ResNet200) | 47.42 | 36.72 | 81.61 |
| Sixth-dev | HieCoAtt (Alt, ResNet200) | 47.45 | 36.76 | 81.64 |

Table 18: The table shows the six state-of-the-art pretrained VQA models evaluation results on the YNBQD and VQA dataset. “–” indicates the results are not available, “std” represents the accuracy of VQA model evaluated on the complete testing set of YNBQD and VQA dataset and “–dev” indicates the accuracy of VQA model evaluated on the partial testing set of YNBQD and VQA dataset. In addition, \( \text{diff} = \text{Original}_{\text{dev}} - X_{\text{dev}} \), where \( X \) is equal to the “First”, “Second”, etc.
Table 19: The table shows the six state-of-the-art pretrained VQA models evaluation results on the YNBQD and VQA dataset. "−" indicates the results are not available, "−std" represents the accuracy of VQA model evaluated on the complete testing set of YNBQD and VQA dataset and "−dev" indicates the accuracy of VQA model evaluated on the partial testing set of YNBQD and VQA dataset. In addition, \(df = \text{Original}_{\text{dev\_val}} - \text{X}_{\text{dev\_val}}\), where \(X\) is equal to the "First", "Second", etc.

| Task Type | Method | Open-Ended (ROUGE) | Open-Ended (BLEU-4) | HieCoAtt (Alt,VGG19) | LSTM Q+i |
|-----------|--------|--------------------|---------------------|----------------------|---------|
| Test Set  | Other  | Otherstd | V/A | All | Other  | Otherstd | V/A | All | Other  | Otherstd | V/A | All |
| Partition | MSE   | MSE     | V/A | All | MSE   | MSE     | V/A | All | MSE   | MSE     | V/A | All |
| First-dev | 1.29  | 1.41   | 27.47 | 14.03 | 47.47 | 1.19  | 1.39   | 27.34 | 14.00 | 47.46 | 1.19  | 1.39   | 27.34 | 14.00 | 47.46 | 1.19  | 1.39   | 27.34 | 14.00 | 47.46 |
| Second-dev | 1.47  | 1.50   | 27.07 | 14.95 | 48.70 | 1.26  | 1.45   | 27.34 | 14.01 | 49.36 | 1.26  | 1.45   | 27.34 | 14.01 | 49.36 | 1.26  | 1.45   | 27.34 | 14.01 | 49.36 |
| Third-dev | 1.47  | 1.50   | 27.07 | 14.95 | 48.70 | 1.26  | 1.45   | 27.34 | 14.01 | 49.36 | 1.26  | 1.45   | 27.34 | 14.01 | 49.36 | 1.26  | 1.45   | 27.34 | 14.01 | 49.36 |
| Fourth-dev | 1.47  | 1.50   | 27.07 | 14.95 | 48.70 | 1.26  | 1.45   | 27.34 | 14.01 | 49.36 | 1.26  | 1.45   | 27.34 | 14.01 | 49.36 | 1.26  | 1.45   | 27.34 | 14.01 | 49.36 |
| Fifth-dev | 1.47  | 1.50   | 27.07 | 14.95 | 48.70 | 1.26  | 1.45   | 27.34 | 14.01 | 49.36 | 1.26  | 1.45   | 27.34 | 14.01 | 49.36 | 1.26  | 1.45   | 27.34 | 14.01 | 49.36 |
| Sixth-dev | 1.47  | 1.50   | 27.07 | 14.95 | 48.70 | 1.26  | 1.45   | 27.34 | 14.01 | 49.36 | 1.26  | 1.45   | 27.34 | 14.01 | 49.36 | 1.26  | 1.45   | 27.34 | 14.01 | 49.36 |
| Original-dev | 48.93 | 49.14 | 50.32 | 50.14 | 50.32 | 49.14 | 49.35 | 50.32 | 50.14 | 50.32 | 49.14 | 49.35 | 50.32 | 50.14 | 50.32 | 49.14 | 49.35 | 50.32 | 50.14 | 50.32 |

Table 20: The table shows the six state-of-the-art pretrained VQA models evaluation results on the YNBQD and VQA dataset. "−" indicates the results are not available, "−std" represents the accuracy of VQA model evaluated on the complete testing set of YNBQD and VQA dataset and "−dev" indicates the accuracy of VQA model evaluated on the partial testing set of YNBQD and VQA dataset. In addition, \(df = \text{Original}_{\text{dev\_val}} - \text{X}_{\text{dev\_val}}\), where \(X\) is equal to the "First", "Second", etc.
Table 21: The table shows the six state-of-the-art pretrained VQA models evaluation results on the YNBQD and VQA dataset. “−” indicates the results are not available, “-std” represents the accuracy of VQA model evaluated on the complete testing set of YNBQD and VQA dataset and “-dev” indicates the accuracy of VQA model evaluated on the partial testing set of YNBQD and VQA dataset. In addition, $d_i f = \text{Original}_{dev_X} - \text{VQA}_{dev_X}$, where $X$ is equal to the “First”, “Second”, etc.

Table 22: The table shows the six-state-of-the-art pretrained VQA models evaluation results on the YNBQD and VQA dataset. “−” indicates the results are not available, “-std” represents the accuracy of VQA model evaluated on the complete testing set of YNBQD and VQA dataset and “-dev” indicates the accuracy of VQA model evaluated on the partial testing set of YNBQD and VQA dataset. In addition, $d_i f = \text{Original}_{dev_X} - \text{VQA}_{dev_X}$, where $X$ is equal to the “First”, “Second”, etc.
References

Agrawal A, Batra D, Parikh D, Kembhavi A (2018) Don’t just assume; look and answer: Overcoming priors for visual question answering. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp 4971–4980

Andreas J, Rohrbach M, Darrell T, Klein D (2016a) Deep compositional question answering with neural module networks. In: Proc. IEEE Conf. Comp. Vis. Patt. Recongn

Andreas J, Rohrbach M, Darrell T, Klein D (2016b) Neural module networks. In: Proceedings of the IEEE International Conference on Computer Vision, pp 2425–2433

Banerjee S, Lavie A (2005) Meteor: An automatic metric for mt evaluation with improved correlation with human judgments. In: Proceedings of the acl workshop on intrinsic and extrinsic evaluation measures for machine translation and/or summarization, vol 29, pp 65–72

Barzilay R, Elhadad M (1999) Using lexical chains for text summarization. Advances in automatic text summarization pp 111–121

Ben-younes H, Cadene R, Cord M, Thome N (2017) Mutan: Multimodal tucker fusion for visual question answering. arXiv preprint arXiv:170506676

Carlini N, Wagner D (2017) Towards evaluating the robustness of deep networks. In: Security and Privacy (SP), 2017 IEEE Symposium on, IEEE, pp 39–57

Chen L, Yan X, Xiao J, Zhang H, Pu S, Zhuang Y (2020) Counterfactual samples synthesizing for robust visual question answering. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp 10800–10809

Chung J, Gulcehre C, Cho K, Bengio Y (2014) Empirical evaluation of gated recurrent neural networks on sequence modeling. arXiv preprint arXiv:14123555

Di Sipio R, Huang JH, Chen SYC, Mangini S, Worring M (2022) The dawn of quantum natural language processing. ICASSP

Elliott D, Keller F (2013) Image description using visual dependency representations. In: Proceedings of the 2013 Conference on Empirical Methods in Natural Language Processing, pp 1292–1302

Fang H, Gupta S, Iandola F, Srivastava RK, Deng L, Dollár P, Gao J, He X, Mitchell M, Platt JC, et al (2015) From captions to visual concepts and back. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp 1473–1482

Fawzi A, Moosavi Dezfooli SM, Frossard P (2017) A geometric perspective on the robustness of deep networks. Tech. rep., Institute of Electrical and Electronics Engineers

Fukui A, Park DH, Yang D, Rohrbach A, Darrell T, Rohrbach M (2016) Multimodal compact bilinear pooling for visual question answering and visual grounding. In: Conference on Empirical Methods in Natural Language Processing (EMNLP)

Gao H, Mao J, Zhou J, Huang Z, Wang L, Xu W (2015) Are you talking to a machine? dataset and methods for multilingual image question. In: Advances in Neural Information Processing Systems, pp 2296–2304

Geman D, Geman S, Hallonquist N, Younes L (2015) Visual Turing test for computer vision systems. Proceedings of the National Academy of Sciences 112(12):3618–3623

Hu T, Mettes P, Huang JH, Snoek CG (2019) Sileo: Show a few images, localize the common object. In: ICCV, pp 5067–5076

Huang JH (2017) Robustness analysis of visual question answering models by basic questions. King Abdullah University of Science and Technology, Master Thesis

Huang JH, Worring M (2020) Query-controllable video summarization. In: ICPR, pp 242–250

Huang JH, Alfadly M, Ghanem B (2017) Vqabq: Visual question answering by basic questions. VQA Challenge Workshop, CVPR

Huang JH, Alfadly M, Ghanem B (2018) Robustness analysis of visual qa models by basic questions. VQA Challenge and Visual Dialog Workshop, CVPR

Huang JH, Alfadly M, Ghanem B (2019) A novel framework for robustness analysis of visual qa models. In: Proceedings of the Thirty-Third AAAI Conference on Artificial Intelligence, vol 33, pp 8449–8456

Huang JH, Murn L, Mrak M, Worring M (2021a) Gpt2mvs: Generative pre-trained transformer-2 for multi-modal video summarization. In: ICMR, pp 580–589

Huang JH, Wu TW, Worring M (2021b) Contextualized keyword representations for multi-modal retinal image captioning. In: ICMR, pp 645–652

Huang JH, Wu TW, Yang CHH, Worring M (2021c) Deep context-encoding network for retinal image captioning. In: ICIP, IEEE, pp 3762–3766

Huang JH, Wu TW, Yang CHH, Worring M (2021d) Longer version for” deep context-encoding network for retinal image captioning”. arXiv preprint arXiv:210514538

Huang JH, Yang CHH, Liu F, Tian M, Liu YC, Wu TW, Lin I, Wang K, Morikawa H, Chang H, et al (2021e) Deepophth: medical report generation for retinal images via deep models and visual explanation. In: WACV, pp 2442–2452

Huang JH, Wu TW, Yang CHH, Shi Z, Lin I, Teigner J, Worring M, et al (2022) Non-local attention improves description generation for retinal images. In: WACV, pp 1606–1615
Huck Yang CH, Liu F, Huang JH, Tian M, Lin IH, Liu YC, Morikawa H, Yang HH, Tegner J (2018) Auto-classification of retinal diseases in the limit of sparse data using a two-streams machine learning model. In: ACCV, Springer, pp 323–338

Ji Z, Ma Y, Pang Y, Li X (2019) Query-aware sparse coding for web multi-video summarization. Information Sciences 478:152–166

Kalle K, Kanan C (2017a) An analysis of visual question answering algorithms. arXiv preprint arXiv:170309684

Kalle K, Kanan C (2017b) Visual question answering: Datasets, algorithms, and future challenges. Computer Vision and Image Understanding

Karpathy A, Fei-Fei L (2015) Deep visual-semantic alignments for generating image descriptions. In: Proceedings of the IEEE Conference on CVPR, pp 3128–3137

Kim JH, On KW, Lim W, Kim J, Ha JW, Zhang BT (2017) Hadamard product for low-rank bilinear pooling. In: 5th International Conference on Learning Representations

Kiros R, Salakhudinov R, Zemel RS (2014) Multimodal neural language models. In: Icml, vol 14, pp 595–603

Kiros R, Zhu Y, Salakhudinov RR, Zemel R, Urtasun R, Torralba A, Fidler S (2015) Skip-thought vectors. In: NIPS, pp 3294–3302

Klein D, Manning CD (2003) Accurate unlexicalized parsing. In: Proceedings of the 41st Annual Meeting on Association for Computational Linguistics-Volume 1, Association for Computational Linguistics, pp 423–430

Kolling C, More M, Gavenski N, Pooch E, Parraga O, Barros RC (2022) Efficient counterfactual debiasing for visual question answering. In: Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision, pp 3001–3010

Krishna R, Zhu Y, Groth O, Johnson J, Hata K, Kravitz J, Chen S, Kalantidis Y, Li LJ, Shamma DA, et al (2017) Visual genome: Connecting language and vision using crowdsourced dense image annotations. International Journal of Computer Vision 123(1):32–73

Kulkarni G, Premraj V, Dhar S, Li S, Choi Y, Berg AC, Berg TL (2011) Baby talk: Understanding and generating image descriptions. In: Proceedings of the 24th CVPR, Citeseer

Li R, Jia J (2016) Visual question answering with question representation update (qru). In: NIPS, pp 4655–4663

Lin CY (2004) Rouge: A package for automatic evaluation of summaries. In: Text summarization branches out: Proceedings of the ACL-04 workshop, Barcelona, Spain, vol 8

Lin TY, Maire M, Belongie S, Hays J, Perona P, Ramanan D, Dollár P, Zitnick CL (2014) Microsoft coco: Common objects in context. In: ECCV, Springer, pp 740–755

Lin TY, RoyChowdhury A, Maji S (2015) Bilinear cnn models for fine-grained visual recognition. In: Proceedings of the IEEE International Conference on Computer Vision, pp 1449–1457

Liu YC, Yang HH, Huck Yang CH, Huang JH, Tian M, Morikawa H, Tsai YCJ, Tegner J (2018) Synthesizing new retinal symptom images by multiple generative models. In: ACCV, Springer, pp 235–250

Lu J, Yang J, Batra D, Parikh D (2016) Hierarchical question-image co-attention for visual question answering. In: NIPS, pp 289–297

Ma L, Lu Z, Li H (2016) Learning to answer questions from image using convolutional neural network. In: AAAI, p 16

Malinowski M, Fritz M (2014a) A multi-world approach to question answering about real-world scenes based on uncertain input. In: Advances in Neural Information Processing Systems, pp 1682–1690

Malinowski M, Fritz M (2014b) Towards a visual turing challenge. arXiv preprint arXiv:14108027

Malinowski M, Fritz M (2015) Hard to cheat: A turing test based on answering questions about images. arXiv preprint arXiv:150103302

Malinowski M, Rohrbach M, Fritz M (2015) Ask your neurons: A neural-based approach to answering questions about images. In: Proceedings of the IEEE International Conference on Computer Vision, pp 1–9

Malinowski M, Rohrbach M, Fritz M (2017) Ask your neurons: A deep learning approach to visual question answering. International Journal of Computer Vision (IJCV)

Mikolov T, Sutskever I, Chen K, Corrado GS, Dean J (2013) Distributed representations of words and phrases and their compositionality. In: NIPS, pp 3111–3119

Moosavi-Dezfooli SM, Fawzi A, Usato J, Frossard P (2018) Robustness via curvature regularization, and vice versa. arXiv preprint arXiv:181109716

Mostafazadeh N, Misra I, Devlin J, Mitchell M, He X, Vanderwende L (2016) Generating natural questions about an image. arXiv preprint arXiv:160306059

Nag Chowdhury S, Malinowski M, Bulling A, Fritz M (2016) Xplore-m-ego: Contextual media retrieval using natural language queries. In: Proceedings of the 2016 ACM on International Conference on Multimedia Retrieval, ACM, pp 243–247

Noh H, Hongsuck Seo P, Han B (2016a) Image question answering using convolutional neural network with dynamic parameter prediction. In: Proceedings of the IEEE Conference on CVPR, pp 30–38

Noh H, Hongsuck Seo P, Han B (2016b) Image question answering using convolutional neural network with dynamic parameter prediction. In: Proceedings of the IEEE Conference on CVPR, pp 30–38
Papineni K, Roukos S, Ward T, Zhu WJ (2002) Bleu: a method for automatic evaluation of machine translation. In: Proceedings of the 40th annual meeting on association for computational linguistics, Association for Computational Linguistics, pp 311–318

Pennington J, Socher R, Manning CD (2014) Glove: Global vectors for word representation. In: EMNLP, vol 14, pp 1532–1543

Regneri M, Rohrbach M, Wetzel D, Thater S, Schiele B, Pinkal M (2013) Grounding action descriptions in videos. Transactions of the Association for Computational Linguistics 1:25–36

Ren M, Kiros R, Zemel R (2015a) Exploring models and data for image question answering. In: Advances in Neural Information Processing Systems, pp 2953–2961

Ren M, Kiros R, Zemel R (2015b) Image question answering: A visual semantic embedding model and a new dataset. Proc Advances in Neural Inf Process Syst 1(2):5

Rips LJ (1994) The psychology of proof: Deductive reasoning in human thinking. Mit Press

Rohrbach A, Rohrbach M, Tandon N, Schiele B (2015) A dataset for movie description. In: Proceedings of the IEEE conference on computer vision and pattern recognition, pp 3202–3212

Sheng S, Singh A, Goswami V, Magana J, Thrush T, Galuba W, Parikh D, Kiela D (2021) Human-adversarial visual question answering. Advances in Neural Information Processing Systems 34

Silberman N, Hoiem D, Kohli P, Fergus R (2012) Indoor segmentation and support inference from rgbd images. Computer Vision–ECCV 2012 pp 746–760

Tapaswi M, Zhu Y, Stiefelhagen R, Torralba A, Urtasun R, Fidler S (2016) Movieqa: Understanding stories in movies through question-answering. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp 4631–4640

Vedantam R, Lawrence Zitnick C, Parikh D (2015) Cider: Consensus-based image description evaluation. In: The IEEE Conference on Computer Vision and Pattern Recognition (CVPR)

Vedantam R, Desai K, Lee S, Rohrbach M, Batra D, Parikh D (2019) Probabilistic neural-symbolic models for interpretable visual question answering. arXiv preprint arXiv:190207864

Vinyals O, Toshev A, Bengio S, Erhan D (2015) Show and tell: A neural image caption generator. In: Proceedings of the IEEE Conference on CVPR, pp 3156–3164

Wu Q, Wang P, Shen C, Dick A, van den Hengel A (2016) Ask me anything: Free-form visual question answering based on knowledge from external sources. In: CVPR, pp 4622–4630

Xiong C, Merity S, Socher R (2016) Dynamic memory networks for visual and textual question answering. arXiv 1603