Exploring Attention Based Model for Captioning Images

par Kelvin Xu

Département d’informatique et de recherche opérationnelle
Faculté des arts et des sciences

Mémoire présenté à la Faculté des arts et des sciences
en vue de l’obtention du grade de Maitre ès sciences (M.Sc.)
en informatique

Août, 2017

© Kelvin Xu, 2017.
Comprendre ce qu’il y a dans une image est l’enjeu primaire de la vision par ordinateur. Depuis 2012, les réseaux de neurones se sont imposés comme le modèle de facto pour de nombreuses applications d’apprentissage automatique. Inspirés par les récents travaux en traduction automatique et en détection d’objet, cette thèse s’intéresse aux modèles capables de décrire le contenu d’une image et explore comment la notion d’attention peut être paramétrisée par des réseaux de neurones et utilisée pour la description d’image.

Cette thèse présente un réseau de neurones basé sur l’attention qui peut décrire le contenu d’images, et explique comment apprendre ce modèle de façon déterministe par backpropagation ou de façon stochastique avec de l’inference variationnelle ou de l’apprentissage par renforcement.

Étonnamment, nous montrons que le modèle apprend automatiquement à concentrer son attention sur les objets correspondant aux mots dans la phrase prédite. Cette notion d’attention obtient l’état de l’art sur trois benchmarks: Flickr9k, Flickr30k et MS COCO.

**Mots-clés:** réseaux de neurones, generation de description, apprentissage profond, apprentissage de representations, apprentissage supervisé, inference variationnelle, apprentissage par renforcement, attention, modelisation de données séquentielles
Summary

Understanding the content of images is arguably the primary goal of computer vision. Beyond merely saying what is in an image, one test of a system’s understanding of an image is its ability to describe the contents of an image in natural language (a task we will refer to in this thesis as “image captioning”).

Since 2012, neural networks have exploded as the de facto modelling tool for many important applications in machine learning. Inspired by recent work in machine translation and object detection, this thesis explores such models that can describe the content of images. In addition, it explores how the notion of “attention” can be both parameterized by neural networks and usefully employed for image captioning.

More technically, this thesis presents a single attention based neural network that can describe images. It describes how to train such models in a purely deterministic manner using standard backpropagation and stochastically by considering techniques used in variational inference and reinforcement learning. Surprisingly, we show through visualization how the model is able to automatically learn an intuitive gaze of salient objects corresponding to words in the output sequence. We validate the use of an attention based approach with state-of-the-art performance on three benchmark datasets: Flickr9k, Flickr30k and MS COCO.

Keywords: neural networks, caption generation, deep learning, representation learning, supervised learning, variational inference, reinforcement learning, attention, sequence modelling
# Table des matières

Summary ................................................................. ii

Summary ................................................................. iii

Contents ................................................................. iv

List of Figures .......................................................... vi

List of Tables ........................................................... viii

List of Abbreviations ................................................... ix

Acknowledgments ......................................................... x

1 **Introduction** ......................................................... 1
   1.1 Why machine learning is a good idea .......................... 1
   1.2 Introduction to Neural Networks ................................. 2
      1.2.1 Notation .................................................. 2
      1.2.2 FeedForward Models ...................................... 3
      1.2.3 Supervised Learning with Backpropagation .............. 5
   1.3 Modeling Sequences with Recurrent Models .................. 6
      1.3.1 “Vanilla” Recurrence ..................................... 7
      1.3.2 Long Term Dependencies and LSTMs .................... 9
      1.3.3 Some inspirational notes on human attention .......... 10
   1.4 Helpful tricks for training neural networks ................. 13
      1.4.1 Initialization ............................................. 14
      1.4.2 Adaptive Learning Rate Algorithms .................... 14
      1.4.3 Dropout .................................................. 15

2 **Prologue to the Article** .......................................... 17

3 **Show, Attend and Tell: Neural Image Caption Generation with Visual Attention** ........................................... 18
   3.1 Introduction ..................................................... 18
   3.2 Related Work .................................................... 20
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3</td>
<td>Image Caption Generation with Attention Mechanism</td>
<td>21</td>
</tr>
<tr>
<td>3.3.1</td>
<td>Model Details</td>
<td>21</td>
</tr>
<tr>
<td>3.4</td>
<td>Learning Stochastic “Hard” vs Deterministic “Soft” Attention</td>
<td>24</td>
</tr>
<tr>
<td>3.4.1</td>
<td>Stochastic “Hard” Attention</td>
<td>25</td>
</tr>
<tr>
<td>3.4.2</td>
<td>Deterministic “Soft” Attention</td>
<td>27</td>
</tr>
<tr>
<td>3.4.3</td>
<td>Training Procedure</td>
<td>29</td>
</tr>
<tr>
<td>3.5</td>
<td>Experiments</td>
<td>30</td>
</tr>
<tr>
<td>3.5.1</td>
<td>Data</td>
<td>30</td>
</tr>
<tr>
<td>3.5.2</td>
<td>Evaluation Procedures</td>
<td>31</td>
</tr>
<tr>
<td>3.5.3</td>
<td>Quantitative Analysis</td>
<td>32</td>
</tr>
<tr>
<td>3.5.4</td>
<td>Qualitative Analysis: Learning to attend</td>
<td>32</td>
</tr>
<tr>
<td>3.6</td>
<td>Conclusion</td>
<td>33</td>
</tr>
<tr>
<td>4</td>
<td>Epilogue</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td>Bibliography</td>
<td>37</td>
</tr>
<tr>
<td>Figure</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>A illustration of a single hidden unit. The input is a vector $\mathbf{x} = {x_1, x_2, ..., x_d}$ which is transformed by a weight vector $\mathbf{w} = {w_1, w_2, ..., w_d}$ and bias $b$. (Figure from Hugo Larochelle’s course on deep learning)</td>
<td></td>
</tr>
<tr>
<td>1.2</td>
<td>A neural net is composed for a number of hidden layers that transform the input distribution to the output through a progressive series of computations. In the above image, each node is a single scalar value representing a unit of the hidden layer. Each edge is a single scalar weight transforming the values of the preceding layer.</td>
<td></td>
</tr>
<tr>
<td>1.3</td>
<td>The Mark I Perceptron machine created at the Cornell Aeronautical Laboratory was the first physical implementation of the perceptron algorithms. Using visible features on a patchboard, it allowed the model to adaptively learn different combinations of weights via arrays of potentiometers. (Source: Cornell Library)</td>
<td></td>
</tr>
<tr>
<td>1.4</td>
<td>An unrolled RNN for $T = 4$ timesteps (Figure from Chris Olah’s blog on deep learning Olah (2015))</td>
<td></td>
</tr>
<tr>
<td>1.5</td>
<td>An illustration of an LSTM cell, where $x_t$ is the input, $i_t$ is the “input” gate, $o_t$ is the “output” gate, $c_t$ is the “memory cell”, $f_t$ is the “forget” gate and finally, $h_t$ is the output of the cell. The subscript $t$ refers to an individual time step. The above diagram is drawn with the common peep-hole connections where the input and forget gate are also conditioned on the previous cell memory and the output gate is conditioned on the current cell memory.</td>
<td></td>
</tr>
<tr>
<td>1.6</td>
<td>An example of the importance of bottom up image features for saliency. In this video game, the importance of the agent causes attention to be focused consistently on the character regardless of circumstance. (Figure from Itti and Koch (2001))</td>
<td></td>
</tr>
<tr>
<td>1.7</td>
<td>A cartoon illustration of a sequence of glances that one might take to classify this digit as a ‘2’. Clearly something smarter can be done than doing a raster-like scan (Figure from Hugo Larochelle)</td>
<td></td>
</tr>
<tr>
<td>1.8</td>
<td>A illustration of the process of foveation. Instead of scanning each part of the image, at each glimpse, salient features of the digit are extracted (Figure from Hugo Larochelle)</td>
<td></td>
</tr>
</tbody>
</table>
1.9 “The Unexpected Visitor”: a classical psychological study tracking the eye movements of a scene. Clearly as the task changes the gaze changes, indicating that the attention process is top down. . . . . . 13

1.10 Dropout illustration (Figure illustrating the process of dropout. Left: a fully connected network, Right: after dropout where with probability $p$, a node in a layer is dropped. This dropping operation is performed for every mini-batch Srivastava et al. (2014)) . . . . . . . 16

3.1 Our model learns a words/image alignment. The visualized attentional maps (3) are explained in Sections 3.3.1 & 3.5.4 . . . . . . . 19

3.2 A LSTM cell, lines with bolded squares imply projections with a learnt weight vector. Each cell learns how to weigh its input components (input gate), while learning how to modulate that contribution to the memory (input modulator). It also learns weights which erase the memory cell (forget gate), and weights which control how this memory should be emitted (output gate). . . . . . . . . . . . . . . . 22

3.3 Visualization of the attention for each generated word. The rough visualizations obtained by upsampling the attention weights and smoothing. (top) “soft” and (bottom) “hard” attention (note that both models generated the same captions in this example). . . . . . . . . . . . . . . . . . . . 25

3.4 Examples of attending to the correct object (white indicates the attended regions, underlines indicated the corresponding word) . . . . . . 30

3.5 Examples of mistakes where we can use attention to gain intuition into what the model saw. . . . . . . . . . . . . . . . . . . . . . . . . . 31

4.1 Figure from Lu et al. (2016). in their approach, they provide skip connections by which the generation can be done without using the image features. This intuitively makes sense for generating words which do not have a visual meaning (e.g, 'to', 'a', 'etc') . . . . . . . 34

4.2 Figure from You et al. (2016). In their approach, they combine RNN based generation of captions using both image features and attention over semantic concepts extracted from the training set. . . . . . . . 35

4.3 figure from Anderson et al. (2017). in their approach, they combine rnn based generation of captions with the faster r-cnn framework which consists of a region proposal step followed by a feature extraction step. attention is done over the different proposed regions which allows for intuitive visualization . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 36
3.1 BLEU-1,2,3,4/METEOR metrics compared to other methods, † indicates a different split, (—) indicates an unknown metric, ◦ indicates the authors kindly provided missing metrics by personal communication, Σ indicates an ensemble, a indicates using AlexNet
# List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AE</td>
<td>Auto-Encoder</td>
</tr>
<tr>
<td>ANN</td>
<td>Artificial Neural Network</td>
</tr>
<tr>
<td>BN</td>
<td>Batch Normalization</td>
</tr>
<tr>
<td>CE</td>
<td>Cross Entropy</td>
</tr>
<tr>
<td>DAE</td>
<td>Denoising Auto-Encoder</td>
</tr>
<tr>
<td>I.I.D</td>
<td>Independent and Identically Distributed</td>
</tr>
<tr>
<td>ReLU</td>
<td>Rectified Linear Unit</td>
</tr>
<tr>
<td>MLP</td>
<td>Multi-Layer Perceptron</td>
</tr>
<tr>
<td>MSE</td>
<td>Mean Squared Error</td>
</tr>
<tr>
<td>NLL</td>
<td>Negative Log-Likelihood</td>
</tr>
<tr>
<td>ReLU</td>
<td>Rectified Linear Unit</td>
</tr>
<tr>
<td>SGD</td>
<td>Stochastic Gradient Descent</td>
</tr>
</tbody>
</table>
Acknowledgments

First and foremost, I would like to thank my advisors Prof. Yoshua Bengio and Prof. Aaron Courville for the privilege of spending two very special years in my life as part of MILA. It has been amazing to see not only the impact that they have had on the ML research community, but also on the lives of the people in MILA and the city of Montreal. I could not have wished for two better role models in my life.

I would also like to thank my labmates for providing such a nice environment to do research and extend a special thanks to Kyunghyun Cho for his constant support and mentorship. This thesis would also not have been possibly without my collaborators Jamie Kiros, Jimmy Ba, Prof. Ruslan Salakhutdinov, and Prof. Richard Zemel. Finally, I would like to thank my family and M.H. for support.
1 Introduction

1.1 Why machine learning is a good idea

A vast majority of computing is devoted to the study of computational “recipes”. Given some input, the goal is to determine what sequence of computations steps will consistently produce the required output. Whether it is determining what restaurant is closest to you, or what book to recommend online, an important caveat is that such a program will have to be able to run efficiently on a real computer. As a result, a lot of computer science is devoted to understanding when such efficient recipes exist and when they can be applied.

While a vast majority of the remarkable applications of computing we interact with operate on this simple principle, a natural question is what can be done when no efficient recipe is known. Surprisingly, many of the problems that fall into this category are ones that humans take for granted such as the ability to quickly comprehend a visual scene or pick out a friend’s voice in a crowd. Clearly, these are abilities that we would expect smart computers to have. The question then becomes figuring out what strategies we can employ when, given an input, there is no simple way to determine the desired output?

The core idea of machine learning is to instead take an alternative approach. Rather than trying to provide a model with its own recipe, it attempts instead to provide a “learning” algorithm for how a computer can derive its own algorithmic solution. This approach not only has the appeal of being intrinsically more scalable, it also allows the computer to learn it’s own understanding of the data (i.e., salient features or “representations”).

In the last few years, the dominant approach that has come to the forefront of machine learning has been to use “deep neural networks”. As the name suggests, the technique very loosely refers to human inspired “neurons”. Unlike simple linear models with are not very expressive, neural networks can be thought of as highly
nonlinear models, capable of learning progressively more abstract representations of high dimensional data. Recent years have seen an explosion of interest in these techniques due to their widespread successes in a variety of disparate domains (vision, speech, natural language processing, etc.). In this thesis, we will focus on the particular problem of image caption generation which is the problem of providing a descriptive sentence for an image. To this end, this thesis will tie together advances in recurrent neural networks, machine translation, reinforcement learning and in particular, by explicitly modeling the process of human attention, take inspiration from the way humans solve image captioning.

1.2 Introduction to Neural Networks

1.2.1 Notation

In the sections to follow, scalar values \((e.g.\ x, y, z)\) will be written in lower case italic font. Vectors (\(e.g.\) those residing in \(\mathbb{R}^n\)) will be written in bold lower case font (\(e.g.\ \mathbf{x}, \mathbf{y}, \mathbf{z}\)). Matrices (\(\mathbb{R}^{n \times m}\)) will be written in bold upper case roman font (\(e.g.\ \mathbf{E}, \mathbf{U}, \mathbf{W}\)). An element-wise product (also known as the Hadamard Product or Schur Product) will be denoted with the following \(\odot\). All quantities are real valued unless noted otherwise.
Figure 1.2 – A neural net is composed for a number of hidden layers that transform the input distribution to the output through a progressive series of computations. In the above image, each node is a single scalar value representing a unit of the hidden layer. Each edge is a single scalar weight transforming the values of the precedent layer.

1.2.2 FeedForward Models

The basic idea of neural networks is that it is possible to construct a very nonlinear function approximator that has parameters which can be tuned by gradient descent. Perhaps the simplest and most widely used architecture of a neural network is a feedforward network. Feedforward neural networks have made huge advances in a broad range of important applications, most notably, speech recognition and image classification Dahl et al. (2012); Krizhevsky et al. (2012). Formally, it is composed of $l$ layers of a weight matrix $W_i$, bias $b_i$, and a nonlinear activation function $f : \mathbb{R}^n \mapsto \mathbb{R}^n$ applied element-wise. Common non-linearities include $tanh(x) = \frac{e^{2x} - 1}{e^{2x} + 1}$, $\sigma = \frac{1}{1+e^{-x}}$, or rectified linear units (ReLu = $\max(0, x)$).

**Algorithm 1** feedforward network

1: Given an input example $x$
2: Set $z_1 = x$
3: for $i = 1 \ldots l$ do
4:  \hspace{1em} $h_i = f(W_i z_1 + b_i)$
5:  \hspace{1em} $z_{i+1} = h_i$
6: end for
7: Return output $z_l$

From this, we can make two important observations. First, the input-output relationship we can model is constrained by the topological connections between
the “neurons”, and second that the relationships are encoded in the weights matrices which progressively transform the data. These weights are typically initially set with random values and adjusted by learning algorithms to improve the performance although it is also possible to use weights from a previous task.

Despite recent resurgence of interest, neural networks are a remarkably old idea, with the first analysis dating back to work by McCulloch and Pitts (1943) who first tried to understand how a simplified model of a neuron could implement certain logical circuits. This work was followed by seminal work on the perceptron algorithm at the Cornell Aeronautical Laboratory by Frank Rosenblatt (Rosenblatt, 1957), which introduced a simple learning rule to train signal layer neural networks referred to as Perceptron models. The promise of self-learning circuits prompted a great deal of enthusiasm. In 1958, the New York Times reported that “[the perceptron is ]the embryo of an electronic computer that [the American Navy]expects will be able to walk, talk, see, write, reproduce itself and be conscious of its existence” (Olazaran, 1996).
It was proved however that such models could only recognize linearly separable patterns, and in a well-known book by Marvin Minsky and Seymour Papert (Minsky and Papert, 1969), it was proved that such models could not learn a XOR function, no matter how much data or computation it was given. The perceived limitations of Perceptron model led to a sharp decline of neural network related research. This almost decade long hiatus in major interest (and funding) is sometimes referred to as the “AI Winter”. It was not until the mid-1980s when David Rumelhart, along with Geoffrey Hinton and Ronald Williams, showed that multi-layer neural networks could be trained effectively with “backpropagation” (Rumelhart et al., 1986).

The term “deep” is meant to refer to the fact that the network was composed of more than one hidden layer. A major benefit of this variant of network over perceptron models is the fact that it can be proved that every continuous function, mapping compact real valued intervals to other real valued intervals of outputs could be approximated with arbitrary precision by a multi-layer sigmoid neural network. This finding (Cybenko, 1988), often referred to as the universal approximation theorem, gives no hints however as to how to set or adjust the weights of the networks, nor does it say anything about how the topology of the networks should be constrained. The study of these questions is in some sense the essence of modern day deep learning research.

1.2.3 Supervised Learning with Backpropagation

One of the major historical breakthroughs was the discovery that “backpropagation”, which can be seen as an application of the chain rule, could provide a simple, efficient and sufficient recipe for learning the weights of a “deep” neural network. While there is long standing controversy over who “invented” backpropagation, the demonstration by Rumelhart et al. (Rumelhart et al., 1986) that it could effectively train multi-layer neural networks undoubtedly was a major catalyst for subsequent research in training neural networks with backpropagation.

Concretely, backpropagation relies upon the chain rule from calculus and use backward differentiation. In order to learn a supervised mapping $\mathbf{x} \rightarrow \mathbf{y}$ (where $\mathbf{x} \in \mathbb{R}^i$ and $\mathbf{y} \in \mathbb{R}^m$), we define a scalar loss function $L(\mathbf{z}_l, \mathbf{y})$ which is a function of the groundtruth $\mathbf{y} \in \mathbb{R}^m$. Next we compute the gradients with respect to parame-
ters \(W_i, b_i\) for \(i = 1, \ldots, l\). We can use the chain rule described below to compute the gradient direction to follow.

**Algorithm 2** Backpropagation

1: Given differentiable loss function \(\frac{\partial L(x, y)}{\partial z_i}\)
2: for \(i = l \ldots 2\) do
3: \(\partial h_i = f'(h_i) \cdot \partial z_i\)
4: \(\partial z_{i-1} = W^T_{i-1} \partial h_i\)
5: \(\partial b_i = \partial h_i\)
6: \(\partial W_{i-1} = \partial x; z^T_{i-1}\)
7: end for
8: Return output \([\partial W_1, \partial b_1, \ldots, \partial W_l, \partial b_l]\)

Given the gradient information returned by Algorithm 2, it becomes possible to take a step on the weights \(W_i, b_i\) for \(i = 1, \ldots, l\) in the direction that approximately minimizes the error. In recent years however, machine learning research has had to increasingly focus on large scale learning problems with datasets that can have billions of training cases. In this setting, computing the gradient for the entire dataset becomes computationally expensive. Instead, stochastic approximation techniques belonging to the class of Robbins-Monro algorithms Robbins and Monro (1951) are typically used. These “stochastic” gradient descent algorithms process a mini-batch of data at every iteration. These model parameters are updated by taking noisy gradient steps estimated by randomly sampled mini-batches. These methods rapidly improve the efficiency of gradient descent methods and form the basis of many of the modern adaptive learning rate algorithms that are used in the vast majority of applications (Tieleman and Hinton, 2012; Kingma and Ba, 2014).

### 1.3 Modeling Sequences with Recurrent Models

When considering variable length data, one of the weaknesses of feedforward networks is the necessity to fix the dimension of the input \((x)\) \textit{a priori}. This requirement can be a significant weakness when modeling naturally variable length sequences such as sentences, audio, or video (\textit{i.e.} a time series \((x_1, x_2, \ldots, x_T))\). The
Figure 1.4 – An unrolled RNN for $T = 4$ timesteps (Figure from Chris Olah’s blog on deep learning Olah (2015))

importance of modeling such relationships is clear in natural language processing. Consider the following sentence: “In Montreal, people speak __”. Modeling the temporal information between the first part of the sentence can help us make complex prediction. In fact, depending on the reader’s own biological neural network, the answer could have been either “French”, “English” or maybe even “Québécois”.

The pervasive need for modeling this type of data motivates what is known as recurrent neural networks (RNNs), which are neural network architectures that incorporate temporal structure to model sequences. Intuitively, they can be understood as a structure that maintains an internal “hidden” representation over time and at every time step decides how to incorporate new data points and produce output.

1.3.1 “Vanilla” Recurrence

The simplest variant of recurrent neural network consists of a hidden state $h_t \in \mathbb{R}^h$ for $t = 1, \ldots, T$ and a series of weights matrices and biases $(W_{hx}, W_{hh}, W_{ho}, b_h, b_o)$ which is shared across time. The role of the weight matrices/biases is to control the interaction between the input, output and previous hidden state so as to propagate information forward and produce the desired outputs. Surprisingly, such models, while conceptually simple, are in fact provably turing complete (Siegelmann and Sontag, 1995).
Algorithm 3 Recurrent Neural Networks

1: Given input sequence \((x_1, \ldots, x_t)\)
2: Given weights \([W_{hx}, W_{hh}, W_{ho}, b_h, b_o]\) and initial hidden state \(h_0\)
3: for \(t = 1 \ldots T\) do
4: \(a_t = W_{hx}x_t + W_{hh}h_{t-1} + b_h\)
5: \(h_t = f(a_t)\)
6: \(o_t = W_{ho}h_t + b_o\)
7: end for

Suppose we are given a sequence of inputs \(x_t\) of length \(T\). If we restrict ourself to a vocabulary (i.e., the set of possible values that \(x_t\) can take) of size \(K\), we can represent it with a \(K\) dimensional vector where only the \(k\)-th entry is 1. Then, by the chain rule of probability we can represent \(\text{Pr}(x_{t+1}|o_t)\) as the following.

\[
\text{Pr}(x_{t+1}^k = 1|o_t) = \frac{\exp \alpha_t^k}{\sum_{k' = 1}^K \exp \alpha_t^{k'}} \quad (1.1)
\]

Note we have assumed here that \(o_t\) is also of dimension \(K\), but if not we can linearly project it with matrix \(W_{ox}\). Next we can define a loss over the parameters of the neural network with the maximum likelihood objective.

\[
\mathcal{L}(x) = - \sum_{t=1}^T \log \text{Pr}(x_{t+1}|o_t) \quad (1.2)
\]

\[
= - \sum_{t=1}^T \log o_t^{x_{t+1}} \quad (1.3)
\]

The gradient of this has an intuitive form.

\[
\frac{\partial \mathcal{L}(x)}{\partial o_t^k} = o_t^k - \delta_{k,x_{t+1}} \quad (1.4)
\]

Using gradient descent, all the parameters of the model can be optimized jointly using mini-batch gradient descent. At test time, we can decode from the model either by sampling from the probability distribution defined by the model. Alternatively, we can try to find the probable sequence through approximate inference methods such as beam search.
Here, we have very subtly introduced a practical challenge. Namely, we have assumed that we can put all the tokens in the universe of what we are modeling into a dictionary of vocabulary size $K$. Choosing this $K$ correctly has strong practical implications, as having a large value of $K$ will cause lead to a large memory requirement while selecting a small number will limit the number of tokens being modelled (Mnih and Hinton, 2009; Jean et al., 2014; Morin and Bengio, 2005).

### 1.3.2 Long Term Dependencies and LSTMs

One issue with learning recurrent models is the phenomena often referred to as “the difficulty of learning long-term dependencies”. Informally speaking, in a learning setting where there exist large time delays between inputs and outputs, it is difficult to determine which inputs/decisions ultimately led to positive or negative outcomes.

Hochreiter (1991) formally showed that in typical deep or recurrent networks, backpropagated error gradients would either shrink exponentially in the number of layers or explodes. Similarly, considering a dynamical system that used attractor states as memory to store information, Bengio et al. (1993) showed that for such systems, either the memory would not be robust to noise or would have gradients that would go to zero as the time horizon increased to infinity.

This realization motivated the investigation into variants of recurrent models employing gating units with a form of persistent memory which prevented frequent read and writes. While these type of models do not completely solve the problem of long term credit assignment, they make credit assignment possible over sufficiently long scales to perform many applications. In fact, almost all the practical successes of recurrent models come from the family of gated recurrent models. The earliest and still most popular form of gated recurrent neural network are “long-short term memory” cells, which were introduced by Hochreiter & Schmidhuber (Hochreiter and Schmidhuber, 1997).

The key idea behind LSTMs that it preserves a memory state $c_t$ which it gets selectively written to. Intuitively, at every step and input and forget gate are computed with sigmoidal nonlinearities (i.e being bound between zero and one to represent maximum ‘forgetting’ and ‘input’) which are used to gate the amount written and forgotten from the cell. Next, the output gate is computed which determines which
Figure 1.5 – An illustration of an LSTM cell, where $x_t$ is the input, $i_t$ is the “input” gate, $o_t$ is the “output” gate, $c_t$ is the “memory cell”, $f_t$ is the “forget” gate and finally, $h_t$ is the output of the cell. The subscript $t$ refers to an individual time step. The above diagram is drawn with the common peep-hole connections where the input and forget gate are also conditioned on the previous cell memory and the output gate is conditioned on the current cell memory.

Part of the output should get written. In equation form, this looks like the following:

$$
i_t = \sigma(W_i E x_t + U_i h_{t-1} + b_i),$$
$$f_t = \sigma(W_f E x_t + U_f h_{t-1} + b_f),$$
$$c_t = f_t \odot c_{t-1} + i_t \odot \tanh(W_c E x_t + U_c h_{t-1} + b_c),$$
$$o_t = \sigma(W_o E x_t + U_o h_{t-1} + b_o),$$
$$h_t = o_t \odot \tanh(c_t).$$

where $\tanh$ denotes the hyperbolic tangent function $\tanh(x) = \frac{e^{2x} - 1}{e^{2x} + 1}$.

1.3.3 Some inspirational notes on human attention

Typically in most of computer vision, every part of the image is treated the same. No part of the image gets “extra” computation. In some ways, this is a sensible default approach because the task of determining which part of an image deserves “extra” computation is itself a challenging problem.

One curious aspect of the way humans deal with visual problems is the notion of “attention”. When given an image, our eyes pick out key points, scanning the image focusing on the most “salient” aspects. In this thesis, we would like to take
some inspiration from how human’s do a visual task, and in this section discuss some modelling cues we can take human attention.

![Image](image.png)

**Figure 1.6** – An example of the importance of bottom up image features for saliency. In this video game, the importance of the agent causes attention to be focused consistently on the character regardless of circumstance. (Figure from Itti and Koch (2001))

1) **Attention is a sequential decision making process**

One of the main observations we can make is that attention is a sequential procedure. Namely, when we glance over an image, we make a series of gazes which are determined by what we have already seen. In particular, on the right of Figure 1.7, we see a toyish example of exactly what a human would not do.

2) **Spatial Focus**

In trying to recognize that the image is in fact a 2, it is extremely unnatural to follow the pattern in the image. Instead, focus is given in a way much closer to Figure 1.8. Another note then is that attention has a spatial focus, whereby certain regions of the image are more in focus than other portions (sometimes referred to as foveation). This weights the contribution of individual regions with pertinent information (the contours of the digit in this example), more than other areas which are less relevant (e.g. the empty background).

3) **Top Down and Bottom Up Models**

Unsurprisingly, attention is bottom up in the sense that it relies heavily on the stimulus in the image Itti and Koch (2001). It is also top down in the sense that it heavily relies on the task at hand. A classical example of this is the study of the unexpected visitor Yarbus (1967), which is an early psychological experiment on the effect of a specified task on the eye movements of a human. As can be seen in
Fig. 1.9, in each of the scenes a different task is given with results in a different series of saccades being produced.

Figure 1.7 – A cartoon illustration of a sequence of glances that one might take to classify this digit as a ‘2’. Clearly something smarter can be done than doing a raster-like scan (Figure from Hugo Larochelle)

Figure 1.8 – A illustration of the process of foveation. Instead of scanning each part of the image, at each glimpse, salient features of the digit are extracted (Figure from Hugo Larochelle)
1.4 Helpful tricks for training neural networks

It is hard to overstate the importance of the small details that make neural networks work. For a long time, the consensus was that neural network models were difficult to optimize because of the problem of local minima and their highly nonlinear behaviour. This, coupled with a lack of understanding of deep networks from a theoretical perspective historically has led many researchers to abandon neural networks in favor of better understood models with theoretical guarantees such as support vector machines. From around 2006, there was a revival of interest in deep learning research largely due to advanced made from “pre-training” Hinton and Salakhutdinov (2006), but eventually, it was discovered this was not necessary with enough labeled data or even careful initialization. Many other tricks, such as the use of adaptive learning rates and regularization techniques such as dropout and batch normalization have significantly improved the reliability and performance of deep neural networks.
Thus, this thesis would be in some sense incomplete without some notes on practical tricks for training neural networks. Simple differences such as choice of initialization can drastically change a larger experimental picture. Often, these differences are more critical than the improvement proposed in any given paper. While not meant to be exhaustive, this section covers a collection of these useful tricks which were used in this paper.

1.4.1 Initialization

While pre-training as a technique has a long history of being helpful for training deep neural networks, for most moderately sized datasets, it is sufficient to start with the right random initialization. A major pitfall would be to initialize the weights of a network to be all zeros. As it turns out, such a model would have the same output for every neuron and thus the same gradient update. Thus, to break this symmetry, it is important to have the model initialized to small random numbers (small to avoid saturating zones of common non-linearities to which restrict gradient flow). Typically, this is done by sampling from a normal distribution $W \sim N(0, \sigma^2)$ where $\sigma$ is chosen to be on the order of less than $10^{-1}$.

There has been work analysing the moments (i.e. mean/variance) of randomly initialized feedforward networks for sigmoid/tanh activation Glorot and Bengio (2010) and ReLu activations He et al. (2015). The most popular initialization strategies are from these two preceding papers. Either with the ‘Glorot Initialization’ for tanh/sigmoid activations $\sigma^2 = \frac{2}{n_{in} + n_{out}}$ (where $n_{in}$ and $n_{out}$ are the number of units in the input layer and next layer respectively or $\sigma^2 = \frac{2}{n}$ (where $n$ is the number of units in the layer) for ReLU activations.

1.4.2 Adaptive Learning Rate Algorithms

When using gradient based optimization methods, it is often important to choose a sufficiently small learning (aka step size) to ensure stability. One intuitive way to see this is that the gradient information only gives a local direction to improve an objective and does not take into account any of the potential curvature which exists for complicated non-convex functions.

While a number of methods have been developed to account for second order information Martens (2010). These methods typically take more time to compute
Algorithm 4 Adam, pseudocode from the original paper. $g_t^2$ indicates the element-wise square $g_t \odot g_t$. Good default settings for the tested machine learning problems are $\alpha = 0.001$, $\beta_1 = 0.9$, $\beta_2 = 0.999$ and $\epsilon = 10^{-8}$. All operations on vectors are element-wise. With $\beta_1^t$ and $\beta_2^t$ we denote $\beta_1$ and $\beta_2$ to the power $t$.

Require: $\alpha$: Stepsize
Require: $\beta_1, \beta_2 \in [0, 1)$: Exponential decay rates for the moment estimates
Require: $f(\theta)$: Stochastic objective function with parameters $\theta$
Require: $\theta_0$: Initial parameter vector

$m_0 \leftarrow 0$ (Initialize 1st moment vector)
$v_0 \leftarrow 0$ (Initialize 2nd moment vector)
$t \leftarrow 0$ (Initialize timestep)

while $\theta_t$ not converged do
  $t \leftarrow t + 1$
  $g_t \leftarrow \nabla_{\theta} f_t(\theta_{t-1})$ (Get gradients w.r.t. stochastic objective at timestep $t$)
  $m_t \leftarrow \beta_1 \cdot m_{t-1} + (1 - \beta_1) \cdot g_t$ (Update biased first moment estimate)
  $v_t \leftarrow \beta_2 \cdot v_{t-1} + (1 - \beta_2) \cdot g_t^2$ (Update biased second raw moment estimate)
  $\hat{m}_t \leftarrow m_t / (1 - \beta_1^t)$ (Compute bias-corrected first moment estimate)
  $\hat{v}_t \leftarrow v_t / (1 - \beta_2^t)$ (Compute bias-corrected second raw moment estimate)
  $\theta_{t+1} \leftarrow \theta_{t-1} - \alpha \cdot \hat{m}_t / (\sqrt{\hat{v}_t} + \epsilon)$ (Update parameters)
end while

return $\theta_t$ (Resulting parameters)

and are tricky to implement in practice. This has motivated the development of adaptive learning rate algorithms to estimate curvature using only first order information. For example, the popular Adam/RMSPProp optimizer use running averages of the second movements of the gradient information which is an approximation of the diagonal of the Fisher Information matrix Pascanu and Bengio (2013).

Well tuned SGD methods with momentum can often perform comparably with such adaptive learning rate methods Wilson et al. (2017). Methods such as Adam/RMSPProp have remained popular like batchnorm however because of their general robustness across problems.

1.4.3 Dropout

Dropout is a popular technique for regularizing deep neural networks. The implementation of dropout is quite simple. During training, each hidden unit in the network is randomly dropped (masked to be zero). During testing time, to account for the fact that the model was trained with not all the units available at each
time, the output of each hidden unit is rescaled to account for the fact that units were not always present. The main hyper-parameter here is the probability that each unit is “dropped”. To illustrate, if each unit was dropped with probability 0.5, then at test time all the outputs are halved. This quite surprising regularization method was presented without real mathematical justification, but was shown to be empirically effective. One of the intuitions as to why dropout works was given in the original paper Srivastava et al. (2014). Simply put, because each unit was not always available during training, it prevented each unit from relying on other units, which was referred to in the original paper Srivastava et al. (2014) as co-adaptation.

Since the original paper, due to the success of dropout as a regularizer, numerous explanations have been put forth to explain the success of dropout due to it being a scale invariant regularizer Wang and Manning (2013) or as an implicit Bayesian method (Gal and Ghahramani, 2016).

**Figure 1.10** — Dropout illustration (Figure illustrating the process of dropout. Left: a fully connected network, Right: after dropout where with probability $p$, a node in a layer is dropped. This dropping operation is performed for every mini-batch Srivastava et al. (2014))
Prologue to the Article


Personal Contribution: The idea to apply attention based models developed in machine translations to image captioning came from Jamie (Ryan) Kiros. I performed the majority of the experimental work with guidance from Kyunghyun Cho and Jamie Kiros. Jamie Kiros helped most in placing this work in the context of previous work in image captioning/multimodal learning. The hard-attention experiments were performed by Jimmy Lei Ba building upon the original code we wrote. I did the majority of the paper writing in preparation for publication, with valuable input from my advisors Prof. Yoshua Bengio, Prof. Aaron Courville, Prof. Ruslan Salakhutdinov, and Prof. Richard Zemel.

The underlying work of this thesis made use of the Theano library (Bergstra et al., 2010; Bastien et al., 2012) to which we (the authors) and many others in the community owe a great debt. We also acknowledge the support of the following organizations for research funding and computing support: NSERC, Samsung, NVIDIA, Calcul Québec, Compute Canada, the Canada Research Chairs and CIFAR. The authors would also like to thank Nitish Srivastava for assistance with his ConvNet package as well as preparing the Oxford convolutional network and Relu Patrascu for helping with numerous infrastructure-related problems.
3.1 Introduction

Automatically generating captions for an image is a task close to the heart of scene understanding — one of the primary goals of computer vision. Not only must caption generation models be able to solve the computer vision challenges of determining what objects are in an image, but they must also be powerful enough to capture and express their relationships in natural language. For this reason, caption generation has long been seen as a difficult problem. It amounts to mimicking the remarkable human ability to compress huge amounts of salient visual information into descriptive language and is thus an important challenge for machine learning and AI research.

Yet despite the difficult nature of this task, there has been a recent surge of research interest in attacking the image caption generation problem. Aided by advances in training deep neural networks (Krizhevsky et al., 2012) and the availability of large classification datasets (Russakovsky et al., 2014), recent work has significantly improved the quality of caption generation using a combination of convolutional neural networks (convnets) to obtain vectorial representation of images and recurrent neural networks to decode those representations into natural language sentences (see Sec. 3.2). One of the most curious facets of the human visual system is the presence of attention (Rensink, 2000; Corbetta and Shulman, 2002). Rather than compress an entire image into a static representation, attention allows for salient features to dynamically come to the forefront as needed. This is especially important when there is a lot of clutter in an image. Using representations (such as those from the very top layer of a convnet) that distill information in images to the most salient objects is one effective solution that has been widely adopted in previous work. Unfortunately, this has one potential drawback of losing information which could be useful for richer, more descriptive captions. Using lower-level
representation such as features from lower layers of a convolutional network can help preserve this information. However working with these features necessitates a powerful mechanism to steer the model to information important to the task at hand, and we show how learning to attend at different locations in order to generate a caption can achieve that. We present two variants: a “hard” stochastic attention mechanism and a “soft” deterministic attention mechanism. We also show how one advantage of including attention is the insight gained by approximately visualizing what the model “sees”. Encouraged by recent advances in caption generation and inspired by recent successes in employing attention in machine translation (Bahdanau et al., 2014) and object recognition (Ba et al., 2014; Mnih et al., 2014), we investigate models that can attend to salient part of an image while generating its caption.

The contributions of this paper are the following:

— We introduce two attention-based image caption generators under a common framework (Sec. 3.3.1): 1) a “soft” deterministic attention mechanism trainable by standard back-propagation methods and 2) a “hard” stochastic attention mechanism trainable by maximizing an approximate variational lower bound or equivalently by REINFORCE (Williams, 1992).

— We show how we can gain insight and interpret the results of this framework by visualizing “where” and “what” the attention focused on (see Sec. 3.5.4.)

— Finally, we quantitatively validate the usefulness of attention in caption generation with state-of-the-art performance (Sec. 3.5.3) on three benchmark datasets: Flickr8k (Hodosh et al., 2013), Flickr30k (Young et al., 2014) and the MS COCO dataset (Lin et al., 2014).
3.2 Related Work

In this section we provide relevant background on previous work on image caption generation and attention. Recently, several methods have been proposed for generating image descriptions. Many of these methods are based on recurrent neural networks and inspired by the successful use of sequence-to-sequence training with neural networks for machine translation (Cho et al., 2014; Bahdanau et al., 2014; Sutskever et al., 2014; Kalchbrenner and Blunsom, 2013). The encoder-decoder framework (Cho et al., 2014) of machine translation is well suited, because it is analogous to “translating” an image to a sentence.

The first approach to using neural networks for caption generation was proposed by Kiros et al. (2014) who used a multimodal log-bilinear model that was biased by features from the image. This work was later followed by Kiros et al. (2014) whose method was designed to explicitly allow for a natural way of doing both ranking and generation. Mao et al. (2014) used a similar approach to generation but replaced a feedforward neural language model with a recurrent one. Both Vinyals et al. (2014) and Donahue et al. (2014) used recurrent neural networks (RNN) based on long short-term memory (LSTM) units (Hochreiter and Schmidhuber, 1997) for their models. Unlike Kiros et al. (2014) and Mao et al. (2014) whose models see the image at each time step of the output word sequence, Vinyals et al. (2014) only showed the image to the RNN at the beginning. Along with images, Donahue et al. (2014) and Yao et al. (2015) also applied LSTMs to videos, allowing their model to generate video descriptions.

Most of these works represent images as a single feature vector from the top layer of a pre-trained convolutional network. Karpathy and Li (2014) instead proposed to learn a joint embedding space for ranking and generation whose model learns to score sentence and image similarity as a function of R-CNN object detections with outputs of a bidirectional RNN. Fang et al. (2014) proposed a three-step pipeline for generation by incorporating object detections. Their models first learn detectors for several visual concepts based on a multi-instance learning framework. A language model trained on captions was then applied to the detector outputs, followed by rescoring from a joint image-text embedding space. Unlike these models, our proposed attention framework does not explicitly use object detectors but instead learns alignments from scratch. This allows our model to go beyond
“objectness” and learn to attend to more flexible abstract concepts.

Prior to the use of neural networks for generating captions, two main approaches were dominant. The first involved generating caption templates which were filled in based on the results of object detections and attribute discovery (Kulkarni et al. (2013), Li et al. (2011), Yang et al. (2011), Mitchell et al. (2012), Elliott and Keller (2013)). The second approach was based on first retrieving similar captioned images from a large database then modifying these retrieved captions to fit the query (Kuznetsova et al., 2012, 2014). These approaches typically involved an intermediate “generalization” step to remove the specifics of a caption that are only relevant to the retrieved image, such as the name of a city. Both of these approaches have since fallen out of favour to the now dominant neural network methods.

There has been a long line of previous work incorporating the idea of attention into neural networks. Some that share the same spirit as our work include Larochelle and Hinton (2010); Denil et al. (2012); Tang et al. (2014) and more recently Gregor et al. (2015). In particular however, our work directly extends the work of Bahdanau et al. (2014); Mnih et al. (2014); Ba et al. (2014); Graves (2013).

### 3.3 Image Caption Generation with Attention Mechanism

#### 3.3.1 Model Details

In this section, we describe the two variants of our attention-based model by first describing their common framework. The key difference is the definition of the $\phi$ function which we describe in detail in Sec. 3.4. See Fig. 3.1 for the graphical illustration of the proposed model.

We denote vectors with bold font and matrices with capital letters. In our description below, we suppress bias terms for readability.
Figure 3.2 – A LSTM cell, lines with bolded squares imply projections with a learnt weight vector. Each cell learns how to weigh its input components (input gate), while learning how to modulate that contribution to the memory (input modulator). It also learns weights which erase the memory cell (forget gate), and weights which control how this memory should be emitted (output gate).

Encoder: Convolutional Features

Our model takes a single raw image and generates a caption $y$ encoded as a sequence of 1-of-$K$ encoded words.

$$y = \{y_1, \ldots, y_C\}, \ y_i \in \mathbb{R}^K$$

where $K$ is the size of the vocabulary and $C$ is the length of the caption.

We use a convolutional neural network in order to extract a set of feature vectors which we refer to as annotation vectors. The extractor produces $L$ vectors, each of which is a $D$-dimensional representation corresponding to a part of the image.

$$a = \{a_1, \ldots, a_L\}, \ a_i \in \mathbb{R}^D$$

In order to obtain a correspondence between the feature vectors and portions of the 2-D image, we extract features from a lower convolutional layer unlike previous work which instead used a fully connected layer. This allows the decoder to selectively focus on certain parts of an image by weighting a subset of all the feature vectors.
Decoder: Long Short-Term Memory Network

We use a long short-term memory (LSTM) network (Hochreiter and Schmidhuber, 1997) that produces a caption by generating one word at every time step conditioned on a context vector, the previous hidden state and the previously generated words. Our implementation of LSTMs, shown in Fig. 3.2, closely follows the one used in Zaremba et al. (2014):

\[
\begin{align*}
    i_t &= \sigma(W_i E y_{t-1} + U_i h_{t-1} + Z_i \hat{z}_t + b_i), \\
    f_t &= \sigma(W_f E y_{t-1} + U_f h_{t-1} + Z_f \hat{z}_t + b_f), \\
    c_t &= f_t c_{t-1} + i_t \tanh(W_c E y_{t-1} + U_c h_{t-1} + Z_c \hat{z}_t + b_c), \\
    o_t &= \sigma(W_o E y_{t-1} + U_o h_{t-1} + Z_o \hat{z}_t + b_o), \\
    h_t &= o_t \tanh(c_t).
\end{align*}
\]

Here, \(i_t, f_t, c_t, o_t, h_t\) are the input, forget, memory, output and hidden state of the LSTM respectively. \(W_*, U_*, Z_*\) and \(b_*\) are learned weight matrices and biases. \(E \in \mathbb{R}^{m \times K}\) is an embedding matrix. Let \(m\) and \(n\) denote the embedding and LSTM dimensionality respectively and \(\sigma\) be the logistic sigmoid activation.

In simple terms, the context vector \(\hat{z}_t\) is a dynamic representation of the relevant part of the image input at time \(t\). We define a mechanism \(\phi\) that computes \(\hat{z}_t\) from the annotation vectors \(a_i, i = 1, \ldots, L\) corresponding to the features extracted at different image locations. For each location \(i\), the mechanism generates a positive weight \(\alpha_i\) which can be interpreted either as the probability that location \(i\) is the right place to focus for producing the next word (stochastic attention mechanism), or as the relative importance to give to location \(i\) in blending the \(a_i's\) together (deterministic attention mechanism). The weight \(\alpha_i\) of each annotation vector \(a_i\) is computed by an attention model \(f_{\text{att}}\) for which we use a multilayer perceptron which is conditioned on the previous hidden state \(h_{t-1}\). To emphasize, we note that the hidden state varies as the output RNN advances in its output sequence: “where” the network looks next depends on the sequence of words that has already been...
Once the weights (which sum to one) are computed, the context vector \( \hat{z}_t \) is computed by

\[
\hat{z}_t = \phi(\{a_i\}, \{\alpha_i\}),
\]

where \( \phi \) is a function that returns a single vector given the set of annotation vectors and their corresponding weights. The details of the \( \phi \) function are discussed in Sec. 3.4.

The initial memory state and hidden state of the LSTM are predicted by an average of the annotation vectors fed through two separate MLPs (init,c and init,h):

\[
c_0 = f_{\text{init},c}\left(\frac{1}{L} \sum_i a_i\right), \quad h_0 = f_{\text{init},h}\left(\frac{1}{L} \sum_i a_i\right)
\]

In this work, we use a deep output layer (Pascanu et al., 2014) to compute the output word probability. Its input are cues from the image (the context vector), the previously generated word, and the decoder state \( (h_t) \).

\[
p(y_t|a, y_{t-1}) \propto \exp(L_o(Ey_{t-1} + L_hh_t + L_z\hat{z}_t)),
\]

where \( L_o \in \mathbb{R}^{K \times m} \), \( L_h \in \mathbb{R}^{m\times n} \), \( L_z \in \mathbb{R}^{m \times D} \), and \( E \) are learned parameters initialized randomly.

### 3.4 Learning Stochastic “Hard” vs Deterministic “Soft” Attention

In this section we discuss two alternative mechanisms for the attention model \( f_{\text{att}} \): stochastic attention and deterministic attention.
3.4.1 Stochastic “Hard” Attention

We represent the location variable $s_t$ as the spatial index where the model decides to focus when generating the $t$-th word. $s_{t,i}$ is an indicator one-hot variable which is set to 1 if the $i$-th location (out of $L$) is the one used to extract visual features. By treating the attention locations as intermediate latent variables, we can assign a multinoulli distribution parametrized by $\{\alpha_i\}$, and view $\hat{z}_t$ as a random variable:

$$p(s_{t,i} = 1 \mid s_{j<t}, a) = \alpha_{t,i} \quad (3.3)$$
$$\hat{z}_t = \sum_i s_{t,i} a_i. \quad (3.4)$$

We define a new objective function $L_s$ that is a variational lower bound on the marginal log-likelihood $\log p(y \mid a)$ of observing the sequence of words $y$ given image features $a$. Similar to work in generative deep generative modeling (Kingma and Welling, 2014; Rezende et al., 2014), the learning algorithm for the parameters $W$ of the models can be derived by directly optimizing

$$L_s = \sum_s p(s \mid a) \log p(y \mid s, a) \leq \log \sum_s p(s \mid a)p(y \mid s, a) = \log p(y \mid a),$$

(3.5)
following its gradient

$$\frac{\partial L_s}{\partial W} = \sum_s p(s \mid a) \left[ \frac{\partial \log p(y \mid s, a)}{\partial W} + \log p(y \mid s, a) \frac{\partial \log p(s \mid a)}{\partial W} \right].$$

(3.6)

We approximate this gradient of $L_s$ by a Monte Carlo method such that

$$\frac{\partial L_s}{\partial W} \approx \frac{1}{N} \sum_{n=1}^{N} \left[ \frac{\partial \log p(y \mid \tilde{s}^n, a)}{\partial W} + \log p(y \mid \tilde{s}^n, a) \frac{\partial \log p(\tilde{s}^n \mid a)}{\partial W} \right],$$

(3.7)

where $\tilde{s}^n = (s^n_1, s^n_2, \ldots)$ is a sequence of sampled attention locations. We sample the location $s^n_t$ from a multinouilli distribution defined by Eq. (3.3):

$$\tilde{s}^n_t \sim \text{Multinouilli}(\{\alpha^n_i\}).$$

We reduce the variance of this estimator with the moving average baseline technique (Weaver and Tao, 2001). Upon seeing the $k$-th mini-batch, the moving average baseline is estimated as an accumulated sum of the previous log likelihoods with exponential decay:

$$b_k = 0.9 \times b_{k-1} + 0.1 \times \log p(y \mid \tilde{s}_k, a)$$

To further reduce the estimator variance, the gradient of the entropy $H[s]$ of the multinouilli distribution is added to the RHS of Eq. (3.7).

The final learning rule for the model is then

$$\frac{\partial L_s}{\partial W} \approx \frac{1}{N} \sum_{n=1}^{N} \left[ \frac{\partial \log p(y \mid \tilde{s}^n, a)}{\partial W} + \lambda_r (\log p(y \mid \tilde{s}^n, a) - b) \frac{\partial \log p(\tilde{s}^n \mid a)}{\partial W} + \lambda_e \frac{\partial H[\tilde{s}^n]}{\partial W} \right]$$

where, $\lambda_r$ and $\lambda_e$ are two hyper-parameters set by cross-validation. As pointed out and used by Ba et al. (2014) and Mnih et al. (2014), this formulation is equivalent to the REINFORCE learning rule (Williams, 1992), where the reward for the attention choosing a sequence of actions is a real value proportional to the log likelihood of the target sentence under the sampled attention trajectory.

In order to further improve the robustness of this learning rule, with probability
0.5 for a given image, we set the sampled attention location \( \tilde{s} \) to its expected value \( \alpha \) (equivalent to the deterministic attention in Sec. 3.4.2).

### 3.4.2 Deterministic “Soft” Attention

Learning stochastic attention requires sampling \( s_t \) (the attention location) each time, instead we can take the expectation of the context vector \( \hat{z}_t \) directly,

\[
\mathbb{E}_{p(s_t|a)}[\hat{z}_t] = \sum_{i=1}^{L} \alpha_{t,i} a_i
\]

and formulate a deterministic attention model by computing a soft attention weighted annotation vector \( \phi(\{a_i\}, \{\alpha_i\}) = \sum_i^L \alpha_i a_i \) as proposed by Bahdanau et al. (2014). This corresponds to computing a soft \( \alpha \) weighted context as input. The whole model is smooth and differentiable under the deterministic attention, so learning end-to-end is trivial by using standard back-propagation.

Learning the deterministic attention can also be understood as approximately optimizing the marginal likelihood in Eq. (3.5) under the attention location random variable \( s_t \) from Sec. 3.4.1. The hidden activation of LSTM \( h_t \) is a linear projection of the stochastic context vector \( \hat{z}_t \) followed by tanh non-linearity. To the first-order Taylor approximation, the expected value \( \mathbb{E}_{p(s_t|a)}[h_t] \) is equivalent to computing \( h_t \) using a single forward computation with the expected context vector \( \mathbb{E}_{p(s_t|a)}[\hat{z}_t] \).

Let us denote by \( n_{t,i} \) as \( n \) in Eq. (3.2) with \( \hat{z}_t \) set to \( a_i \). Then, we can write the normalized weighted geometric mean (NWGM) of the softmax of \( k \)-th word prediction as

\[
\text{NWGM}[p(y_t = k \mid a)] = \frac{\prod_i \exp(n_{t,k,i} p(s_t,i=1|a))}{\sum_j \prod_i \exp(n_{t,j,i} p(s_t,i=1|a))} = \frac{\exp(\mathbb{E}_{p(s_t|a)}[n_{t,k}])}{\sum_j \exp(\mathbb{E}_{p(s_t|a)}[n_{t,j}])}
\]

This implies that the NWGM of the word prediction can be well approximated by using the expected context vector \( \mathbb{E}[\hat{z}_t] \), instead of the sampled context vector \( a_i \).

Furthermore, from the result by Baldi and Sadowski (2014), the NWGM in Eq. (3.9) which can be computed by a single feedforward computation approximates the expectation \( \mathbb{E}[p(y_t = k \mid a)] \) of the output over all possible attention
locations induced by random variable $s_t$. This suggests that the proposed deterministic attention model approximately maximizes the marginal likelihood over all possible attention locations.

**Doubly Stochastic Attention**

In training the deterministic version of our model, we introduce a form of doubly stochastic regularization that encourages the model to pay equal attention to every part of the image. Whereas the attention at every point in time sums to 1 by construction ($\sum t \alpha_{ti} = 1$), the attention $\sum t \alpha_{ti}$ is not constrained in any way. This makes it possible for the decoder to ignore some parts of the input image. In order to alleviate this, we encourage $\sum t \alpha_{ti} \approx \tau$ where $\tau \geq \frac{L}{D}$. In our experiments, we observed that this penalty quantitatively improves overall performance and that this qualitatively leads to more descriptive captions.

Additionally, the soft attention model predicts a gating scalar $\beta$ from previous hidden state $h_{t-1}$ at each time step $t$, such that, $\phi(\{a_i\}, \{\alpha_i\}) = \beta \sum_i \alpha_i a_i$, where $\beta_t = \sigma(f_{\beta}(h_{t-1}))$. This gating variable lets the decoder decide whether to put more emphasis on language modeling or on the context at each time step. Qualitatively, we observe that the gating variable is larger than the decoder describes an object in the image.

Table 3.1 – BLEU-1,2,3,4/METEOR metrics compared to other methods, † indicates a different split, (—) indicates an unknown metric, ◦ indicates the authors kindly provided missing metrics by personal communication, Σ indicates an ensemble, a indicates using AlexNet

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Model</th>
<th>BLEU-1</th>
<th>BLEU-2</th>
<th>BLEU-3</th>
<th>BLEU-4</th>
<th>METEOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flickr8k</td>
<td>Google NIC(Vinyals et al., 2014)</td>
<td>63</td>
<td>41</td>
<td>27</td>
<td>—</td>
<td>17.31</td>
</tr>
<tr>
<td></td>
<td>Log Bilinear (Kiros et al., 2014)</td>
<td>65.6</td>
<td>42.4</td>
<td>27.7</td>
<td>17.7</td>
<td>18.93</td>
</tr>
<tr>
<td></td>
<td>Soft-Attention</td>
<td>67</td>
<td>44.8</td>
<td>29.9</td>
<td>19.5</td>
<td>17.31</td>
</tr>
<tr>
<td></td>
<td>Hard-Attention</td>
<td>67</td>
<td>45.7</td>
<td>31.4</td>
<td>21.3</td>
<td>20.30</td>
</tr>
<tr>
<td>Flickr3k</td>
<td>Google NIC†Σ</td>
<td>66.3</td>
<td>42.3</td>
<td>27.7</td>
<td>18.3</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>Log Bilinear</td>
<td>60.0</td>
<td>38</td>
<td>25.4</td>
<td>17.1</td>
<td>16.88</td>
</tr>
<tr>
<td></td>
<td>Soft-Attention</td>
<td>66.7</td>
<td>43.4</td>
<td>28.8</td>
<td>19.1</td>
<td>18.49</td>
</tr>
<tr>
<td></td>
<td>Hard-Attention</td>
<td>66.9</td>
<td>43.9</td>
<td>29.6</td>
<td>19.9</td>
<td>18.46</td>
</tr>
<tr>
<td>COCO</td>
<td>CMU/MS Research (Chen and Zitnick, 2014)</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>20.41</td>
</tr>
<tr>
<td></td>
<td>MS Research (Fang et al., 2014)</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>20.71</td>
</tr>
<tr>
<td></td>
<td>BRNN (Karpathy and Li, 2014)</td>
<td>64.2</td>
<td>45.1</td>
<td>30.4</td>
<td>20.3</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>Google NIC†Σ</td>
<td>66.6</td>
<td>46.1</td>
<td>32.9</td>
<td>24.6</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>Log Bilinear</td>
<td>70.8</td>
<td>48.9</td>
<td>34.4</td>
<td>24.3</td>
<td>20.03</td>
</tr>
<tr>
<td></td>
<td>Soft-Attention</td>
<td>70.7</td>
<td>49.2</td>
<td>34.4</td>
<td>24.3</td>
<td>23.90</td>
</tr>
<tr>
<td></td>
<td>Hard-Attention</td>
<td><strong>71.8</strong></td>
<td><strong>50.4</strong></td>
<td><strong>35.7</strong></td>
<td><strong>25.0</strong></td>
<td>23.04</td>
</tr>
</tbody>
</table>

The soft attention model is trained end-to-end by minimizing the following
penalized negative log-likelihood:

\[ L_d = -\log(p(y|a)) + \lambda \sum_{i}^{L} (1 - \sum_{t}^{C} \alpha_{ti})^2, \quad (3.9) \]

where we simply fixed \( \tau \) to 1.

### 3.4.3 Training Procedure

Both variants of our attention model were trained with stochastic gradient descent using adaptive learning rates. For the Flickr8k dataset, we found that RMSProp (Tieleman and Hinton, 2012) worked best, while for Flickr30k/MS COCO dataset we found the recently proposed Adam algorithm (Kingma and Ba, 2014) to be quite effective.

To create the annotations \( a_i \) used by our decoder, we used the Oxford VGGnet (Simonyan and Zisserman, 2014) pre-trained on ImageNet without finetuning. In our experiments we use the 14\( \times \)14\( \times \)512 feature map of the fourth convolutional layer before max pooling. This means our decoder operates on the flattened 196\( \times \)512 (i.e \( L \times D \)) encoding. In principle however, any encoding function could be used. In addition, with enough data, the encoder could also be trained from scratch (or fine-tune) with the rest of the model.

As our implementation requires time proportional to the length of the longest sentence per update, we found training on a random group of captions to be computationally wasteful. To mitigate this problem, in preprocessing we build a dictionary mapping the length of a sentence to the corresponding subset of captions. Then, during training we randomly sample a given length and retrieve a mini-batch of size 64 of that length. We found that this greatly improved convergence speed with no noticeable diminishment in performance. On our largest dataset (MS COCO), our soft attention model took less than 3 days to train on an NVIDIA Titan Black GPU.

In addition to dropout (Srivastava et al., 2014), the only other regularization strategy we used was early stopping on BLEU score. We observed a breakdown in correlation between the validation set log-likelihood and BLEU in the later stages of training during our experiments. Since BLEU is the most commonly reported metric, we used BLEU on our validation set for model selection.
In our experiments with soft attention, we used Whetlab\(^1\) (Snoek et al., 2012, 2014) in our Flickr8k experiments. Some of the intuitions we gained from hyperparameter regions it explored were especially important in our Flickr30k and COCO experiments.

We make our code for these models publicly available to encourage future research in this area\(^2\).

**Figure 3.4** – Examples of attending to the correct object (white indicates the attended regions, underlines indicated the corresponding word)

3.5 Experiments

We describe our experimental methodology and quantitative results which validate the effectiveness of our model for caption generation.

3.5.1 Data

We report results on the widely-used Flickr8k and Flickr30k dataset as well as the more recently introduced MS COCO dataset. Each image in the Flickr8k/30k dataset have 5 reference captions. In preprocessing our COCO dataset, we maintained a the same number of references between our datasets by discarding caption in excess of 5. We applied only basic tokenization to MS COCO so that it is consistent

---

1. [https://www.whetlab.com/](https://www.whetlab.com/)
2. [https://github.com/kelvinxu/arctic-captions](https://github.com/kelvinxu/arctic-captions)
with the tokenization present in Flickr8k and Flickr30k. For all our experiments, we used a fixed vocabulary size of 10,000.

Results for our attention-based architecture are reported in Table 3.1. We report results with the frequently used BLEU metric\(^3\) which is the standard in image caption generation research. We report BLEU\(^4\) from 1 to 4 without a brevity penalty. There has been, however, criticism of BLEU, so we report another common metric METEOR (Denkowski and Lavie, 2014) and compare whenever possible.

\section*{Figure 3.5 – Examples of mistakes where we can use attention to gain intuition into what the model saw.}

\begin{figure}[h]
\centering
\begin{tabular}{ccc}
\includegraphics[width=0.3\textwidth]{example1} & \includegraphics[width=0.3\textwidth]{example2} & \includegraphics[width=0.3\textwidth]{example3} \\
A large white \underline{bird} standing in a forest. & A woman holding a \underline{clock} in her hand. & A man wearing a hat and a hat on a \underline{skateboard}. \\
\includegraphics[width=0.3\textwidth]{example4} & \includegraphics[width=0.3\textwidth]{example5} & \includegraphics[width=0.3\textwidth]{example6} \\
A person is standing on a beach with a \underline{surfboard}. & A woman is sitting at a table with a large \underline{pizza}. & A man is talking on his cell phone while another man watches. \\
\end{tabular}
\end{figure}

\subsection*{3.5.2 Evaluation Procedures}

A few challenges exist for comparison, which we explain here. The first challenge is a difference in choice of convolutional feature extractor. For identical decoder architectures, using a more recent architectures such as GoogLeNet (Szegedy et al., 2014) or Oxford VGG (Simonyan and Zisserman, 2014) can give a boost in performance over using the AlexNet (Krizhevsky et al., 2012). In our evaluation, we compare directly only with results which use the comparable GoogLeNet/Oxford

\begin{itemize}
\item We verified that our BLEU evaluation code matches the authors of Vinyals et al. (2014), Karpathy and Li (2014) and Kiros et al. (2014). For fairness, we only compare against results for which we have verified that our BLEU evaluation code is the same.
\item BLEU-n is the geometric average of the n-gram precision. For instance, BLEU-1 is the unigram precision, and BLEU-2 is the geometric average of the unigram and bigram precision.
\end{itemize}

31
VGG features, but for METEOR comparison we include some results that use AlexNet.

The second challenge is a single model versus ensemble comparison. While other methods have reported performance boosts by using ensembling, in our results we report a single model performance.

Finally, there is a challenge due to differences between dataset splits. In our reported results, we use the pre-defined splits of Flickr8k. However, for the Flickr30k and COCO datasets is the lack of standardized splits for which results are reported. As a result, we report the results with the publicly available splits\(^5\) used in previous work (Karpathy and Li, 2014). We note, however, that the differences in splits do not make a substantial difference in overall performance.

### 3.5.3 Quantitative Analysis

In Table 3.1, we provide a summary of the experiment validating the quantitative effectiveness of attention. We obtain state of the art performance on the Flickr8k, Flickr30k and MS COCO. In addition, we note that in our experiments we are able to significantly improve the state-of-the-art performance METEOR on MS COCO. We speculate that this is connected to some of the regularization techniques we used (see Sec. 3.4.2) and our lower-level representation.

### 3.5.4 Qualitative Analysis: Learning to attend

By visualizing the attention learned by the model, we are able to add an extra layer of interpretability to the output of the model (see Fig. 3.1). Similar systems have relied on object detection systems to produce candidate alignment targets (Karpathy and Li, 2014). Our approach is much more flexible, since the model can attend to “non-object” salient regions.

The 19-layer OxfordNet uses stacks of 3x3 filters meaning the only time the feature maps decrease in size are due to the max pooling layers. The input image is resized so that the shortest side is 256-dimensional with preserved aspect ratio. The input to the convolutional network is the center-cropped 224x224 image. Consequently, with four max pooling layers, we get an output dimension of the top convolutional layer of 14x14. Thus in order to visualize the attention weights

---

\(^5\) [http://cs.stanford.edu/people/karpathy/deepimagesent/](http://cs.stanford.edu/people/karpathy/deepimagesent/)
for the soft model, we upsample the weights by a factor of $2^4 = 16$ and apply a Gaussian filter to emulate the large receptive field size.

As we can see in Figs. 3.3 and 3.4, the model learns alignments that agree very strongly with human intuition. Especially from the examples of mistakes in Fig. 3.5, we see that it is possible to exploit such visualizations to get an intuition as to why those mistakes were made. We provide a more extensive list of visualizations as the supplementary materials for the reader.

### 3.6 Conclusion

We propose an attention based approach that gives state of the art performance on three benchmark datasets using the BLEU and METEOR metric. We also show how the learned attention can be exploited to give more interpretability into the models generation process, and demonstrate that the learned alignments correspond very well to human intuition. We hope that the results of this paper will encourage future work in using visual attention. We also expect that the modularity of the encoder-decoder approach combined with attention to have useful applications in other domains.
In this work, we proposed an attention based approach for image captioning which we validated with three benchmark datasets using the BLEU and METEOR metric. We also showed how the learned attention can be exploited to give more interpretability into the model’s generation process, and demonstrate that the learned alignments correspond very well to human intuition.

Since the work done in this thesis, recurrent neural networks have continued to be the dominant approach for image captioning. Different groups have continued to improve the performance of captioning systems, innovating either the architecture used or the training algorithm of the model.

You et al. (2016) explored conditioning the caption generation procedure with attributes obtained by either clustering or through prediction (see Figure 4.2). Yang et al. (2016) future augmented the attention based framework by introducing a series of ‘reviewer’ steps which produced a soft-attention weighted ‘thought’ vector that was used to condition the decoder. Finally, Lu et al. (2016) introduced a variant
of the attention model presented here which essentially provides a skip connection from the decoder which can bypass the image input. Their variant removed the need to attend when generating ‘stop words’ which have no visual basis.

In general, improved vision encodings improve performance regardless decoder architecture. Along this line, Jin et al. (2015) used selective search with a convolutional network classifier to filter salient regions before inputting it into a captioning model with attention. This work was followed by Anderson et al. (2017), which used the ‘Faster R-CNN’ feature extractor to give more expressive features. This work can also be thought of a ‘hard attention’ model where the regions are selected by the ‘Faster R-CNN model’.

![Figure 4.2](image)

**Figure 4.2** – Figure from You et al. (2016). In their approach, they combine RNN based generation of captions using both image features and attention over semantic concepts extracted from the training set.

Captioning and other sequence generation tasks have also since been improved by methods that better optimize the underlying objective. Log-likelihood has no known relationship to many of the metrics used in captioning. Early work on this included MIXER Ranzato et al. (2015), which merged log-likelihood training with a REINFORCE objective on the underlying metric in a curriculum fashion. This work was followed by work with actor-critic style training Bahdanau et al. (2016) which different in that it used a learned Q-function for more dense credit assignment.
Finally, Rennie et al. (2017) proposed a ‘self-critical’ REINFORCE style objective, where the reward was essentially baselined by the models’ own greedy decoding.

**Figure 4.3** — figure from Anderson et al. (2017). In their approach, they combine RNN based generation of captions with the faster R-CNN framework which consists of a region proposal step followed by a feature extraction step. Attention is done over the different proposed regions which allows for intuitive visualization.


Mnih, V., N. Hees, A. Graves, and K. Kavukcuoglu (2014). Recurrent models of visual attention. In NIPS.


43


