CHAPTER

11 Transfer Learning with Pre-trained Language Models and Contextual Embeddings

"How much do we know at any time? Much more, or so I believe, than we know we know."

Agatha Christie, *The Moving Finger*

Fluent speakers bring an enormous amount of knowledge to bear during comprehension and production of language. This knowledge is embodied in many forms, perhaps most obviously in the vocabulary. That is, in the rich representations associated with the words we know, including their grammatical function, meaning, real-world reference, and pragmatic function. This makes the vocabulary a useful lens to explore the acquisition of knowledge from text, by both people and machines.

Estimates of the size of adult vocabularies vary widely both within and across languages. For example, estimates of the vocabulary size of young adult speakers of American English range from 30,000 to 100,000 depending on the resources used to make the estimate and the definition of what it means to know a word. What is agreed upon is that the vast majority of words that mature speakers use in their day-to-day interactions are acquired early in life through spoken interactions in context with care givers and peers, usually well before the start of formal schooling. This active vocabulary is extremely limited compared to the size of the adult vocabulary (usually on the order of 2000 words for young speakers) and is quite stable, with very few additional words learned via casual conversation beyond this early stage. Obviously, this leaves a very large number of words to be acquired by some other means.

A simple consequence of these facts is that children have to learn about 7 to 10 words a day, *every single day*, to arrive at observed vocabulary levels by the time they are 20 years of age. And indeed empirical estimates of vocabulary growth in late elementary through high school are consistent with this rate. How do children achieve this rate of vocabulary growth given their daily experiences during this period? We know that most of this growth is not happening through direct vocabulary instruction in school since these methods are largely ineffective, and are not deployed at a rate that would result in the reliable acquisition of words at the required rate.

The most likely remaining explanation is that the bulk of this knowledge acquisition happens as a by-product of reading. Research into the average amount of time children spend reading, and the lexical diversity of the texts they read, indicate that it is possible to achieve the desired rate. But the mechanism behind this rate of learning must be remarkable indeed, since at some points during learning the rate of vocabulary growth exceeds the rate at which new words are appearing to the learner!

Many of these facts have motivated approaches to word learning based on the

distributional hypothesis, introduced in Chapter 6. This is the idea that something about what we're loosely calling word meanings can be learned even without any grounding in the real world, solely based on the content of the texts we've encountered over our lives. This knowledge is based on the complex association of words with the words they co-occur with (and with the words that those words occur with).

The crucial insight of the distributional hypothesis is that the knowledge that we acquire through this process can be brought to bear during language processing long after its initial acquisition in novel contexts. We saw in Chapter 6 that embeddings (static word representations) can be learned from text and then employed for other purposes like measuring word similarity or studying meaning change over time.

In this chapter, we expand on this idea in two large ways. First, we'll introduce the idea of **contextual embeddings**: representations for words in context. The methods of Chapter 6 like word2vec or GloVe learned a single vector embedding for each unique word w in the vocabulary. By contrast, with contextual embeddings, such as those learned by popular methods like BERT (Devlin et al., 2019) or GPT (Radford et al., 2019) or their descendants, each word w will be represented by a different vector each time it appears in a different context.

pretraining   Second, we'll introduce in this chapter the idea of **pretraining** and **fine-tuning**.
fine-tuning   We call **pretraining** the process of learning some sort of representation of meaning for words or sentences by processing very large amounts of text. We'll call these pretrained models **pretrained language models**, since they can take the form of the transformer language models we introduced in Chapter 9. We call **fine-tuning** the process of taking the representations from these pretrained models, and further training the model, often via an added neural net classifier, to perform some downstream task like named entity tagging or question answering or coreference. The intuition is that the pretraining phase learns a language model that instantiates a rich representations of word meaning, that thus enables the model to more easily learn ('be fine-tuned to') the requirements of a downstream language understanding task.

transfer   The pretrain-finetune paradigm is an instance of what is called **transfer learning**
learning   in machine learning: the method of acquiring knowledge from one task or domain, and then applying it (transferring it) to solve a new task. Of course, adding grounding from vision or from real-world interaction into pretrained models can help build even more powerful models, but even text alone is remarkably useful, and we will limit our attention here to purely textual models.

There are two common paradigms for pretrained language models. One is the **causal** or left-to-right transformer model we introduced in Chapter 9. In this chapter we'll introduce a second paradigm, called the **bidirectional transformer** encoder, and the method of **masked language modeling**, introduced with the BERT model (Devlin et al., 2019) that allows the model to see entire texts at a time, including both the right and left context.

Finally, we'll show how the contextual embeddings from these pretrained language models can be used to transfer the knowledge embodied in these models to novel applications via fine-tuning. Indeed, in later chapters we'll see pretrained language models fine-tuned to tasks from parsing to question answering, from information extraction to semantic parsing.

11.1 Bidirectional Transformer Encoders

Let's begin by introducing the bidirectional transformer encoder that underlies models like BERT and its descendants like **RoBERTa** (Liu et al., 2019) or **SpanBERT** (Joshi et al., 2020). In Chapter 9 we explored causal (left-to-right) transformers that can serve as the basis for powerful language models—models that can easily be applied to autoregressive generation problems such as contextual generation, summarization and machine translation. However, when applied to sequence classification and labeling problems causal models have obvious shortcomings since they are based on an incremental, left-to-right processing of their inputs. If we want to assign the correct named-entity tag to each word in a sentence, or other sophisticated linguistic labels like the parse tags we'll introduce in later chapters, we'll want to be able to take into account information from the right context as we process each element. Fig. 11.1, reproduced here from Chapter 9, illustrates the information flow in the purely left-to-right approach of Chapter 9. As can be seen, the hidden state computation at each point in time is based solely on the current and earlier elements of the input, ignoring potentially useful information located to the right of each tagging decision.
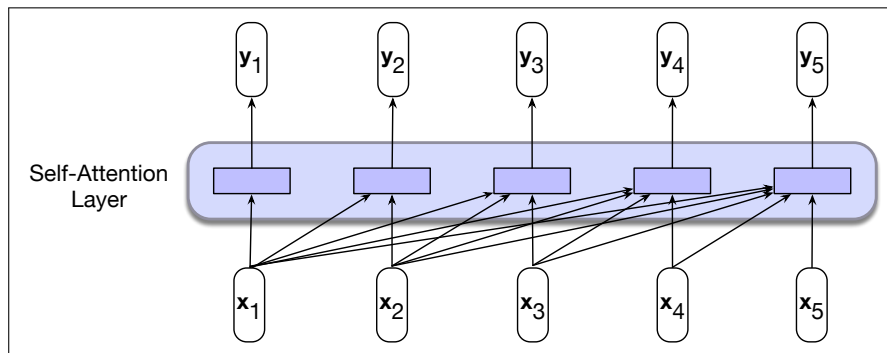

Figure 11.1 A causal, backward looking, transformer model like Chapter 9. Each output is computed independently of the others using only information seen earlier in the context.
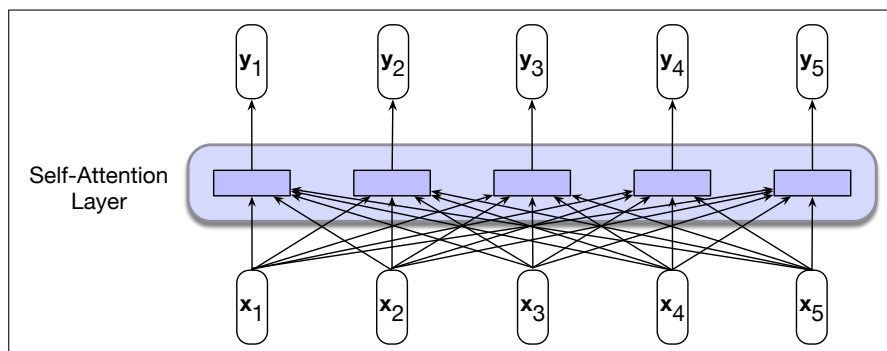

Figure 11.2 Information flow in a bidirectional self-attention model. In processing each element of the sequence, the model attends to all inputs, both before and after the current one.

Bidirectional encoders overcome this limitation by allowing the self-attention mechanism to range over the entire input, as shown in Fig. 11.2. The focus of bidirectional encoders is on computing contextualized representations of the tokens in an

input sequence that are generally useful across a range of downstream applications. Therefore, bidirectional encoders use self-attention to map sequences of input embeddings $(\mathbf{x}_1, ..., \mathbf{x}_n)$ to sequences of output embeddings the same length $(\mathbf{y}_1, ..., \mathbf{y}_n)$, where the output vectors have been contextualized using information from the entire input sequence.

This contextualization is accomplished through the use of the same self-attention mechanism used in causal models. As with these models, the first step is to generate a set of key, query and value embeddings for each element of the input vector $\mathbf{x}$ through the use of learned weight matrices $\mathbf{W}^{\mathbf{Q}}$, $\mathbf{W}^{\mathbf{K}}$, and $\mathbf{W}^{\mathbf{V}}$. These weights project each input vector $\mathbf{x}_i$ into its specific role as a key, query, or value.

$$\mathbf{q}_i = \mathbf{W}^{\mathbf{Q}}\mathbf{x}_i; \;\; \mathbf{k}_i = \mathbf{W}^{\mathbf{K}}\mathbf{x}_i; \;\; \mathbf{v}_i = \mathbf{W}^{\mathbf{V}}\mathbf{x}_i \tag{11.1}$$

The output vector $\mathbf{y}_i$ corresponding to each input element $\mathbf{x}_i$ is a weighted sum of all the input value vectors $\mathbf{v}$, as follows:

$$\mathbf{y}_i \;=\; \sum_{j=i}^{n} \alpha_{ij}\mathbf{v}_j \tag{11.2}$$

The α weights are computed via a softmax over the comparison scores between every element of an input sequence considered as a query and every other element as a key, where the comparison scores are computed using dot products.

$$\alpha_{ij} \;=\; \frac{\exp(\text{score}_{ij})}{\sum_{k=1}^{n} \exp(\text{score}_{ik})} \tag{11.3}$$

$$\text{score}_{ij} \;=\; \mathbf{q}_i \cdot \mathbf{k}_j \tag{11.4}$$

Since each output vector, $\mathbf{y}_i$, is computed independently, the processing of an entire sequence can be parallelized via matrix operations. The first step is to pack the input embeddings $\mathbf{x}_i$ into a matrix $\mathbf{X} \in \mathbb{R}^{N \times d_h}$. That is, each row of $\mathbf{X}$ is the embedding of one token of the input. We then multiply $\mathbf{X}$ by the key, query, and value weight matrices (all of dimensionality $d \times d$) to produce matrices $\mathbf{Q} \in \mathbb{R}^{N \times d}$, $\mathbf{K} \in \mathbb{R}^{N \times d}$, and $\mathbf{V} \in \mathbb{R}^{N \times d}$, containing all the key, query, and value vectors in a single step.

$$\mathbf{Q} = \mathbf{X}\mathbf{W}^{\mathbf{Q}}; \;\; \mathbf{K} = \mathbf{X}\mathbf{W}^{\mathbf{K}}; \;\; \mathbf{V} = \mathbf{X}\mathbf{W}^{\mathbf{V}} \tag{11.5}$$

Given these matrices we can compute all the requisite query-key comparisons simultaneously by multiplying $\mathbf{Q}$ and $\mathbf{K}^{\mathsf{T}}$ in a single operation. Fig. 11.3 illustrates the result of this operation for an input with length 5.

Finally, we can scale these scores, take the softmax, and then multiply the result by $\mathbf{V}$ resulting in a matrix of shape $N \times d$ where each row contains a contextualized output embedding corresponding to each token in the input.

$$\textit{SelfAttention}(\mathbf{Q}, \mathbf{K}, \mathbf{V}) \;=\; \text{softmax}\left(\frac{\mathbf{Q}\mathbf{K}^{\mathsf{T}}}{\sqrt{d_k}}\right)\mathbf{V} \tag{11.6}$$

As shown in Fig. 11.3, the full set of self-attention scores represented by $\mathbf{Q}\mathbf{K}^{T}$ constitute an all-pairs comparison between the keys and queries for each element of the input. In the case of causal language models in Chapter 9, we masked the upper triangular portion of this matrix (in Fig. **??**) to eliminate information about future words since this would make the language modeling training task trivial. With

Figure 11.3 The $N \times N$ **QK**$^\mathsf{T}$ matrix showing the complete set of $q_i \cdot k_j$ comparisons.

bidirectional encoders we simply skip the mask, allowing the model to contextualize each token using *information from the entire input*.

Beyond this simple change, all of the other elements of the transformer architecture remain the same for bidirectional encoder models. Inputs to the model are segmented using subword tokenization and are combined with positional embeddings before being passed through a series of standard transformer blocks consisting of self-attention and feedforward layers augmented with residual connections and layer normalization, as shown in Fig. 11.4.
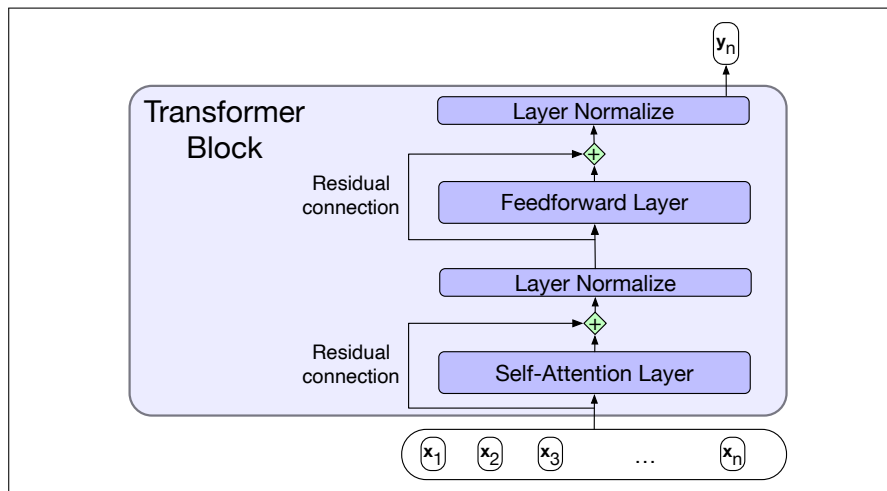

Figure 11.4 A transformer block showing all the layers.

To make this more concrete, the original bidirectional transformer encoder model, BERT (Devlin et al., 2019), consisted of the following:

- A subword vocabulary consisting of 30,000 tokens generated using the Word-Piece algorithm (Schuster and Nakajima, 2012),
- Hidden layers of size of 768,
- 12 layers of transformer blocks, with 12 multihead attention layers each.

The result is a model with over 100M parameters. The use of WordPiece (one of the large family of subword tokenization algorithms that includes the BPE algorithm we saw in Chapter 2) means that BERT and its descendants are based on subword tokens rather than words. Every input sentence first has to be tokenized, and then

all further processing takes place on subword tokens rather than words. This will require, as we'll see, that for some NLP tasks that require notions of words (like named entity tagging, or parsing) we will occasionally need to map subwords back to words.

Finally, a fundamental issue with transformers is that the size of the input layer dictates the complexity of model. Both the time and memory requirements in a transformer grow quadratically with the length of the input. It's necessary, therefore, to set a fixed input length that is long enough to provide sufficient context for the model to function and yet still be computationally tractable. For BERT, a fixed input size of 512 subword tokens was used.

11.2 Training Bidirectional Encoders

We trained causal transformer language models in Chapter 9 by making them iteratively predict the next word in a text. But eliminating the causal mask makes the guess-the-next-word language modeling task trivial since the answer is now directly available from the context, so we're in need of a new training scheme. Fortunately, the traditional learning objective suggests an approach that can be used to train bidirectional encoders. Instead of trying to predict the next word, the model learns to perform a fill-in-the-blank task, technically called the **cloze task** (Taylor, 1953). To see this, let's return to the motivating example from Chapter 3. Instead of predicting which words are likely to come next in this example:

cloze task

> Please turn your homework _____ .

we're asked to predict a missing item given the rest of the sentence.

> Please turn _____ homework in.

That is, given an input sequence with one or more elements missing, the learning task is to predict the missing elements. More precisely, during training the model is deprived of one or more elements of an input sequence and must generate a probability distribution over the vocabulary for each of the missing items. We then use the cross-entropy loss from each of the model's predictions to drive the learning process.

This approach can be generalized to any of a variety of methods that corrupt the training input and then asks the model to recover the original input. Examples of the kinds of manipulations that have been used include masks, substitutions, reorderings, deletions, and extraneous insertions into the training text.

11.2.1 Masking Words

Masked Language Modeling MLM

The original approach to training bidirectional encoders is called **Masked Language Modeling** (MLM) (Devlin et al., 2019). As with the language model training methods we've already seen, **MLM** uses unannotated text from a large corpus. Here, the model is presented with a series of sentences from the training corpus where a random sample of tokens from each training sequence is selected for use in the learning task. Once chosen, a token is used in one of three ways:

- It is replaced with the unique vocabulary token [MASK].
- It is replaced with another token from the vocabulary, randomly sampled based on token unigram probabilities.
- It is left unchanged.

In BERT, 15% of the input tokens in a training sequence are sampled for learning. Of these, 80% are replaced with [MASK], 10% are replaced with randomly selected tokens, and the remaining 10% are left unchanged.

The MLM training objective is to predict the original inputs for each of the masked tokens using a bidirectional encoder of the kind described in the last section. The cross-entropy loss from these predictions drives the training process for all the parameters in the model. Note that all of the input tokens play a role in the self-attention process, but only the sampled tokens are used for learning.

More specifically, the original input sequence is first tokenized using a subword model. The sampled items which drive the learning process are chosen from among the set of tokenized inputs. Word embeddings for all of the tokens in the input are retrieved from the word embedding matrix and then combined with positional embeddings to form the input to the transformer.
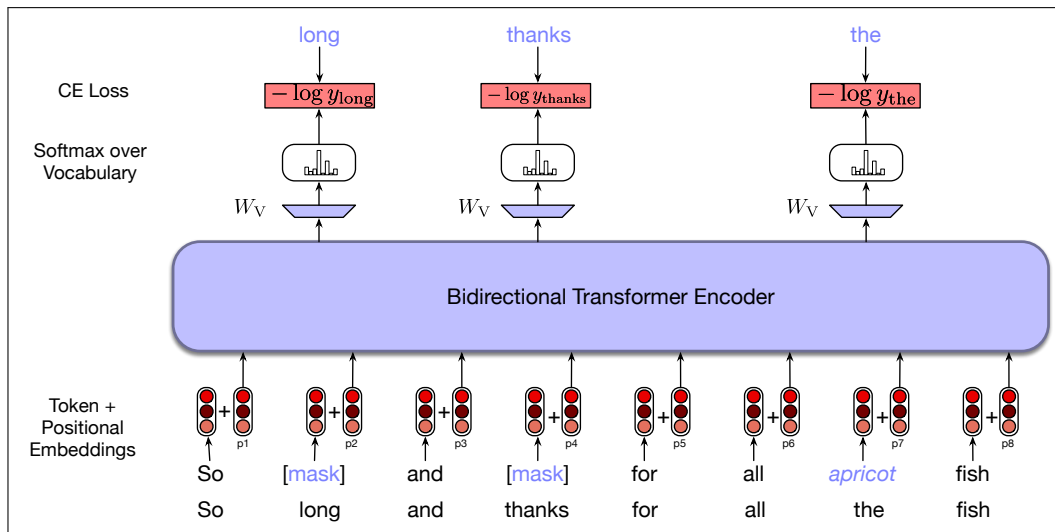

Figure 11.5 Masked language model training. In this example, three of the input tokens are selected, two of which are masked and the third is replaced with an unrelated word. The probabilities assigned by the model to these three items are used as the training loss. (In this and subsequent figures we display the input as words rather than subword tokens; the reader should keep in mind that BERT and similar models actually use subword tokens instead.)

Fig. 11.5 illustrates this approach with a simple example. Here, *long*, *thanks* and *the* have been sampled from the training sequence, with the first two masked and *the* replaced with the randomly sampled token *apricot*. The resulting embeddings are passed through a stack of bidirectional transformer blocks. To produce a probability distribution over the vocabulary for each of the masked tokens, the output vector from the final transformer layer for each of the masked tokens is multiplied by a learned set of classification weights $\mathbf{W}_V \in \mathbb{R}^{|V| \times d_h}$ and then through a softmax to yield the required predictions over the vocabulary.

$$y_i = \text{softmax}(\mathbf{W}_V h_i)$$

With a predicted probability distribution for each masked item, we can use cross-entropy to compute the loss for each masked item—the negative log probability assigned to the actual masked word, as shown in Fig. 11.5. The gradients that form

the basis for the weight updates are based on the average loss over the sampled learning items from a single training sequence (or batch of sequences).

11.2.2   Masking Spans

For many NLP applications, the natural unit of interest may be larger than a single word (or token). Question answering, syntactic parsing, coreference and semantic role labeling applications all involve the identification and classification of constituents, or phrases. This suggests that a span-oriented masked learning objective might provide improved performance on such tasks.

A span is a contiguous sequence of one or more words selected from a training text, prior to subword tokenization. In span-based masking, a set of randomly selected spans from a training sequence are chosen. In the SpanBERT work that originated this technique (Joshi et al., 2020), a span length is first chosen by sampling from a geometric distribution that is biased towards shorter spans an with upper bound of 10. Given this span length, a starting location consistent with the desired span length and the length of the input is sampled uniformly.

Once a span is chosen for masking, all the words within the span are substituted according to the same regime used in BERT: 80% of the time the span elements are substituted with the [MASK] token, 10% of the time they are replaced by randomly sampled words from the vocabulary, and 10% of the time they are left as is. Note that this substitution process is done at the span level—all the tokens in a given span are substituted using the same method. As with BERT, the total token substitution is limited to 15% of the training sequence input. Having selected and masked the training span, the input is passed through the standard transformer architecture to generate contextualized representations of the input tokens.

Downstream span-based applications rely on span representations derived from the tokens within the span, as well as the start and end points, or the boundaries, of a span. Representations for these boundaries are typically derived from the first and last words of a span, the words immediately preceding and following the span, or some combination of them. The SpanBERT learning objective augments the MLM objective with a boundary oriented component called the Span Boundary Objective (SBO). The SBO relies on a model's ability to predict the words within a masked span from the words immediately preceding and following it. This prediction is made using the output vectors associated with the words that immediately precede and follow the span being masked, along with positional embedding that signals which word in the span is being predicted:

$$L(x) = L_{MLM}(x) + L_{SBO}(x) \tag{11.7}$$
$$L_{SBO}(x) = -logP(x|x_s, x_e, p_x) \tag{11.8}$$

where s denotes the position of the word before the span and e denotes the word after the end. The prediction for a given position i within the span is produced by concatenating the output embeddings for words s and e span boundary vectors with a positional embedding for position i and passing the result through a 2-layer feedforward network.

$$s = \text{FFNN}([y_{s-1}; y_{e+1}; p_{i-s+1}]) \tag{11.9}$$
$$z = \text{softmax}(Es) \tag{11.10}$$

The final loss is the sum of the BERT MLM loss and the SBO loss.

Fig. 11.6 illustrates this with one of our earlier examples. Here the span selected is *and thanks for* which spans from position 3 to 5. The total loss associated with the masked token *thanks* is the sum of the cross-entropy loss generated from the prediction of *thanks* from the output $\mathbf{y}_4$, plus the cross-entropy loss from the prediction of *thanks* from the output vectors for $\mathbf{y}_2$, $\mathbf{y}_6$ and the embedding for position 4 in the span.
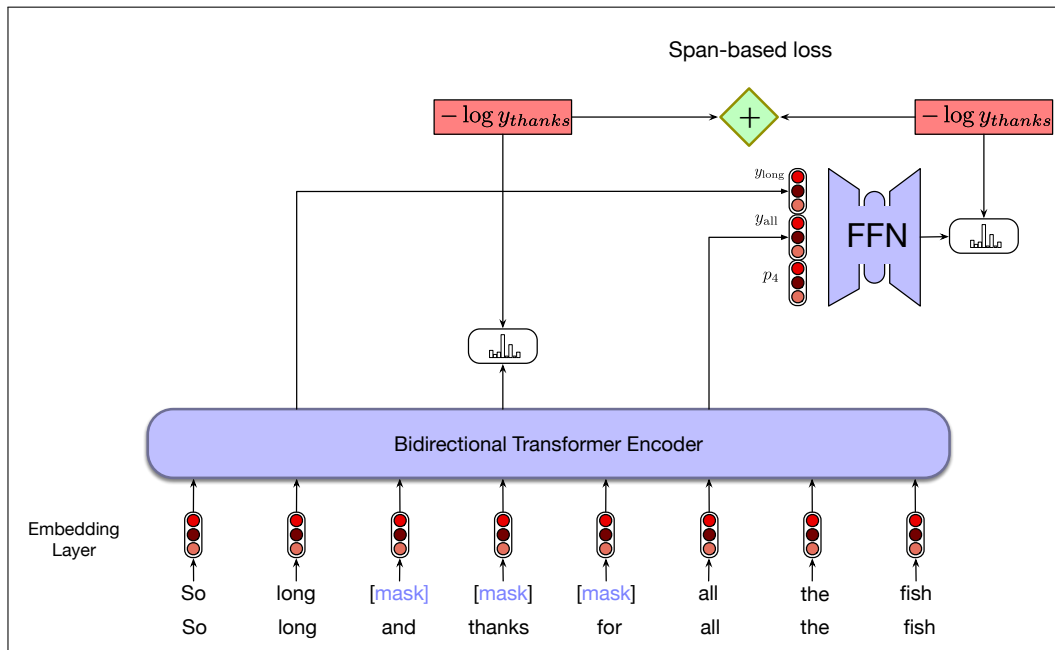

Figure 11.6   Span-based language model training. In this example, a span of length 3 is selected for training and all of the words in the span are masked. The figure illustrates the loss computed for word *thanks*; the loss for the entire span is based on the loss for all three of the words in the span.

11.2.3 Next Sentence Prediction

The focus of masked-based learning is on predicting words from surrounding contexts with the goal of producing effective word-level representations. However, an important class of applications involves determining the relationship between pairs of sentences. These includes tasks like paraphrase detection (detecting if two sentences have similar meanings), entailment (detecting if the meanings of two sentences entail or contradict each other) or discourse coherence (deciding if two neighboring sentences form a coherent discourse).

To capture the kind of knowledge required for applications such as these, BERT introduced a second learning objective called **Next Sentence Prediction** (NSP). In this task, the model is presented with pairs of sentences and is asked to predict whether each pair consists of an actual pair of adjacent sentences from the training corpus or a pair of unrelated sentences. In BERT, 50% of the training pairs consisted of positive pairs, and in the other 50% the second sentence of a pair was randomly selected from elsewhere in the corpus. The NSP loss is based on how well the model can distinguish true pairs from random pairs.

To facilitate NSP training, BERT introduces two new tokens to the input representation (tokens that will prove useful for fine-tuning as well). After tokenizing the

Next Sentence Prediction

input with the subword model, the token [CLS] is prepended to the input sentence pair, and the token [SEP] is placed between the sentences and after the final token of the second sentence. Finally, embeddings representing the first and second segments of the input are added to the word and positional embeddings to allow the model to more easily distinguish the input sentences.

During training, the output vector from the final layer associated with the [CLS] token represents the next sentence prediction. As with the MLM objective, a learned set of classification weights $\mathbf{W_{NSP}} \in \mathbb{R}^{2 \times d_h}$ is used to produce a two-class prediction from the raw [CLS] vector.

$$y_i \;=\; \text{softmax}(\mathbf{W_{NSP}}h_i)$$

Cross entropy is used to compute the NSP loss for each sentence pair presented to the model. Fig. 11.7 illustrates the overall NSP training setup. In BERT, the NSP loss was used in conjunction with the MLM training objective to form final loss.
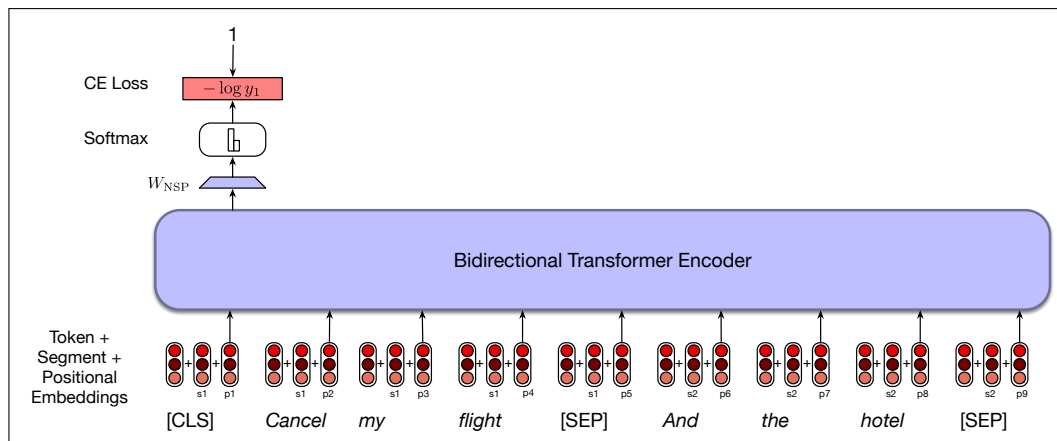

Figure 11.7   An example of the NSP loss calculation.

11.2.4   Training Regimes

The corpus used in training BERT and other early transformer-based language models consisted of an 800 million word corpus of book texts called BooksCorpus (Zhu et al., 2015) and a 2.5 Billion word corpus derived from the English Wikipedia, for a combined size of 3.3 Billion words. The BooksCorpus is no longer used (for intellectual property reasons), and in general, as we'll discuss later, state-of-the-art models employ corpora that are orders of magnitude larger than these early efforts.

To train the original BERT models, pairs of sentences were selected from the training corpus according to the next sentence prediction 50/50 scheme. Pairs were sampled so that their combined length was less than the 512 token input. Tokens within these sentence pairs were then masked using the MLM approach with the combined loss from the MLM and NSP objectives used for a final loss. Approximately 40 passes (epochs) over the training data was required for the model to converge.

The result of this pretraining process consists of both learned word embeddings, as well as all the parameters of the bidirectional encoder that are used to produce contextual embeddings for novel inputs.

11.2.5 Contextual Embeddings

contextual embeddings

Given a pretrained language model and a novel input sentence, we can think of the output of the model as constituting **contextual embeddings** for each token in the input. These contextual embeddings can be used as a contextual representation of the meaning of the input token for any task requiring the meaning of word.

Contextual embeddings are thus vectors representing some aspect of the meaning of a token in context. For example, given a sequence of input tokens $x_1, ..., x_n$, we can use the output vector y_i from the final layer of the model as a representation of the meaning of token x_i in the context of sentence $x_1, ..., x_n$. Or instead of just using the vector y_i from the final layer of the model, it's common to compute a representation for x_i by averaging the output tokens y_i from each of the last four layers of the model.

Just as we used static embeddings like word2vec to represent the meaning of words, we can use contextual embeddings as representations of word meanings in context for any task that might require a model of word meaning. Where static embeddings represent the meaning of word *types* (vocabulary entries), contextual embeddings represent the meaning of word *tokens*: instances of a particular word type in a particular context. Contextual embeddings can thus by used for tasks like measuring the semantic similarity of two words in context, and are useful in linguistic tasks that require models of word meaning.

In the next section, however, we'll see the most common use of these representations: as embeddings of word or even entire sentences that are the inputs to classifiers in the fine-tuning process for downstream NLP applications.

11.3 Transfer Learning through Fine-Tuning

The power of pretrained language models lies in their ability to extract generalizations from large amounts of text—generalizations that are useful for myriad downstream applications. To make practical use of these generalizations, we need to create interfaces from these models to downstream applications through a process **fine-tuning** called **fine-tuning**. Fine-tuning facilitates the creation of applications on top of pretrained models through the addition of a small set of application-specific parameters. The fine-tuning process consists of using labeled data from the application to train these additional application-specific parameters. Typically, this training will either freeze or make only minimal adjustments to the pretrained language model parameters.

The following sections introduce fine-tuning methods for the most common applications including sequence classification, sequence labeling, sentence-pair inference, and span-based operations.

11.3.1 Sequence Classification

Sequence classification applications often represent an input sequence with a single consolidated representation. With RNNs, we used the hidden layer associated with the final input element to stand for the entire sequence. A similar approach is used with transformers. An additional vector is added to the model to stand for the entire **sentence embedding** sequence. This vector is sometimes called the **sentence embedding** since it refers to the entire sequence, although the term 'sentence embedding' is also used in other ways. In BERT, the [CLS] token plays the role of this embedding. This unique token

is added to the vocabulary and is prepended to the start of all input sequences, both during pretraining and encoding. The output vector in the final layer of the model for the [CLS] input represents the entire input sequence and serves as the input to **classifier head** a **classifier head**, a logistic regression or neural network classifier that makes the relevant decision.

As an example, let's return to the problem of sentiment classification. A simple approach to fine-tuning a classifier for this application involves learning a set of weights, $\mathbf{W_C}$, to map the output vector for the [CLS] token, $\mathbf{y_{CLS}}$ to a set of scores over the possible sentiment classes. Assuming a three-way sentiment classification task (positive, negative, neutral) and dimensionality d_h for the size of the language model hidden layers gives $\mathbf{W_C} \in \mathbb{R}^{3 \times d_h}$. Classification of unseen documents proceeds by passing the input text through the pretrained language model to generate $\mathbf{y_{CLS}}$, multiplying it by $\mathbf{W_C}$, and finally passing the resulting vector through a softmax.

$$\mathbf{y} = \text{softmax}(\mathbf{W_C y_{CLS}}) \qquad (11.11)$$

Finetuning the values in $\mathbf{W_C}$ requires supervised training data consisting of input sequences labeled with the appropriate class. Training proceeds in the usual way; cross-entropy loss between the softmax output and the correct answer is used to drive the learning that produces $\mathbf{W_C}$.

A key difference from what we've seen earlier with neural classifiers is that this loss can be used to not only learn the weights of the classifier, but also to update the weights for the pretrained language model itself. In practice, reasonable classification performance is typically achieved with only minimal changes to the language model parameters, often limited to updates over the final few layers of the transformer. Fig. 11.8 illustrates this overall approach to sequence classification.
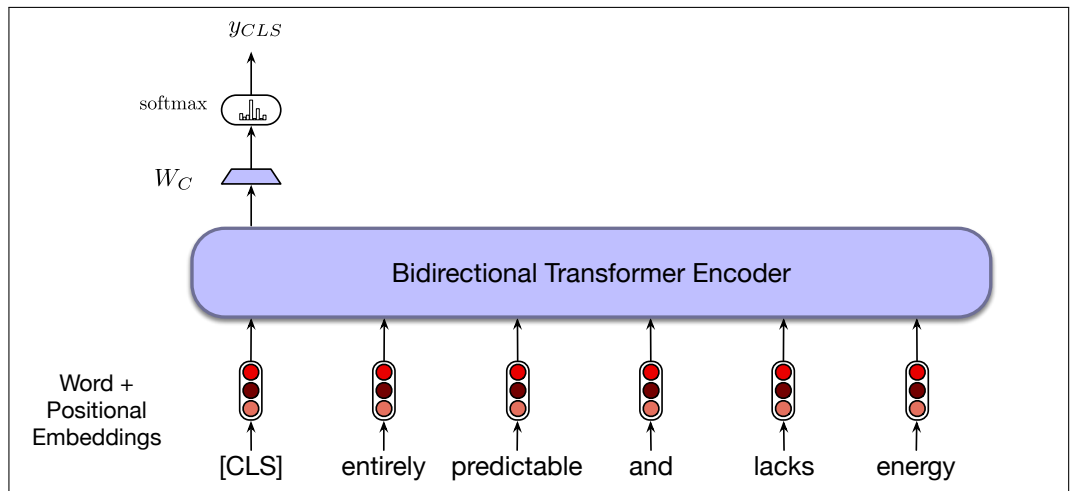

Figure 11.8 Sequence classification with a bidirectional transformer encoder. The output vector for the [CLS] token serves as input to a simple classifier.

11.3.2 Pair-Wise Sequence Classification

As mentioned in Section 11.2.3, an important type of problem involves the classification of pairs of input sequences. Practical applications that fall into this class include logical entailment, paraphrase detection and discourse analysis.

Fine-tuning an application for one of these tasks proceeds just as with pretraining using the NSP objective. During fine-tuning, pairs of labeled sentences from the supervised training data are presented to the model. As with sequence classification, the output vector associated with the prepended [CLS] token represents the model's view of the input pair. And as with NSP training, the two inputs are separated by the a [SEP] token. To perform classification, the [CLS] vector is multiplied by a set of learning classification weights and passed through a softmax to generate label predictions, which are then used to update the weights.

As an example, let's consider an entailment classification task with the Multi-Genre Natural Language Inference (MultiNLI) dataset (Williams et al., 2018). In **natural language inference** the task of **natural language inference** or **NLI**, also called **recognizing textual entailment**, a model is presented with a pair of sentences and must classify the relationship between their meanings. For example in the MultiNLI corpus, pairs of sentences are given one of 3 labels: *entails*, *contradicts* and *neutral*. These labels describe a relationship between the meaning of the first sentence (the premise) and the meaning of the second sentence (the hypothesis). Here are representative examples of each class from the corpus:

- Neutral
    - a: Jon walked back to the town to the smithy.
    - b: Jon traveled back to his hometown.

- Contradicts
    - a: Tourist Information offices can be very helpful.
    - b: Tourist Information offices are never of any help.

- Entails
    - a: I'm confused.
    - b: Not all of it is very clear to me.

A relationship of *contradicts* means that the premise contradicts the hypothesis; *entails* means that the premise entails the hypothesis; *neutral* means that neither is necessarily true. The meaning of these labels is looser than strict logical entailment or contradiction indicating that a typical human reading the sentences would most likely interpret the meanings in this way.

To fine-tune a classifier for the MultiNLI task, we pass the premise/hypothesis pairs through a bidirectional encoder as described above and use the output vector for the [CLS] token as the input to the classification head. As with ordinary sequence classification, this head provides the input to a three-way classifier that can be trained on the MultiNLI training corpus.

11.3.3   Sequence Labelling

Sequence labelling tasks, such as part-of-speech tagging or BIO-based named entity recognition, follow the same basic classification approach. Here, the final output vector corresponding to *each input token* is passed to a classifier that produces a softmax distribution over the possible set of tags. Again, assuming a simple classifier consisting of a single feedforward layer followed by a softmax, the set of weights to be learned for this additional layer is $\mathbf{W_K} \in \mathbb{R}^{k \times d_h}$, where k is the number of possible tags for the task. As with RNNs, a greedy approach, where the argmax tag for each token is taken as a likely answer, can be used to generate the final output

tag sequence. Fig. 11.9 illustrates an example of this approach.

$$\mathbf{y_i} = \text{softmax}(\mathbf{W_K z_i}) \tag{11.12}$$

$$\mathbf{t_i} = \text{argmax}_k(\mathbf{y}_i) \tag{11.13}$$

Alternatively, the distribution over labels provided by the softmax for each input token can be passed to a conditional random field (CRF) layer which can take global tag-level transitions into account.
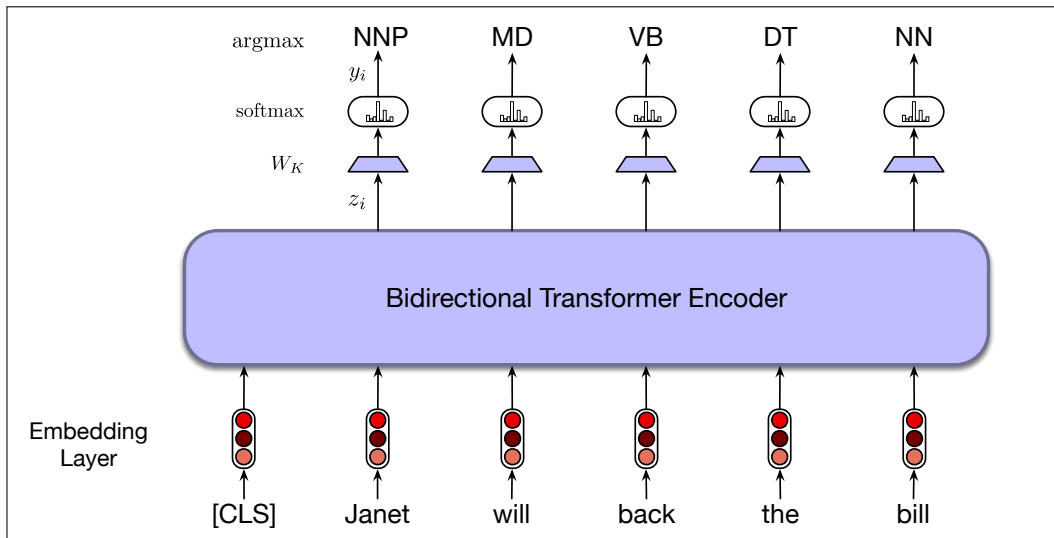

Figure 11.9 Sequence labeling for part-of-speech tagging with a bidirectional transformer encoder. The output vector for each input token is passed to a simple k-way classifier.

A complication with this approach arises from the use of subword tokenization such as WordPiece or Byte Pair Encoding. Supervised training data for tasks like named entity recognition (NER) is typically in the form of BIO tags associated with text segmented at the word level. For example the following sentence containing two named entities:

[$_{\text{LOC}}$ **Mt. Sanitas**] is in [$_{\text{LOC}}$ **Sunshine Canyon**] .

would have the following set of per-word BIO tags.

(11.14) *Mt.   Sanitas is in Sunshine Canyon .*
     B-LOC I-LOC O O B-LOC   I-LOC O

Unfortunately, the WordPiece tokenization for this sentence yields the following sequence of tokens which doesn't align directly with BIO tags in the ground truth annotation:

```
'Mt', '.', 'San', '##itas', 'is', 'in', 'Sunshine', 'Canyon' '.'
```

To deal with this misalignment, we need a way to assign BIO tags to subword tokens during training and a corresponding way to recover word-level tags from subwords during decoding. For training, we can just assign the gold-standard tag associated with each word to all of the subword tokens derived from it.

For decoding, the simplest approach is to use the argmax BIO tag associated with the first subword token of a word. Thus, in our example, the BIO tag assigned to

"Mt" would be assigned to "Mt." and the tag assigned to "San" would be assigned to "Sanitas", effectively ignoring the information in the tags assigned to "." and "##itas". More complex approaches combine the distribution of tag probabilities across the subwords in an attempt to find an optimal word-level tag.

11.3.4   Fine-tuning for Span-Based Applications

Span-oriented applications operate in a middle ground between sequence level and token level tasks. That is, in span-oriented applications the focus is on generating and operating with representations of contiguous sequences of tokens. Typical operations include identifying spans of interest, classifying spans according to some labeling scheme, and determining relations among discovered spans. Applications include named entity recognition, question answering, syntactic parsing, semantic role labeling and coreference resolution.

Formally, given an input sequence x consisting of T tokens, $(x_1, x_2, ..., x_T)$, a span is a contiguous sequence of tokens with start i and end j such that $1 <= i <= j <= T$. This formulation results in a total set of spans equal to $\frac{T(T-1)}{2}$. For practical purposes, span-based models often impose an application-specific length limit L, so the legal spans are limited to those where $j - i < L$. In the following, we'll refer to the enumerated set of legal spans in x as $S(x)$.

The first step in fine-tuning a pretrained language model for a span-based application using the contextualized input embeddings from the model to generate representations for all the spans in the input. Most schemes for representing spans make use of two primary components: representations of the span boundaries and summary representations of the contents of each span. To compute a unified span representation, we concatenate the boundary representations with the summary representation.

In the simplest possible approach, we can use the contextual embeddings of the start and end tokens of a span as the boundaries, and the average of the output embeddings within the span as the summary representation.

$$g_{ij} \;=\; \frac{1}{(j-i)+1}\sum_{k=i}^{j} h_k \tag{11.15}$$

$$\text{spanRep}_{ij} \;=\; [h_i; h_j; g_{i,j}] \tag{11.16}$$

A weakness of this approach is that it doesn't distinguish the use of a word's embedding as the beginning of a span from its use as the end of one. Therefore, more elaborate schemes for representing the span boundaries involve learned representations for start and end points through the use of two distinct feedforward networks:

$$s_i \;=\; \text{FFNN}_{start}(h_i) \tag{11.17}$$

$$e_j \;=\; \text{FFNN}_{end}(h_j) \tag{11.18}$$

$$\text{spanRep}_{ij} \;=\; [s_i; e_j; g_{i,j}] \tag{11.19}$$

Similarly, a simple average of the vectors in a span is unlikely to be an optimal representation of a span since it treats all of a span's embeddings as equally important. For many applications, a more useful representation would be centered around the head of the phrase corresponding to the span. One method for getting at such information in the absence of a syntactic parse is to use a standard self-attention layer to generate a span representation.

$$\mathbf{g}_{ij} = \text{SelfATTN}(\mathbf{h}_{i:j}) \tag{11.20}$$

Now, given span representations **g** for each span in $S(x)$, classifiers can be fine-tuned to generate application-specific scores for various span-oriented tasks: binary span identification (is this a legitimate span of interest or not?), span classification (what kind of span is this?), and span relation classification (how are these two spans related?).

To ground this discussion, let's return to named entity recognition (NER). Given a scheme for representing spans and set of named entity types, a span-based approach to NER is a straightforward classification problem where each span in an input is assigned a class label. More formally, given an input sequence x, we want to assign a label y, from the set of valid NER labels, to each of the spans in $S(x)$. Since most of the spans in a given input will not be named entities we'll add the label NULL to the set of types in Y.

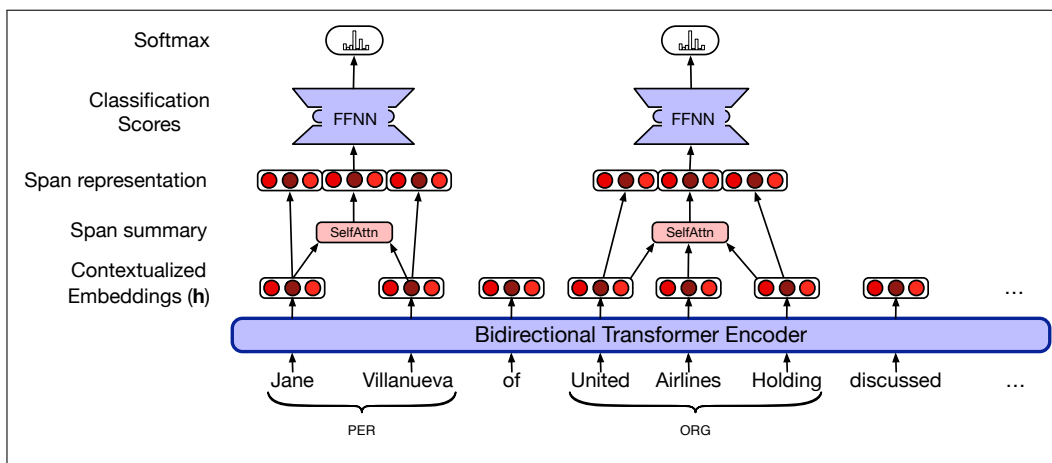$$y_{ij} = \text{softmax}(\text{FFNN}(g_{ij})) \tag{11.21}$$

Figure 11.10 A span-oriented approach to named entity classification. The figure only illustrates the computation for 2 spans corresponding to ground truth named entities. In reality, the network scores all of the $\frac{T(T-1)}{2}$ spans in the text. That is, all the unigrams, bigrams, trigrams, etc. up to the length limit.

With this approach, fine-tuning entails using supervised training data to learn the parameters of the final classifier, as well as the weights used to generate the boundary representations, and the weights in the self-attention layer that generates the span content representation. During training, the model's predictions for all spans are compared to their gold-standard labels and cross-entropy loss is used to drive the training.

During decoding, each span is scored using a softmax over the final classifier output to generate a distribution over the possible labels, with the argmax score for each span taken as the correct answer. Fig. 11.10 illustrates this approach with an example. A variation on this scheme designed to improve precision adds a calibrated threshold to the labeling of a span as anything other than NULL.

There are two significant advantages to a span-based approach to NER over a BIO-based per-word labeling approach. The first advantage is that BIO-based approaches are prone to a labeling mis-match problem. That is, every label in a longer named entity must be correct for an output to be judged correct. Returning to the example in Fig. 11.10, the following labeling would be judged entirely wrong due to the incorrect label on the first item. Span-based approaches only have to make one classification for each span.

(11.22) *Jane Villanueva of United Airlines Holding discussed ...*
          B-PER I-PER   O I-ORG I-ORG I-ORG O

The second advantage to span-based approaches is that they naturally accommodate embedded named entities. For example, in this example both *United Airlines* and *United Airlines Holding* are legitimate named entities. The BIO approach has no way of encoding this embedded structure. But the span-based approach can naturally label both since the spans are labeled separately.

11.4 Transfer Learning via Prompting

11.4.1 Text-to-Text Models

11.4.2 Prompting

11.4.3 Contextual (Few-Shot) Learning

11.5 Training Corpora

11.6 Potential Harms from Language Models

Large pretrained neural language models exhibit many of the potential harms discussed in Chapter 4 and Chapter 6. Many of these harms become realized when pretrained language models are fine-tuned to downstream tasks, particularly those involving text generation, such as in assistive technologies like web search query completion, or predictive typing for email (Olteanu et al., 2020).

For example, language models can generate toxic language. Gehman et al. (2020) show that many kinds of completely non-toxic prompts can nonetheless lead large language models to output hate speech and abuse. Brown et al. (2020) and Sheng et al. (2019) showed that large language models generate sentences displaying negative attitudes toward minority identities such as being Black or gay.

Indeed, language models are biased in a number of ways by the distributions of their training data. Gehman et al. (2020) shows that large language model training datasets include toxic text scraped from banned sites. In addition to problems of toxicity, internet data is disproportionately generated by authors from developed countries, and many large language models train on data from Reddit, whose authors skew male and young. Such biased population samples likely skew the resulting generation away from the perspectives or topics of underrepresented populations. Furthermore, language models can amplify demographic and other biases in training data, just as we saw for embedding models in Chapter 6.

Language models can also be a tool for generating text for misinformation, phishing, radicalization, and other socially harmful activities (Brown et al., 2020). McGuffie and Newhouse (2020) show how large language models generate text that emulates online extremists, with the risk of amplifying extremist movements and their attempt to radicalize and recruit.

Finally, there are important privacy issues. Language models, like other machine

learning models, can **leak** information about their training data. It is thus possible for an adversary to extract individual training-data phrases from a language model such as an individual person's name, phone number, and address (Henderson et al. 2017, Carlini et al. 2020). This is a problem if large language models are trained on private datasets such has electronic health records (EHRs).

Mitigating all these harms is an important but unsolved research question in NLP. Extra pretraining (Gururangan et al., 2020) on non-toxic subcorpora seems to reduce a language model's tendency to generate toxic language somewhat (Gehman et al., 2020). And analyzing the data used to pretrain large language models is important to understand toxicity and bias in generation, as well as privacy, making it extremely important that language models include **datasheets** (page **??**) or **model cards** (page **??**) giving full replicable information on the corpora used to train them.

11.7   Summary

This chapter has introduced the topic of transfer learning from pretrained language models. Here's a summary of the main points that we covered:

- Bidirectional encoders can be used to generate contextualized representations of input embeddings using the entire input context.
- Pretrained language models based on bidirectional encoders can be learned using a masked language model objective where a model is trained to guess the missing information from an input.
- Pretrained language models can be fine-tuned for specific applications by adding lightweight classifier layers on top of the outputs of the pretrained model.

Bibliographical and Historical Notes

Brown, T. B., B. Mann, N. Ryder, M. Subbiah, J. Kaplan, P. Dhariwal, A. Neelakantan, P. Shyam, G. Sastry, A. Askell, S. Agarwal, A. Herbert-Voss, G. Krueger, T. Henighan, R. Child, A. Ramesh, D. M. Ziegler, J. Wu, C. Winter, C. Hesse, M. Chen, E. Sigler, M. Litwin, S. Gray, B. Chess, J. Clark, C. Berner, S. McCandlish, A. Radford, I. Sutskever, and D. Amodei. 2020. Language models are few-shot learners. ArXiv preprint arXiv:2005.14165.

Carlini, N., F. Tramer, E. Wallace, M. Jagielski, A. Herbert-Voss, K. Lee, A. Roberts, T. Brown, D. Song, U. Erlingsson, A. Oprea, and C. Raffel1. 2020. Extracting training data from large language models. ArXiv preprint arXiv:2012.07805.

Devlin, J., M.-W. Chang, K. Lee, and K. Toutanova. 2019. BERT: Pre-training of deep bidirectional transformers for language understanding. *NAACL HLT*.

Gehman, S., S. Gururangan, M. Sap, Y. Choi, and N. A. Smith. 2020. RealToxicityPrompts: Evaluating neural toxic degeneration in language models. *Findings of EMNLP*.

Gururangan, S., A. Marasović, S. Swayamdipta, K. Lo, I. Beltagy, D. Downey, and N. A. Smith. 2020. Don't stop pretraining: Adapt language models to domains and tasks. *ACL*.

Henderson, P., K. Sinha, N. Angelard-Gontier, N. R. Ke, G. Fried, R. Lowe, and J. Pineau. 2017. Ethical challenges in data-driven dialogue systems. *AAAI/ACM AI Ethics and Society Conference*.

Joshi, M., D. Chen, Y. Liu, D. S. Weld, L. Zettlemoyer, and O. Levy. 2020. SpanBERT: Improving pre-training by representing and predicting spans. *TACL*, 8:64–77.

Liu, Y., M. Ott, N. Goyal, J. Du, M. Joshi, D. Chen, O. Levy, M. Lewis, L. Zettlemoyer, and V. Stoyanov. 2019. RoBERTa: A robustly optimized BERT pretraining approach. ArXiv preprint arXiv:1907.11692.

McGuffie, K. and A. Newhouse. 2020. The radicalization risks of GPT-3 and advanced neural language models. ArXiv preprint arXiv:2009.06807.

Olteanu, A., F. Diaz, and G. Kazai. 2020. When are search completion suggestions problematic? *CSCW*.

Radford, A., J. Wu, R. Child, D. Luan, D. Amodei, and I. Sutskever. 2019. Language models are unsupervised multitask learners. OpenAI tech report.

Schuster, M. and K. Nakajima. 2012. Japanese and korean voice search. *ICASSP*.

Sheng, E., K.-W. Chang, P. Natarajan, and N. Peng. 2019. The woman worked as a babysitter: On biases in language generation. *EMNLP*.

Taylor, W. L. 1953. Cloze procedure: A new tool for measuring readability. *Journalism Quarterly*, 30:415–433.

Williams, A., N. Nangia, and S. Bowman. 2018. A broad-coverage challenge corpus for sentence understanding through inference. *NAACL HLT*.

Zhu, Y., R. Kiros, R. Zemel, R. Salakhutdinov, R. Urtasun, A. Torralba, and S. Fidler. 2015. Aligning books and movies: Towards story-like visual explanations by watching movies and reading books. *IEEE International Conference on Computer Vision*.