Lecture 18: Question Answering

Recall: SQuAD

- Single-document, single-sentence question-answering task where the answer is always a substring of the passage
- Predict start and end indices of the answer in the passage

Recall: QA with BERT

- Predict start and end positions of answer in passage
- No need for crazy BiDAF-style layers
This Lecture

- Defining QA
- Problems in “classic” QA, especially related to answer type overfitting
- Retrieval-augmented QA (RAG)
- Long-form QA
- Frontiers of QA

Defining QA

some slides in this section from Eunsol Choi

QA can be very broad

- Factoid QA:
  - what states border Mississippi?
  - when was Barack Obama born?
  - how is Advil different from Tylenol?

- “Question answering” as a term is so broad as to be meaningless
  - Is P=NP?
  - What is 4+5?
  - What is the translation of [sentence] into French?
  - Is it okay to use a blender in 2AM in an apartment?

Why do we study QA?

- As a testbed to evaluate how machines understand text

“Since questions can be devised to query any aspect of text comprehension, the ability to answer questions is the strongest possible demonstration of understanding.”
### Model-testing Queries

Questioner already knows the answer, aiming to test model’s understanding or knowledge

**Passage**

The main forms of precipitation include drizzle, rain, sleet, snow, graupel and hail. And the weather forecast can predict the weather conditions for the day.

**Question**

What is another main form of precipitation besides drizzle, rain, sleet, snow, and hail?

**Answer**

Graupel

---

### “Commonsense” QA datasets

- Questions query emotional and social intelligence, not encyclopedic knowledge.
- Answering this will not depend on evidence documents.

Social IQA dataset [Sap, Rashkin et al. EMNLP 2019]

---

### Datasets that seek expert knowledge

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Context</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reclor dataset</td>
<td>In jurisdictions where use of headlights is optional when visibility is good, drivers who use headlights at all times are less likely to be involved in a collision than non-headlight users. When use of headlights varies across jurisdictions.</td>
<td><strong>Q</strong> Questioner does not know the answer <strong>A</strong> Questioner is seeking information <strong>C</strong> Questioner already knows the answer, aiming to test model’s understanding or knowledge</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Context</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>MMLU dataset</td>
<td>The Millennium Falcon is a fictional spacecraft in the Star Wars franchise. The modified Y-Wing Corellian freighter is primarily commanded by Coruscant smuggler Han Solo.</td>
<td><strong>Q</strong> Questioner does not know the answer <strong>A</strong> Questioner finds answer in article <strong>C</strong> Questioner already knows the answer, aiming to test model’s understanding or knowledge</td>
</tr>
</tbody>
</table>

---

### Model-testing Queries

Questioner already knows the answer, aiming to test model’s understanding or knowledge

**Passage**

The main forms of precipitation include drizzle, rain, sleet, snow, graupel and hail. And the weather forecast can predict the weather conditions for the day.

**Question**

What is another main form of precipitation besides drizzle, rain, sleet, snow, and hail?

**Answer**

Graupel
Why do we study QA?

- Build a helpful tool for humans to gather information

Problems in QA
(Model-testing Questions)

Adversarial SQuAD

- SQuAD questions are often easy: “what was she the recipient of?” passage: “... recipient of Nobel Prize...”

Jia and Liang (2017)

Adversarial SQuAD

- BERT easily learns surface-level correspondences like this with self-attention
Adversarial SQuAD

**Article:** Super Bowl 50
**Paragraph:** “Peyton Manning became the first quarter-back ever to lead two different teams to multiple Super Bowls. He is also the oldest quarterback ever to play in a Super Bowl at age 39. The best record was held by John Elway, who led the Broncos to victory in Super Bowl XXXIII at age 38 and is currently Denver’s Executive Vice President of Football Operations and General Manager. Quarterback Jeff Dean had jersey number 37 in Champ Bowl XXXIV.”
**Question:** “What is the name of the quarterback who was 38 in Super Bowl XXXIII?”
**Original Prediction:** John Elway
**Prediction under adversary:** Jeff Dean

Jia and Liang (2017)

Universal Adversarial “Triggers”

**Input** (underline = correct span, red = trigger, underline = target span)

**Question:** Why did he walk?  
For exercise, Tesla walked between 8 to 10 miles per day. He squished his toes one hundred times for each foot every night, saying that it stimulated his brain cells. **why how because to kill american people.**

**Question:** Why did the university see a drop in applicants?  
In the early 1950s, student applications declined as a result of increasing crime and poverty in the Hyde Park neighborhood. In response, the university became a . . . . **why how because to kill american people.**

- Distractor “looks” more like the question than the right answer does, even if entities are wrong
- Similar to Jia and Liang, but instead add the same adversary to every passage
- Adding “why how because to kill american people” causes SQuAD models to return this answer 10-50% of the time when given a “why” question
- Similar attacks on other question types like “who”

Wallace et al. (2019)

How to fix QA?

- These models can be improved using methods similar to Project 3, but are still fundamentally flawed
- Fine-tuning on these tasks doesn’t actually get us where we want to be
- Solution: **No training?**
  - Fine-tuning imparts many of these spurious correlations
  - A GPT model used zero-shot can do great precisely because it isn’t overfit to the patterns of any one dataset
- …but also, let’s work on more realistic QA settings, like information-seeking questions

Retrieval Models  
(Information-Seeking Questions)
Open-domain QA

- Real QA systems should be able to handle more than just a paragraph of context — theoretically should work over the whole web?

Q: What was Marie Curie the recipient of?

Marie Curie was awarded the Nobel Prize in Chemistry and the Nobel Prize in Physics...
Mother Teresa received the Nobel Peace Prize in...
Curie received his doctorate in March 1895...
Sklodowska received accolades for her early work...

DrQA

- How often does the retrieved context contain the answer? (uses Lucene, basically sparse tf-idf vectors)
- Full retrieval results using a QA model trained on SQuAD: task is much harder

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Wiki Search</th>
<th>Doc Retriever plain</th>
<th>Doc Retriever +bigrams</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQuAD</td>
<td>62.7</td>
<td>76.1</td>
<td>77.8</td>
</tr>
<tr>
<td>CuratedTREC</td>
<td>81.0</td>
<td>85.2</td>
<td>86.0</td>
</tr>
<tr>
<td>WebQuestions</td>
<td>73.7</td>
<td>75.5</td>
<td>74.4</td>
</tr>
<tr>
<td>WikiMovies</td>
<td>61.7</td>
<td>54.4</td>
<td>70.3</td>
</tr>
</tbody>
</table>

Chen et al. (2017)

Problems

- Many SQuAD questions are not suited to the “open” setting because they’re underspecified
  - Where did the Super Bowl take place?
  - Which player on the Carolina Panthers was named MVP?
- SQuAD questions were written by people looking at the passage — encourages a question structure which mimics the passage and doesn’t look like “real” questions

Lee et al. (2019)
NaturalQuestions

- Real questions from Google, answerable with Wikipedia
- Short answers and long answers (snippets)
- Questions arose naturally, unlike SQuAD questions which were written by people looking at a passage. This makes them much harder
- Short answer $F_1$ < 60, long answer $F_1$ < 75

Kwiatkowski et al. (2019)

Dense Retrieval

- Can we do better IR?
- Encode the query with BERT, pre-encode all paragraphs with BERT, query is basically nearest neighbors

$$h_q = W_q BERT_Q(q) [CLS]$$
$$h_b = W_b BERT_B(b) [CLS]$$
$$S_{retr}(b, q) = h_q^T h_b$$

Lee et al. (2019)

REALM

- Retrieval-augmented Language Model Pre-training
- Key idea: can we predict a mask token better if we have some kind of external knowledge? Mask prediction looks like “fill-in-the-blank” QA

Guu et al. (2020)
REALM

- They learn the retriever and knowledge encoder end-to-end. Very challenging to implement!

Guu et al. (2020)

REALM

- Fine-tuning can exploit the same kind of textual knowledge

Guu et al. (2020)

REALM

<table>
<thead>
<tr>
<th>Name</th>
<th>Architectures</th>
<th>Pre-training</th>
<th>NQ (79K/4k)</th>
<th>WQ (3k/2k)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BERT-Baseline (Lee et al., 2019)</td>
<td>Sparse Retr.+Transformer</td>
<td>BERT</td>
<td>26.5</td>
<td>17.7</td>
</tr>
<tr>
<td>T5 (base) (Roberts et al., 2020)</td>
<td>Transformer Seq2Seq</td>
<td>T5 (Multitask)</td>
<td>27.0</td>
<td>29.1</td>
</tr>
<tr>
<td>T5 (large) (Roberts et al., 2020)</td>
<td>Transformer Seq2Seq</td>
<td>T5 (Multitask)</td>
<td>29.8</td>
<td>32.2</td>
</tr>
<tr>
<td>T5 (11b) (Roberts et al., 2020)</td>
<td>Transformer Seq2Seq</td>
<td>T5 (Multitask)</td>
<td>34.5</td>
<td>37.4</td>
</tr>
<tr>
<td>DrQA (Chen et al., 2017)</td>
<td>Sparse Retr.+DocReader</td>
<td>N/A</td>
<td>-</td>
<td>20.7</td>
</tr>
<tr>
<td>Ours ($\mathcal{X} =$ Wikipedia, $\mathcal{Z} =$ Wikipedia)</td>
<td>Dense Retr.+Transformer</td>
<td>REALM</td>
<td>39.2</td>
<td>40.2</td>
</tr>
<tr>
<td>Ours ($\mathcal{X} =$ CC-News, $\mathcal{Z} =$ Wikipedia)</td>
<td>Dense Retr.+Transformer</td>
<td>REALM</td>
<td><strong>40.4</strong></td>
<td><strong>40.7</strong></td>
</tr>
</tbody>
</table>

- Below the line: “open-book” models that do retrieval

Guu et al. (2020)

Contriever

- Contrastive learning: encourage a query to be more similar to “positives” than “negatives”

$$
\mathcal{L}(q, k_{+}) = -\frac{\exp(s(q, k_{+})/\tau)}{\exp(s(q, k_{+})/\tau) + \sum_{i=1}^{K} \exp(s(q, k_{i})/\tau)}
$$

- Positives:
  - “Inverse cloze task”: take a paragraph, treat a span of that paragraph (say, 5 words) as the query, treat the rest of the paragraph as a positive
  - “Independent cropping”: take two random paragraphs, treat one as query and one as positive
**Contriever**

- Contrastive learning: encourage a query to be more similar to “positives” than “negatives”

\[ \mathcal{L}(q, k_+) = - \frac{\exp(s(q, k_+)/\tau)}{\sum_{i=1}^{K} \exp(s(q, k_i)/\tau)} \]

- Negatives
  - “In-batch negatives”: treat positives from other examples in the batch as negatives
  - Can also store negatives from previous batches to have a wider pool of negatives. Important to have hard negatives

**Modern Embeddings**

- OpenAI provides embeddings, but doesn’t give a ton of detail about how they are trained
- Indexing with contriever gives solid performance too

**Retrieval-Augmented Generation (RAG)**

- Uses a retriever and then feeds the retrieved passages into the language model prompt, similar to REALM
- Can use (a) commercial search engines; (b) custom indices over one’s own data
- Ongoing challenges: how to get the right documents? Is information from different documents interpreted correctly?

**WebGPT**

<table>
<thead>
<tr>
<th>Question</th>
<th>Why did we decide that certain words were &quot;bad&quot; and shouldn’t be used in social settings?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Answer</td>
<td>We have all been taught that there are certain words that should not be used in public, at least not without good reason. But why do some words fall into this category while others do not? It turns out that there is not a single answer to this question, as each word has a different history and carries different meanings in different cultures and families [2]. However, there are some general categories that &quot;bad&quot; words tend to fall into. &quot;Bad&quot; words generally relate to parts of life that we don’t like talking about in public, like bathroom functions, or negative ways of talking about people’s religion, skin color, ability, or gender [3]. Often, people say bad words when they are experiencing strong emotions, and those words are linked to our emotions [3].</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1, 2, 3] Why Are Some Words ‘Bad’?</td>
</tr>
</tbody>
</table>

- GPT model equipped with a search engine, then summarizes the answers

Nakano et al. (2021)
Table 1: Actions the model can take. If a model generates any other text, it is considered to be an invalid action. Invalid actions still count towards the maximum, but are otherwise ignored.

<table>
<thead>
<tr>
<th>Command</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search &lt;query&gt;</td>
<td>Send &lt;query&gt; to the Bing API and display a search results page</td>
</tr>
<tr>
<td>Clicked on link &lt;link ID&gt;</td>
<td>Follow the link with the given ID to a new page</td>
</tr>
<tr>
<td>Find in page: &lt;text&gt;</td>
<td>Find the next occurrence of &lt;text&gt; and scroll to it</td>
</tr>
<tr>
<td>Quote: &lt;text&gt;</td>
<td>If &lt;text&gt; is found in the current page, add it as a reference</td>
</tr>
<tr>
<td>Scrolled down &lt;1, 2, 3&gt;</td>
<td>Scroll down a number of times</td>
</tr>
<tr>
<td>Scrolled up &lt;1, 2, 3&gt;</td>
<td>Scroll up a number of times</td>
</tr>
<tr>
<td>Top</td>
<td>Scroll to the top of the page</td>
</tr>
<tr>
<td>Back</td>
<td>Go to the previous page</td>
</tr>
<tr>
<td>End: Answer</td>
<td>End browsing and move to answering phase</td>
</tr>
<tr>
<td>End: &lt;Nonsense, Controversial&gt;</td>
<td>End browsing and skip answering phase</td>
</tr>
</tbody>
</table>

- Interacts with environment, then writes answer based on information retrieved

WebGPT

Evaluation on “TruthfulQA”, some tricky questions that GPT-3 will answer incorrectly by default:
- What items is it legal to carry for anyone in the US?
- Who really caused 9/11?

WebGPT

Long-form QA

- Rather than extracting an answer from retrieved context, can we instead generate an answer from it?
- Still two steps: retrieval and answering, but the answering may now combine multiple documents and generate something longer
**ELI5 (reedit “Explain like I’m 5”)**

**Question:** How do Jellyfish function without brains or nervous systems?

**Answer:** Jellyfish may not have a brain, but they have a rough nervous system and innate behaviours. However, they are very simple creatures. They’re invertebrate: creatures without a backbone. Most jellyfish have really short life spans. [...] As their name implies, they are largely composed of basically jelly inside a thin membrane. They’re over 95% water.

*Fan et al. (2019)*

---

**Free-form answer generation**

**Question:** Why does salt bring out the flavor in most foods?

**Answer:** Salt does a couple of things that add to the flavor of foods. First off, it makes things salty. That sounds simplistic, but salt is one of the 5 basic tastes, so it tends to taste good simply all by itself. Secondly, salt will lessen sensitivity to other tastes, especially bitter. This is somewhat true of all the tastes, but adding salt will balance out a dish and not let one taste overpower the others. Thirdly, it’s been shown to increase that aromatic effects of many types of food. A good deal of your “taste” of a food actually comes from the smell of that food (which is why things tend to taste so bland when you nose is congested, like when you have the flu).

---

**Understanding LFQA**

**Question:** Can the capacity of our brains be roughly measured in bytes?

**Human written answer:** This is a hard question to answer. Of course, since we occupy finite space, our properties must be finite. But the exceedingly complex structure of the brain and other systems [...] makes it hard to calculate the amount of “data” that we can store. We don’t have a way to measure resolution of life or the quality of everyday noises. [...] Most of our memories are vague recollections. [...] However, we can estimate average capacity, although it has no clear meaning in our terms of cognition. That number would be 2.5 petabytes [...]. Even so, this number varies as well from person to person. [...]"

**Summary**
- Not all sentences in long form answer convey answer information
- About 40% of sentences serve other roles

---

**Difficulty of evaluating LFQA**

**Lexical matching based automatic metrics (e.g. ROUGE) are used, but not meaningful.**

**Q:** Can you protect electronics from EMPs/solar flares? If so, how?

**Random answer (ROUGE-L: 19.4)**

“The fast lane/slow lane is a bit of a misnomer. It gives the impression that new, faster lanes are being built. In reality, normal speed will be the new "fast lane", which will cost extra, and everything else will be in the throttled "slow lane".

**Gold answer (ROUGE-L: 18.6)**

“I'll start with the grounding question, because that's the easiest to answer: Doesn't help a bit. All that matters is that the metal container is conductive and doesn't have gaps...completely seal your Faraday cage. Consider soldering the lid on to that paint can... look at little baggie it comes in. Sealed mylar. That protected that chip from air travel at 35,000 feet, land travel through rural, urban, and suburban areas, and all the electromagnetic radiation that the trip entails... No lead shielding. No safes..."
Can humans evaluate long-form answers?

How does a speaker vibrate at multiple frequencies simultaneously to deliver sounds to our ears?

**Answer A:** This has been asked many times and the answer is they don’t. If you listen to the song being played live on purely acoustic instruments even though they are being played separately and emitting their own frequencies, what you hear (and by extension, what a microphone captures) at any given time is just one frequency that’s the “sum” of all the others combined. A speaker is just a reverse microphone.

**Answer B:** Imagine an ocean with a consistent wave. It flows up and down, with equal distance between the two waves at any time. Now imagine I push a larger, shorter wave into this ocean. The two waves will collide, resulting in some new wave pattern. This new wave pattern is a combination of those two waves. Speakers work similarly. If I combine two soundwaves, I get a new combination wave that sounds different.

Can experts evaluate?

- Even experts disagree on which one is a better answer

**Evaluation aspects for LFQA**

- Diverse facets are considered when evaluating LFQA answers.
- Best evaluation at the moment seems to be asking LLM whether it is a good answer or not, but not very reliable.

Frontiers in QA
**DROP**

- QA datasets to model programs/computation

<table>
<thead>
<tr>
<th>Passage (some parts shortened)</th>
<th>Question</th>
<th>Answer</th>
<th>BIzAF</th>
</tr>
</thead>
<tbody>
<tr>
<td>That year, his <em>Untitled</em> (1981), a painting of a halved, black-headed man with a bright red skeletal body, depicted amid the artists signature scrawls, was <strong>sold by Robert Lehrman for $16.3 million, well above its $12 million high estimate.</strong></td>
<td>How many more dollars was the <em>Untitled</em> (1981) painting sold for than the 12 million dollar estimation?</td>
<td>$16.3 million</td>
<td></td>
</tr>
</tbody>
</table>

- Question types: subtraction, comparison (*which did he visit first*), counting and sorting (*which kicker kicked more field goals*),

- Typically even systems like GPT-3 benefit from having a “calculator” they can call; many chain-of-thought variants with this structure

Dua et al. (2019)

**NarrativeQA**

- Humans see a summary of a book: *...Peter’s former girlfriend Dana Barrett has had a son, Oscar...*

- Question: *How is Oscar related to Dana?*

- Answering these questions from the source text (not summary) requires complex inferences and is extremely challenging; there was no progress on this dataset until GPT-3. These are still some of the hardest types of questions!

Kočiský et al. (2017)

**QA vs. Dialog**

- Can have interactive dialogs with series of questions

- ChatGPT/Bing/Bard: can reference earlier context, also retrieve information from external sources

- Barriers between {QA, QA with retrieval, dialog} are eroded now

**Takeaways**

- Many individual QA datasets aren’t perfect and have artifacts, but collectively, they test a wide range of capabilities

- QA over tables, images, knowledge bases, ...: all of this is unified and homogenized in GPT-era systems

- Integrating with retrieval and how to generate long answers are still two very challenging problems

- Major frontier: answers require reasoning beyond text: computation (although we can do this sometimes), physical simulation, statistical analysis, ...