Domain-robust VQA with diverse datasets and methods but no target labels

Mingda Zhang Tristan Maidment Ahmad Diab Adriana Kovashka Rebecca Hwa
Department of Computer Science, University of Pittsburgh
{mzhang, kovashka, hwa}@cs.pitt.edu {tdm51, ahd23}@pitt.edu
https://people.cs.pitt.edu/~mzhang/domain-robust-vqa/

Abstract

The observation that computer vision methods overfit to dataset specifics has inspired diverse attempts to make object recognition models robust to domain shifts. However, similar work on domain-robust visual question answering methods is very limited. Domain adaptation for VQA differs from adaptation for object recognition due to additional complexity: VQA models handle multimodal inputs, methods contain multiple steps with diverse modules resulting in complex optimization, and answer spaces in different datasets are vastly different. To tackle these challenges, we first quantify domain shifts between popular VQA datasets, in both visual and textual space. To disentangle shifts between datasets arising from different modalities, we also construct synthetic shifts in the image and question domains separately. Second, we test the robustness of different families of VQA methods (classic two-stream, transformer, and neuro-symbolic methods) to these shifts. Third, we test the applicability of existing domain adaptation methods and devise a new one to bridge VQA domain gaps, adjusted to specific VQA models. To emulate the setting of real-world generalization, we focus on unsupervised domain adaptation and the open-ended classification task formulation.

1. Introduction

Visual question answering (VQA) borders on AI-completeness: it requires perception (visual and linguistic) and cognition. Despite the strong performance of recent VQA methods, they fall short of generalization and true reasoning: they are known to suffer from dataset bias [22], require domain-specific languages or domain-specific executable program annotations [34, 41], or must be trained separately for each new dataset.

Prior work in domain adaptation for object recognition examines how robust methods are when trained and tested on different datasets (domains), and further proposes techniques to bridge domain gaps. In contrast, there is a shortage of analyses of how domain-robust visual question answering methods are. Importantly, domain adaptation techniques cannot successfully be applied in the VQA setting in a straightforward manner. First, VQA models take inputs across multiple modalities, each of which could contribute to the domain specificity of the trained models. Second, different VQA methods have multiple intermediate stages and processing steps over the inputs, which makes optimization challenging. Domain adaptation techniques could be applied at multiple of these stages, and domain adaptation can be performed jointly or separately from VQA training, with varying success. Third, answer spaces in different datasets are vastly different. While domain adaptation methods exist to tackle non-identical answer spaces in object recognition, this setting is not very common. Conversely, in VQA, it is the norm, since many datasets are highly specialized (for example, VizWiz [23] contains special answers “unanswerable” or “unsuitable image” because image-question pairs...
are provided by visually impaired users).

To tackle each of these challenges, we propose the following steps. First, to understand how the multiple modalities contribute to domain shifts, we break down and measure both visual and textual domain shifts across datasets. We disentangle shifts in image and question space by constructing synthetic dataset variants, to test how VQA methods respond to these separate shifts. To understand how the multiple steps and mechanisms in recent VQA models make them robust or fragile to shifts, we compare different families (classic two-stream, transformer, and neuro-symbolic methods) by exposing them to different shifts. We examine multiple mechanisms to bridge domain gaps for these methods, in the challenging setting of unsupervised adaptation where no labels from the target set are available, and discuss the differences in successful versus unsuccessful attempts. Third, to examine the contribution of answer space differences, we use the open-ended VQA classification formulation. Because no embedding is available for the answer options, the gap in answer spaces is more pronounced. We compare performance across datasets and observe relations between particular modality shifts and domain robustness.

In more detail, we compare image and question representations across nine datasets: VQA v1 and v2, VQA Abstract, Visual 7w, Visual Genome, COCO QA, CLEVR, GQA, and VizWiz. We find there are large shifts in both visual and textual space, both at a low- and high-level (e.g. syntax and meaning). We separately apply automatic style transfer (for the visual modality) and paraphrasing (for the textual modality) to disentangle VQA methods’ robustness separately to each of these artificial shifts. We also observe disparate contributions of these shifts in methods’ performance across real domain gaps.

We find evidence that neuro-symbolic, compositional models are more robust to domain shift than others, because in those methods, perception and reasoning are more disentangled. We argue that reasoning has the potential to be domain-independent: for example, the process of reasoning about spatial relationships can in theory be abstracted away from pixel space, thus should not need retraining if the pixel space changes. Inspired by the potential of perception-reasoning disentanglement, we design a two-stage domain adaptation technique to bridge domain gaps. We show that this two-stage variant is more successful than a direct, one-stage application of [17], and a version of [47], for recovering performance lost due to domain gaps.

We are only aware of two prior works on domain adaptation for VQA [10, 38]. Both of these consider supervised domain adaptation (labels present in target dataset) while we operate in an unsupervised setting (labels on source dataset only). They work with fewer datasets (2-5) and apply domain adaptation to fewer and simpler VQA methods. Our work can be seen as a “reality check” for VQA methods, similar to prior reality checks for metric learning and weakly supervised object detection [13, 43].

To summarize, our contribution is to answer the following questions: (1) In what ways (visual, semantic, syntactic) are image-question pairs from recent VQA datasets different? (2) What kind of dataset differences most affect VQA generalization? (3) Which methods are more robust to synthetic visual shifts? (4) Which methods allow more generalization when training/testing on different VQA datasets? (5) What domain adaptation techniques most successfully bridge domain gaps? (6) What are the challenges of performing domain adaptation in unsupervised VQA?

2. Related Work

VQA method families. We consider three families of methods and their robustness to domain shifts. Classic two-stream methods [3, 32, 42, 55] represent the input image and question separately, then fuse the representations to obtain an answer. Perception and cognition are entangled. Transformer methods [12, 16, 39, 58, 65] compute multiple layers of attention between entities in each modality (e.g. words to visual regions). They often use unsupervised pre-training on massive vision-language datasets (e.g. images with text captions). Other than positional encodings, these methods have no separate relational reasoning component. Neuro-symbolic, knowledge base, and graph methods are conceptually distinct as they break down question-answering into modules. Some of these perform perception (e.g. recognize objects) while others perform cognition (e.g. relational reasoning about object position). Notable representatives include [1, 2, 4, 29, 31, 34, 41, 44, 61, 62]. For example, in [2, 4, 41, 60], entities are first parsed in a perception step, then reasoning takes a composable logic form, and questions are answered by verifying if objects satisfy a relationship implied by the question. [44] extract information about objects, then look up related concepts in a knowledge base, and perform reasoning using a GCN. In this paper, we show that the ability to disentangle perception and reasoning enables more domain-robust question answering.

Dataset bias in VQA. Prior work has found it is easy to introduce undesirable artifacts during dataset construction, which models can utilize to achieve misleadingly strong results. For example, [22] find that questions can be answered well using language priors (and bypassing the need for reasoning). [51] help a model cope with priors by discouraging it from producing an answer similar to that produced by an image-blind model. [56] accomplish robustness through adversarial regularization, [21] by constructing logic compositions of existing questions, [20] through semantic image mutations, and [27] by adding noise to the questions. All of these are concerned with bias or lack of robustness within a single dataset, but do not examine how datasets differ in terms of image and question compositions.

Domain adaptation (DA) and generalization (DG) cope
with domain shifts, e.g. for object recognition. Unlike generalization [9, 49, 57], adaptation [6, 17, 26, 47] assumes that some (unlabeled and/or sparsely labeled) data is available in the target domain. In the most common, classical DA setting, source and target class vocabularies overlap. Domain adaptation is challenging for VQA in that answer spaces do not overlap. This setting has also been tackled in DA for object recognition, but less commonly: in partial DA [7, 8, 67], the target class space is a subset of the source space; and in open-set DA [46, 54], the target space could have new classes not present in the source. The key idea in DA is to bridge the source and target distributions and arrive at a shared representation. Some influential methods include gradient reversal from a domain classifier to ensure domain-agnostic features [17], cycle-consistency [26], separating shared and domain-specific features [6, 38], minimizing moments of features in different domains [47], maximizing norm which correlates with transferrability [63], maximizing overlap between prototypes from different datasets [45], etc. Methods specific to particular vision tasks also exist, e.g. for object detection where gradient reversal is applied at both the image and instance (region) level [11], for semantic segmentation [68], etc. Some prior work [15, 36, 37, 40, 48, 53, 59, 66] leverages style transfer techniques to bridge domain gaps, while we use style transfer and language paraphrasing to factor our shifts in the complex multi-input setting (images and question) in VQA.

Prior work in domain-robust VQA. Our work is the first to perform fully unsupervised domain adaptation for VQA. There are only two prior works in domain-robust VQA we are aware of, but both operate in the supervised setting (i.e. some target labels are available) [10]: find most of the domain shift lies in questions and answers. We consider more recent and diverse datasets, and find these contain significant image shifts as well. Further, [10] only considered a simple two-input MLP and two 2016 methods, while we consider three families of recent VQA methods. [10] is partially unsupervised; they do not use target labels to train the VQA model, but do use them to compute adaptable features. [64] only study the shift between two datasets, and only apply domain adaptation over a non-standard method for VQA. In contrast to [10, 64], we study nine datasets, and a new style transfer setting to isolate shifts in visual space.

3. Approach

We assume we have a labeled source dataset \( D^S = \{d^S_1, \ldots, d^S_i, \ldots, d^S_{|D^S|}\} \), where each \( d^S_i \) is an image-question-answer triplet \( \{v^S_i, q^S_i, a^S_i\} \). The image and question are inputs to the VQA model, and the ground-truth answer is the desired output. We also have an unlabeled target dataset \( D^T = \{d^T_1, \ldots, d^T_i, \ldots, d^T_{|D^T|}\} \) where each \( d^T_i \) is an image-question pair \( \{v^T_i, q^T_i\} \), and no answers are provided even in the training set. We aim to build a VQA model using \( D^S \) and \( D^T \), which can answer questions in \( D^T \). Any two datasets \( D^S \) and \( D^T \) have potentially large domains gaps, in terms of marginal distributions (of images, questions, or answers) or conditional distributions (e.g. answers given the images or questions). Therefore, the major challenge is to maximize the performance on \( D^T \) despite the domain gaps, and our strategy is to ensure the model trained on \( D^S \) is as transferable to \( D^T \) as possible.

We measure domain gaps for nine datasets (Sec. 3.1), describe how to construct synthetic gaps to disentangle visual and linguistic shifts (Sec. 3.2), and how to adapt domain adaptation techniques to bridge gaps (Sec. 3.3) for individual VQA methods (Sec. 3.4).

3.1. Measuring real domain gaps

The first step towards building a domain-robust VQA model is to understand the multi-faceted dataset gaps. We analyze the following datasets: (1) VQA v1 [5]; (2) VQA v2 [22]; (3) Visual Genome [35]; (4) Visual7W [69]; (5) COCO-QA [52]; (6) GQA [30]; (7) CLEVR [33]; (8) VQA Abstract [5]; (9) VizWiz [23]. We could measure shifts in the following distributions across datasets: (1) \( P(v) \); (2) \( P(q) \); (3) \( P(a) \); (4) \( P(q|v) \); (5) \( P(a|v) \); (6) \( P(a|q) \); (7) \( P(a|v, q) \), where \( v, q \) and \( a \) represent image, question and answer respectively. Here, we focus on measuring shifts in \( P(v) \) and \( P(q) \). To measure how much the corresponding distribution changes across datasets, we use Maximum Mean Discrepancy (MMD):

\[
\text{MMD} = \|E_{X \sim D^S} [\varphi(X)] - E_{Y \sim D^T} [\varphi(Y)]\|_H
\]

\[
= \frac{1}{n^2} \sum_{i=1}^{n} \sum_{j=1}^{n} k(x_i, x_j) + \frac{1}{n^2_t} \sum_{i=1}^{n_s} \sum_{j=1}^{n_t} k(y_i, y_j) - \frac{2}{n_s n_t} \sum_{i=1}^{n_s} \sum_{j=1}^{n_t} k(x_i, y_j)
\]

where \( k \) represents the RBF kernel and \( n_s, n_t \) represent sample size in the source and target domains. For visual representations, we use pretrained ResNet-101 [25] to extract image embeddings \( \{v_i, v_j\} \) for 10,000 randomly sampled images in each pair of datasets \( \{D^S, D^T\} \). We use the final 2048-D embedding as \textit{high-level semantic features}, and the spatially average-pooled embedding after conv3_4 layer (512-D) as \textit{low-level features}. For questions, we measure both semantic and syntactic gaps using two different representations. For the semantic representation, we choose pre-trained BERT [18] to encode 10,000 randomly sampled questions \( \{q_i, q_j\} \) from pairwise datasets \( \{D^S, D^T\} \). For syntactic features, we follow the approach in [19] to extract 20 low-level features: question length, number of conjunctions, pronouns, prepositions, etc. We show the results in Tables 1 and 2.
3.2. Constructing synthetic shifts to isolate effects

As we can see in Tables 1 and 2, many dataset pairs differ in both their image and question distributions. Our goal is to understand precisely how different VQA methods respond to shifts in each distribution, but this is not straightforward because both modalities would affect the VQA performance. Therefore, to disentangle domain gaps arising from the image or question modality, we synthetically construct gaps in either image or question space. To do this, we use image style transfer and question paraphrasing.

Specifically, we create stylized variants of each image in $\mathcal{D}^S$. Let $F(v, f)$ be a style transfer function which takes in a content image $v$ and style image $f$ and outputs the content image now with a new style, $v^f$. We choose Ada-IN [28] as our style transfer function $F$. We also pay extra attention to ensure colors are preserved in the style transfer process, which is important to ensure answers to color-related questions remain valid. We achieve the color preservation by converting style-transferred images into the YUV color space, and copying the UV channels from the original images. We also experimented with the color histogram matching in [18], but ultimately chose luminance-only transfer. We also control the transfer strength $\alpha$ in [28] to avoid losing too much information. We manually verified color and answers were preserved on a small set of images.

For questions, let $G$ be a paraphrasing function, $G(q, g) = q^g$, where $q$ is a question and $g$ is a reference “style”. We finetuned a massively pretrained sequence-to-sequence generative T5 model [50] on Quora duplicate questions\(^1\), to shift the question $q$ to a different style.

**Synthetic dataset pairs:** We apply the image style transfer and question paraphrasing separately, to construct new pairs of VQA datasets that only have domain shift in one modality. For example, by experimenting on $\mathcal{D}^S = \{v, q, a\}$ and $\mathcal{D}^T = \{v^f, q\}$, the results would reveal the model’s robustness on image domain shift. If we choose $\mathcal{D}^T = \{v, v^G\}$, then similar experiments would show the impacts from question domain shift. Note that in both settings, the answers are kept unchanged thus the impacts from answer space shift will be eliminated. We do not use the answers on the target domain to train, even though they are identical to those in the source domain.

3.3. Bridging domain gaps

Our goal is to ensure high accuracy on $\mathcal{D}^T$, even though we have no ground-truth answers in the target domain as supervision. Thus, we minimize a loss of this type:

$$L(D^S, D^T; \theta) = L_{ce}(D^S; \theta) + \lambda L_{fd}(D^T, D^S; \bar{\theta})$$  \(2\)

In the above, $\bar{\theta}$ refers to the parameters of a VQA model, computed on the source dataset only, and $L_{fd}$ is a loss that computes the discrepancy between the feature distributions of the source and target domains, computed over images and/or questions. The bar in $\bar{\theta}$ refers to the model component over which we apply $L_{fd}$ (see Sec. 3.4).

For $L_{fd}$, we consider two domain adaptation strategies from object recognition, and a new variant of one of them. First, we adapt a discriminative domain classifier as described in DANN [17], and reverse its gradient. The idea is to learn features that prevent the model $\theta$ from being able to successfully distinguish between source and target domains. To successfully adapt DANN, we have to consider the differences between DA for object recognition and DA for VQA. In particular, DANN can be applied over both image and question inputs (or over intermediate representations that depend on both). We describe how we adapt DANN for each VQA method, in Sec. 3.4. Second, we use a simplified single-source version of Moment Matching [47] which minimizes moment-related distances to reduce domain gaps.

We treat answering as 1000-way open-ended classification, and ensure the output space is the same for all datasets; we provide details in Sec. 4. Alternatives include answering-as-generation (which is challenging for automatic evaluation) or as a multiple-choice task (which may introduce biases due to the choice of the incorrect answers [10]).

3.4. Adaptation for VQA models

**VQA models:** We analyze domain robustness of VQA models from different families: (1) Classic two-stream methods (RelNet [55]); (2) Neuro-symbolic methods (NSCL [41]); and (3) Transformer methods (LXMERT [58]). We also test MAC [29] and TbD [42], which are hybrids of classic and neuro-symbolic methods.

**Challenges:** Applying domain adaptation is challenging in the unsupervised open-ended classification setting. The first challenge is the lack of labels on the target dataset, in the setting we assume. To the best of our knowledge, only two prior works [10, 64] tried to tackle the domain adaptation problem for VQA. However, one leveraged multiple-choice options [10], and both leveraged labels in the target domains, which are not available in our setting. More specifically, Chao et al. [10] minimize Jensen-Shannon Divergence (JSD) to achieve domain adaptation in the multiple-choice VQA task. All datasets they investigated are derived from COCO so there is little visual domain shift, thus they only focused on dealing with question and answer/decoys shift. We noticed their improvements mostly come from minimizing JSD over answer/decoys (i.e. minimizing JSD over questions brings negligible $< 0.4\%$ performance boost). In addition, [10]’s feature transformation method (impoverished VQA model without image inputs) requires labels from the target dataset. However, this is not applicable under the open-ended setting because we assume

\(^1\)https://www.kaggle.com/c/quora-question-pairs

7049
How many people are standing?

Figure 2. Illustration of the domain adaption strategies as described in Section 3.4. We show both training and inference stages for the baseline where no domain adaptation is applied (top left), and the training procedure for one-stage domain adaption with DANN or Moment Matching (top right). In the bottom, we show the training procedure of our proposed two-stage DANN approach. Specifically, we first train a domain-adaptive visual feature extractor in the first stage, with a MSE loss to encourage preserving semantics, and a domain confusion loss (DANN) to reduce domain gaps. Next, using extracted features from the domain-invariant extractor, we train a VQA model on source data. The gradient reversal layer (GR) \[17\] is only used with DANN. Dashed lines indicate no gradients due to module being frozen or for inference only.

A second challenge is that joint optimization of VQA with a domain adaptation objective (Eq. 2) is unstable because the VQA loss and DA loss may compete, making optimization difficult. This is especially true for complex, state-of-the-art VQA models. To cope with the challenge of applying domain adaptation over VQA, \[10\] break up adaptation and VQA training into two stages; they primarily use a simple MLP, while we evaluate DA with recent VQA models. \[10\] empirically use a GAN-like approach to estimate JSD, which makes their training computationally intensive and hard to adapt to more complicated VQA models. \[64\] also reports similar challenges in training a complex multitask (VQA+DA) method, and they handle it by carefully tuning the scalars for their multitask loss. Notably, they make the scalars corresponding to the unsupervised feature alignment very small (e.g., 0.003, 0.025), and the multiplier for the source classifier is also small (0.001 vs 1 for the supervised target loss). This highlights the challenge of leveraging transfer from the source domain without target labels.

**Baseline and one-stage approaches:** We report the performance of two reference models: (1) the accuracy on the source dataset, which indicates model capacity, and (2) the accuracy on the target dataset assuming target labels are fully available, which serves as an empirical upper bound for domain adaptation. The simplest baseline is directly applying a model trained on a source dataset, on test data from the target domain, without any domain adaptation. The training and inference procedure is illustrated in Fig. 2. As another baseline, we also investigated an end-to-end pipeline to combine the DANN training with VQA training, shown as “One-stage DA”. Specifically, we added the domain discrimination loss and reversed its gradients to update the visual representations. However, it is non-trivial to find the best place for applying domain discrimination for different VQA methods. For example, for MAC we added a linear classifier to distinguish the domains and applied the DANN loss on the visual embedding before feeding them into the MAC unit. In addition to DANN, we experimented with moment matching \[47\] where the first- and second-order moments are enforced to align across domains. In this case the gradient reversal layer is no longer needed.

**Proposed two-stage DA approach:** To better cope with the challenges, we also propose a two-stage approach to build a domain-invariant feature extractor and VQA module sequentially. A figurative illustration of the process is shown in Fig. 2 (bottom). The motivation for breaking up domain adaptation and VQA modeling is to stabilize the training for greater robustness. The idea is partially inspired by neurosymbolic methods, which separate perception (in this case, feature extraction) and reasoning (the VQA model after feature extraction). Our two-stage strategy is summarized as:
1. Extract features for images in the source dataset, as defined in the VQA method (e.g. use pre-trained ResNet).
2. Train a domain-invariant feature extractor with both source and target datasets (without labels), using (a) an MSE loss which encourages the extracted features on source dataset to preserve semantics, and (b) a BCE loss with gradient reversal layer to prevent distinguishing the source and target domains.
3. Apply the backbone from step 2 to extract visual features and train a VQA model on the source dataset.
4. Take the visual feature extractor from step 2 and VQA model from step 3, then feed in the target dataset and evaluate the performance.

**VQA method specifics:** Each VQA method extracts features in a particular way, resulting in small variances in our two-stage DA implementation. For MAC and TbD, feature extraction is executed with ResNet-101 prior to training the VQA model, following the methodology outlined previously. NSCL uses ResNet-34 to extract features from different regions in the image (region proposals via a pre-trained Mask R-CNN [24]), and allows for NSCL to fine-tune ResNet-34 during training. To most closely follow our two-stage methodology, we replace the pretrained ResNet-34 with a frozen ResNet-34 backbone trained in step 2. ResNet uses 4 convolutional layers to extract features from the images. We used a pre-trained set of these convolutional layers to export the source features for VQA and DA. For LXMERT, the initial visual features are from pre-trained Faster R-CNN and processed by vision-only transformer layers. We kept the Faster R-CNN backbone untouched and fine-tuned the transformer layers to be domain-invariant.

### 4. Experimental Validation

We show four groups of results: shifts in visual and question space for nine datasets (Sec. 4.1), robustness of five methods to synthetic shifts in visual or textual space using the CLEVR dataset (Sec. 4.2), different ways to apply unsupervised domain adaptation using MAC on three datasets (Sec. 4.3), and finally robustness of two methods using eight real dataset pairs (Sec. 4.4).

#### 4.1. Domain shifts in nine datasets

Tables 1 and 2 show how the questions and images in nine datasets differ. Each table is a composition of two triangles. In Table 1, the lower triangle contains Maximum Mean Discrepancy (MMD) statistics using BERT embeddings, while the upper triangle shows MMD statistics using syntax features (Sec. 3.1). MMD computes how different two distributions are, with higher values indicating larger difference. The shading ranges from white to red/blue, with darker, more vivid colors indicating larger values.

In the lower triangle of Table 1, we observe that Visual 7W and Visual Genome (VG) are similar, and VQA v1 and v2 are similar, as expected. GQA is similar to VQA v1/v2 in terms of semantics (captured through BERT), but it is different in terms of syntax. VQA Abstract is much more similar to VQA v1/v2 in terms of syntax than to other datasets (blue triangle), but in terms of semantic content (red triangle), it is also fairly similar to Visual 7W and VG. COCO QA and CLEVR stand out from other datasets both in terms of semantics and syntax (both rows/columns for COCO QA and CLEVR have high values except on diag-

<table>
<thead>
<tr>
<th>Visual 7W</th>
<th>VG</th>
<th>VQA v1</th>
<th>VQA v2</th>
<th>COCO QA</th>
<th>CLEVR</th>
<th>VQA Abs.</th>
<th>GQA Bal.</th>
<th>VizWiz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visual 7W</td>
<td>–</td>
<td>0.04</td>
<td>0.18</td>
<td>0.18</td>
<td>0.56</td>
<td>0.85</td>
<td>0.18</td>
<td>0.46</td>
</tr>
<tr>
<td>VG</td>
<td>0.01</td>
<td>–</td>
<td>0.16</td>
<td>0.16</td>
<td>0.54</td>
<td>0.87</td>
<td>0.16</td>
<td>0.44</td>
</tr>
<tr>
<td>VQA v1</td>
<td>0.06</td>
<td>0.07</td>
<td>–</td>
<td>0.00</td>
<td>0.44</td>
<td>0.81</td>
<td>0.03</td>
<td>0.34</td>
</tr>
<tr>
<td>VQA v2</td>
<td>0.06</td>
<td>0.07</td>
<td>0.00</td>
<td>–</td>
<td>0.44</td>
<td>0.81</td>
<td>0.03</td>
<td>0.35</td>
</tr>
<tr>
<td>COCO QA</td>
<td>0.20</td>
<td>0.20</td>
<td>0.15</td>
<td>0.15</td>
<td>–</td>
<td>0.69</td>
<td>0.44</td>
<td>0.26</td>
</tr>
<tr>
<td>CLEVR</td>
<td>0.22</td>
<td>0.22</td>
<td>0.17</td>
<td>0.17</td>
<td>0.19</td>
<td>–</td>
<td>0.81</td>
<td>0.58</td>
</tr>
<tr>
<td>VQA Abs.</td>
<td>0.06</td>
<td>0.06</td>
<td>0.02</td>
<td>0.02</td>
<td>0.15</td>
<td>0.19</td>
<td>–</td>
<td>0.34</td>
</tr>
<tr>
<td>GQA Bal.</td>
<td>0.10</td>
<td>0.11</td>
<td>0.06</td>
<td>0.06</td>
<td>0.15</td>
<td>0.13</td>
<td>0.07</td>
<td>–</td>
</tr>
<tr>
<td>VizWiz</td>
<td>0.06</td>
<td>0.06</td>
<td>0.10</td>
<td>0.10</td>
<td>0.23</td>
<td>0.22</td>
<td>0.10</td>
<td>0.12</td>
</tr>
</tbody>
</table>

Table 1. Domain gaps in question space; red shading is MMD over 768-D BERT embeddings, blue is MMD over 20-D syntax statistics.

<table>
<thead>
<tr>
<th>Visual 7W</th>
<th>VG</th>
<th>VQA v1</th>
<th>VQA v2</th>
<th>COCO QA</th>
<th>CLEVR</th>
<th>VQA Abs.</th>
<th>GQA Bal.</th>
<th>VizWiz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visual 7W</td>
<td>–</td>
<td>0.00</td>
<td>0.01</td>
<td>0.01</td>
<td>0.01</td>
<td>0.10</td>
<td>0.08</td>
<td>0.00</td>
</tr>
<tr>
<td>VG</td>
<td>0.01</td>
<td>–</td>
<td>0.00</td>
<td>0.01</td>
<td>0.01</td>
<td>0.10</td>
<td>0.08</td>
<td>0.00</td>
</tr>
<tr>
<td>VQA v1</td>
<td>0.02</td>
<td>0.02</td>
<td>–</td>
<td>0.00</td>
<td>0.00</td>
<td>0.10</td>
<td>0.08</td>
<td>0.01</td>
</tr>
<tr>
<td>VQA v2</td>
<td>0.03</td>
<td>0.02</td>
<td>0.01</td>
<td>–</td>
<td>0.00</td>
<td>0.10</td>
<td>0.08</td>
<td>0.01</td>
</tr>
<tr>
<td>COCO QA</td>
<td>0.04</td>
<td>0.04</td>
<td>0.03</td>
<td>0.03</td>
<td>–</td>
<td>0.10</td>
<td>0.08</td>
<td>0.01</td>
</tr>
<tr>
<td>CLEVR</td>
<td>0.54</td>
<td>0.54</td>
<td>0.54</td>
<td>0.54</td>
<td>0.54</td>
<td>–</td>
<td>0.10</td>
<td>0.10</td>
</tr>
<tr>
<td>VQA Abs.</td>
<td>0.36</td>
<td>0.36</td>
<td>0.36</td>
<td>0.36</td>
<td>0.36</td>
<td>0.59</td>
<td>–</td>
<td>0.08</td>
</tr>
<tr>
<td>GQA Bal.</td>
<td>0.03</td>
<td>0.03</td>
<td>0.03</td>
<td>0.03</td>
<td>0.04</td>
<td>0.54</td>
<td>0.36</td>
<td>–</td>
</tr>
<tr>
<td>VizWiz</td>
<td>0.22</td>
<td>0.22</td>
<td>0.21</td>
<td>0.21</td>
<td>0.21</td>
<td>0.52</td>
<td>0.42</td>
<td>0.22</td>
</tr>
</tbody>
</table>

Table 2. Domain gaps in image space; red shading is MMD over ResNet-101 2048-D features, blue is MMD over conv3_4 512-D features.
demonstrates each method’s change in performance when evaluated with paraphrased questions (first column), style-transferred images using two separate styles, I1 and I2 (second and fourth columns), and combined question and image shifts (third and fifth columns). LXMER-T is most robust to question shifts, likely due to its extensive pre-training on language data, followed by TbD. Neuro-symbolic or hybrid methods (NSCL or TbD) are most robust to image shifts, consistent with our hypothesis.

### 4.3. Domain adaptation for synthetic shifts

In Table 5, we evaluate different domain adaptation strategies with MAC as the backbone model on VQA v2, CLEVR, and GQA Balanced, where artificial domain shifts are created in the image space. By comparing Source and Target (full) accuracy, we deduce the image style transfer preserves the information required for VQA as accuracy only drops slightly. However, in all datasets, we see quite significant performance drop if a trained model is directly applied to the corresponding target dataset. The domain adaptation strategies (1-stage DANN [17] and Moment Matching [47], and our 2-stage DANN) help to different degree. Our proposed 2-stage DANN is always significantly better than then 1-stage DANN, and better than the 1-stage MM on two of three datasets. Note that differences between methods are significant in that the range between Target (direct) and Target (full) is very small for two of the three datasets. It is worth mentioning that training the 1-stage DANN baseline is highly unstable as the optimization is more difficult. We repeated the experiments multiple times, but the best result and those within 1% of the best are bolded.

### Tables

#### Table 3. Method robustness on CLEVR, using style transfer of the original images (domain shift in image space).

<table>
<thead>
<tr>
<th>Method / Type</th>
<th>Source Acc.</th>
<th>Target Acc. (direct)</th>
<th>Target Acc. (2-stage DANN)</th>
<th>Target Acc. (10% scratch)</th>
<th>Target Acc. (10% finetune)</th>
<th>Target Acc. (full)</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSCL (NS)</td>
<td>98.0</td>
<td>59.7</td>
<td>68.6</td>
<td>60.0</td>
<td>75.8</td>
<td>95.9</td>
</tr>
<tr>
<td>MAC (NS/CL)</td>
<td>93.4</td>
<td>62.6</td>
<td>65.2</td>
<td>84.6</td>
<td>82.1</td>
<td>88.6</td>
</tr>
<tr>
<td>TbD (NS/CL)</td>
<td>99.1</td>
<td>36.3</td>
<td>41.3</td>
<td>72.5</td>
<td>84.2</td>
<td>95.3</td>
</tr>
<tr>
<td>RelNet (CL)</td>
<td>93.7</td>
<td>44.8</td>
<td>47.2</td>
<td>61.5</td>
<td>77.1</td>
<td>91.4</td>
</tr>
<tr>
<td>LXMER-T (TR)</td>
<td>94.8</td>
<td>58.0</td>
<td>–</td>
<td>60.9</td>
<td>65.9</td>
<td>91.3</td>
</tr>
</tbody>
</table>

#### Table 4. Method robustness on CLEVR, under artificial Question shifts, followed by Image shifts with two styles (resulting in I1 and I2), and two settings where both Image and Question shifts are applied (I+Q). – means we were unable to test on NSCL since their semantic parser is not open-sourced. We bold the best result and those within 1% of the best.

<table>
<thead>
<tr>
<th>Method / Type</th>
<th>Q</th>
<th>I1</th>
<th>I1+Q</th>
<th>I2</th>
<th>I2+Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSCL (NS)</td>
<td>–</td>
<td>71.0</td>
<td>–</td>
<td>60.6</td>
<td>–</td>
</tr>
<tr>
<td>MAC (NS/CL)</td>
<td>52.2</td>
<td>45.9</td>
<td>28.1</td>
<td>60.9</td>
<td>37.9</td>
</tr>
<tr>
<td>TbD (NS/CL)</td>
<td>52.9</td>
<td>55.7</td>
<td><strong>36.1</strong></td>
<td><strong>70.4</strong></td>
<td><strong>42.6</strong></td>
</tr>
<tr>
<td>RelNet (CL)</td>
<td>49.6</td>
<td>20.5</td>
<td>19.1</td>
<td>46.2</td>
<td>31.6</td>
</tr>
<tr>
<td>LXMER-T (TR)</td>
<td><strong>53.4</strong></td>
<td>50.6</td>
<td><strong>36.6</strong></td>
<td>58.0</td>
<td>40.5</td>
</tr>
</tbody>
</table>

#### Table 5. Different DA methods on MAC (NS/CL), image shift.

<table>
<thead>
<tr>
<th>Method</th>
<th>Source Accuracy</th>
<th>VQA v2</th>
<th>CLEVR</th>
<th>GQA Bal.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target (direct)</td>
<td>41.0</td>
<td>45.9</td>
<td>37.3</td>
<td></td>
</tr>
<tr>
<td>Target (1-stage DANN)</td>
<td>42.2</td>
<td>45.7</td>
<td>37.4</td>
<td></td>
</tr>
<tr>
<td>Target (1-stage MM)</td>
<td>42.6</td>
<td>46.6</td>
<td><strong>38.6</strong></td>
<td></td>
</tr>
<tr>
<td>Target (2-stage DANN)</td>
<td>42.8</td>
<td>46.7</td>
<td>38.5</td>
<td></td>
</tr>
<tr>
<td>Target (full)</td>
<td>49.1</td>
<td>90.0</td>
<td>42.1</td>
<td></td>
</tr>
</tbody>
</table>

Methods’ robustness to synthetic domain shifts

Tables 3 and 4 show how robust different VQA methods are to synthetic shifts on the CLEVR dataset. In Table 3, we show robustness to visual shifts. We evaluate performance by the method on the original CLEVR dataset, performance of the model trained on CLEVR and applied in the shifted setting (e.g. style-transferred images) directly, target performance with unsupervised domain adaptation (specifically, 2-stage DANN), and three supervised settings for comparison – two that use 10% of the target training data, and one that uses 100% of the target training data. We use the default recommended hyperparameters without exhaustive search. We observe all methods’ performance drops in the Target setting compared to Source, as expected. However, in Target (direct) and Target (2-stage DANN), both of which do not use labels on the target, NSCL and MAC (both neuro-symbolic or NS hybrid) retain the best performance. Using a small amount of target data for fine-tuning, MAC and TbD (both NS hybrids) perform best.

Table 4 demonstrates each method’s change in performance when evaluated with paraphrased questions (first column), style-transferred images using two separate styles, I1 and I2 (second and fourth columns), and combined question and image shifts (third and fifth columns). LXMER-T is most robust to question shifts, likely due to its extensive pre-training on language data, followed by TbD. Neuro-symbolic or hybrid methods (NSCL or TbD) are most robust to image shifts, consistent with our hypothesis.
Table 6. Robustness across VQA datasets; best viewed in color.

<table>
<thead>
<tr>
<th>Datasets</th>
<th>MAC</th>
<th>LXMERT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A</strong></td>
<td><strong>B</strong></td>
<td><strong>A → B</strong></td>
</tr>
<tr>
<td>VQA v2</td>
<td>CLEVR</td>
<td>53.3</td>
</tr>
<tr>
<td>GQA Bal.</td>
<td>44.4</td>
<td>32.0</td>
</tr>
<tr>
<td>VQA Abs.</td>
<td>48.3</td>
<td>33.6</td>
</tr>
<tr>
<td>VG</td>
<td>33.3</td>
<td>26.2</td>
</tr>
<tr>
<td>VQA v2</td>
<td>CLEVR</td>
<td>67.6</td>
</tr>
<tr>
<td>GQA Bal.</td>
<td>58.2</td>
<td>50.5</td>
</tr>
<tr>
<td>VQA Abs.</td>
<td>56.3</td>
<td>34.3</td>
</tr>
<tr>
<td>VG</td>
<td>41.0</td>
<td>36.7</td>
</tr>
</tbody>
</table>

Table 7. Summary of shifts, VQA-v2 ↔ selected datasets.

<table>
<thead>
<tr>
<th>Datasets</th>
<th>Image</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appearance</td>
<td>Semantic</td>
<td>Syntactic</td>
</tr>
<tr>
<td>CLEVR</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>GQA Bal.</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>VQA Abs.</td>
<td>Med. High</td>
<td>Med. High</td>
</tr>
<tr>
<td>VG</td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>

4.4. Generalization under real domain shifts

Table 6 shows the robustness of two recent VQA methods among five datasets: VQA v2, CLEVR, GQA Balanced, VQA Abstract and Visual Genome. These datasets have different answer spaces, as shown in Fig. 3. Since the final classification layer is coupled with the answer vocabulary, models trained on one dataset cannot be directly applied to another. To mitigate this issue, we obtain a shared 1000-class answer space by computing the 1000 most common answers across all five selected datasets. We report training and evaluating a model on the same dataset (i.e., Acc of A and B), and training on one and evaluating on the other (e.g., Acc of A → B denotes training on A and evaluating on B). The accuracy is calculated on the validation split for individual datasets (except for GQA where we use testdev split as recommended), and is obtained by matching the top-1 prediction with the ground-truth answer(s).

Since source/target datasets have different upper bounds (i.e., B Acc), we normalize the transferred accuracy by dividing by B, and illustrate the relative normalized performance using the intensity of shading: darker background of a cell indicates higher ratio of the transferred accuracy and the source/target accuracy. Blue backgrounds measure how well a transferred model A → B performs compared to its upper bound, as they are all transferring from the same source A, while red backgrounds measure how well different source models B → A transfer to the same target A.

By comparing the accuracy on the training and evaluation datasets, we see that in most cases LXMERT (TR) generalizes better across datasets than MAC (NS/CL). We hypothesize that transformer-based methods like LXMERT benefit from their massive pre-training (which includes disjoint GQA and VQA v2 data). We also observe that GQA and Visual Genome are more useful sources when transferring knowledge to VQA v2, compared to CLEVR. This observation is consistent with our statistical analysis in Tables 1 and 2, and for simplicity we extracted relevant information in Table 7. We see that GQA Balanced and Visual Genome are similar to VQA v2 in multiple aspects. We also note that GQA Balanced has smaller semantic shifts than syntactic shifts with respect to VQA v2, while VG has smaller syntactic than semantic shifts with VQA v2. This makes GQA Balanced more helpful as a source dataset (darker shading for GQA→VQA-v2 than for VG→VQA-v2 in Table 6, for both MAC and LXMERT). Finally, the only case MAC is more robust than LXMERT (in terms of shading) is VQA-v2↔VQA-Abstract, which is the dataset with largest visual shifts after CLEVR. One possibility is that LXMERT is better suited to deal with question shifts and MAC with visual shifts, because of its neuro-symbolic nature and dedicated perception module.

5. Conclusion

We showed domain differences between VQA datasets can come from the visual and linguistic space; different methods are more susceptible to visual or linguistic shifts, and high-level semantic shifts make methods more fragile than syntactic ones. We found neuro-symbolic methods are more robust to synthetic visual-only domain shifts and some real dataset shifts, but transformer methods handle real linguistic and some visual shifts better due to pretraining. We demonstrated that while unsupervised domain adaptation in VQA is challenging, better gains can be made through a two-stage DANN which shares similar intuition as neuro-symbolic methods. In the future, we will explicitly handle shifts in answer space, and develop DA techniques that can flexibly choose how much to adapt over each modality.

Acknowledgements: This material is based upon work supported by the National Science Foundation under Grant No. 1718262. It was also supported by the Univ. of Pittsburgh Momentum Fund, and Google/Amazon/Adobe gifts. We thank the reviewers and AC for their suggestions.
References


ings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016.


