YaleNUSCollege

Object Detection Without Bounding Boxes via Deep Reinforcement Learning

Aaron Sing Wo Pang

Capstone Final Report for BSc (Honours) in

Mathematical, Computational and Statistical Sciences

AY 2018/2019

Yale-NUS College Capstone Project

DECLARATION & CONSENT

1. I declare that the product of this Project, the Thesis, is the end result of my own work and that due acknowledgement has been given in the bibliography and references to ALL sources be they printed, electronic, or personal, in accordance with the academic regulations of Yale-NUS College.

2. I acknowledge that the Thesis is subject to the policies relating to Yale-NUS College Intellectual Property (Yale-NUS HR 039).

ACCESS LEVEL

3. I agree, in consultation with my supervisor(s), that the Thesis be given the access level specified below: [check one only]

✖ Unrestricted access
Make the Thesis immediately available for worldwide access.

o Access restricted to Yale-NUS College for a limited period
Make the Thesis immediately available for Yale-NUS College access only from _____ (mm/yyyy) to _____ (mm/yyyy), up to a maximum of 2 years for the following reason(s): (please specify; attach a separate sheet if necessary):
_____.

After this period, the Thesis will be made available for worldwide access.

o Other restrictions: (please specify if any part of your thesis should be restricted)
_____
_____

_____
Name & Residential College of Student

_____ _____
Signature of Student Date

Robby Tan 24/4/2018
_____ _____
Name & Signature of Supervisor Date

YALE-NUS COLLEGE

Abstract

Bachelor of Science (Hons.)

Object Detection Without Bounding Boxes via Deep Reinforcement Learning

by Aaron PANG

Finding relevant objects in a given environment is an important task for both humans and artificial intelligence agents. Within a given scene a variety of objects can appear at a variety of sizes and locations, increasing the difficulty of the task. Traditional solutions thus usually used a sliding window approach or used features at several scales of the input of the image. Current state of the art deep learning solutions aim to use a variety of convolutional neural networks to solve the problem, yet these require vast amounts of hand labelled data to succeed. This capstone project thus attempts to solve both problems by applying reinforcement learning to the task of object detection. The goal is to be able to train a new neural network that can detect objects within an image without the need of additional data from our object detection dataset such as the ground truth bounding boxes and to only learn from the images themselves. Here unsupervised is to mean that neither the class labels nor bounding box data from our object detection training dataset will be used to train our network.

Our proposed agent thus takes in an input image and emits a proposed set of candidate bounding boxes by searching for regions it is most confident an objects exists within, rather than by using hand labelled bounding boxes as a comparison. This agent initially performed poorly when trained on synthesized MNIST data, but when trained on PASCAL VOC 2012 data it is able to produce qualitatively acceptable bounding boxes.

The contributions of this project are a proof of concept of the methodology, and the evidence that this methodology has the potential to be improved upon.

Acknowledgements

Thanks to my friends Silvia and Pratyush for always providing emotional and technical support over the course of this project.

Thanks to all my other friends I haven't listed for always listening.

Thanks to Robby for his advice and bringing my attention to a variety of papers and being the school's advocate for deep learning.

Thanks to Maurice Cheung for always listening to us and being a helpful member of our community and for always reviewing my drafts late at night.

Contents

To my family for always putting up with me...

Chapter 1

Introduction

1.1 Motivation and Goal

Society more than ever is governed by photographic images. In order to better understand the billions of images uploaded daily, computer vision systems have also grown in usage. This means they must be able to extract exact locations of important features within an image. By doing so we can first individually identify multiple elements of a complex image, and then only extract its meaningful components. As a result we can improve the utility of surveillance cameras, autonomous vehicles and satellite cameras. Tasks such as reviewing security footage can be further automated by only including clips with humans or objects inside.

Current state of the art systems such as Faster R-CNN [1] and SSD [2], however, require huge amounts of labelled data to train. Datasets such as MS-COCO [3] require thousands individuals to draw boxes around portions of an image that they deem relevant to be included in the training data. Additionally these images may not be able to fully capture all types of objects that are relevant, nor would they be able to capture the ways in which objects are placed or obscured in all sorts of images. On the whole, training models for object detection and classification is incredibly difficult because of the required volume and type of data needed.

This project aims to address these issues by creating an unsupervised object localization methodology. This system will learn to draw bounding boxes over a given series of test data, without needing to be told either what is present inside our images or its set of bounding boxes. The aim of this system is not to outperform existing supervised solutions, but to provide a proof of concept that such an unsupervised

system can be created in the first place. Such a system would also reduce the number of proposed object candidates as compared to current systems.

1.2 Background

1.2.1 Deep Learning

Deep learning is a subset of machine learning that is primarily concerned with neural networks. The basics of a neural network are as follows. For a given input vector x with each of its entries representing some sort feature, we multiply it with a matrix of weights W, add it to a bias term b and then apply a non-linear function σ such as *sigmoid* or *ReLU*. Sigmoid is defined as $\sigma(x) = \frac{1}{1+e^{-x}}$, while *ReLU* is $ReLU(x) = \max(0, x)$. These non-linearities act as step functions for our network, allowing our network to model non-linear relationships in our data. This was largely inspired by how biological neurons also appear to utilize a step function.

$$f(x) = \sigma(Wx + b) \tag{1.1}$$

The domain and co-domain of this function are the real numbers. Since sigmoid only affects a single entry, it is applied to entires of the vector.

Each layer within a neural net represents an additional set of weights and bias we apply consecutively to our input. In order for this system to learn then we must thus use a process called Stochastic Gradient Descent (SGD)[4].

Stochastic gradient descent is method of non-convex optimization that can be summarized as follows. After applying our input vector to several layers of our neural network we will get some output vector y. We can then compare y with $\hat{y}$, also known as the ground truth vector through a loss function such as mean squared or cross entropy loss.

$$Loss_{MSE} = (y - \hat{y})^2 \tag{1.2}$$

$$Loss_{CE} = -\sum_i y_i log(\hat{y}_i) \tag{1.3}$$

We can take the derivatives of each weight and bias term in our network with respect to this loss function, finding which direction to move our weight matrices and bias vectors to decrease this value for loss. We multiply this derivative with some scalar α, also called our learning rate, and subtract it from the current value [5].

$$W_{new} = W_{old} - \alpha * \frac{\partial Loss}{\partial w} \tag{1.4}$$

Repeating this process over millions of time steps, we will eventually find values for weight and bias that minimize our loss. In order to make this process stochastic gradients are also calculated with respect to a randomly sampled batch of data. This induces a slight amount of noise into our model and minimizes the chance our network gets stuck at locally optimal solutions.

Other optimizers then such as RMSProp [6] and Adam [5], then apply several other improvements to the optimization process. Both were chosen for this capstone for different experiments. One shortcoming both of these optimizers aim to overcome was the selection of a suitable learning rate for training.

Adam and RMSProp address this by introducing learning rate annealing, which decreases our learning rate over time with respect to previous values either linearly or exponentially. Another idea that these then aimed to introduce was momentum. This means that instead of only considering the gradients with respect to the current input, both these optimizers choose to keep a fraction of the previous gradients and sum them to our current value. This dampens the oscillations of directions in which our network chooses to go towards. Empirically this has resulted in better performance over time [6]. Adam improves upon other optimizers by taking into account past values to calculate both first second-order moment of our gradients to better decay the value of its learning rate.

One improvement to neural networks is called dropout. This layer will randomly select a subset of the previous layers entries and sets them to 0. Our network learns a more robust mapping between each layer, relying on fewer of its parameters at each step of training. This both helps our network overfit less and increases our accuracy at evaluation time [7].

1.3 Image Classification and Convolutional Neural Nets

Image classification is one of the few tasks in supervised machine learning that has become largely solved [8]. The idea is that for a given image a system will do its best to determine a class label, eg. whether its a dog, cat, car etc.

1.3.1 Kernels

Starting in 2012 with AlexNet [9] most modern classification systems heavily rely on the use of convolutional neural nets (CNNs). These are similar to regular neural nets in that they consist of a series of weights and bias vectors and apply these to non-linear functions. The crucial difference is that they aim to apply a matrix of trainable values, also known as a kernel, across an image to extract features from it. Each kernel has a specified width and height, and sweep across our image at intervals determined by its stride. At each layer we stack many of these kernels together to create a volume of extracted features. Each kernel will learn a different representation of the image, extracting several different features from one another.

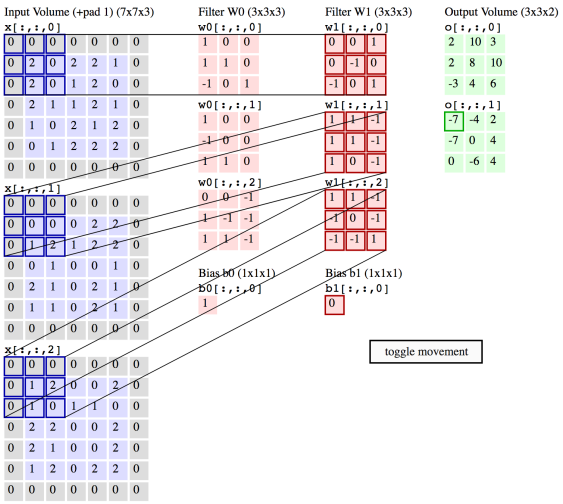

FIGURE 1.1: Example of a CNN [10]. Here the blue is a matrix representation of our input image. Each red square is one of our kernels that are slid across our input image. The green is the resultant output.

Through SGD we can then determine what exact values are in each kernel, which over time allows our system to learn to detect features such as edges, eyes and fur from a given image. These kernels are are shared throughout the image in a sliding window fashion, allowing us to detect the same items across all sections of the

image. CNNs are also a more compact method of analyzing images as compared to regular neural nets. This is because by sliding the kernels over an image it also shares the same weights multiple times, rather than directly connect a single neuron to each pixel of an image.

1.3.2 Pooling

Pooling layers are a way ot reducing our feature block size. These do so by considering a sliding window upon our feature map, and performing some sort of operation to reduce the values in that window into a single value. Examples such as max-pooling will take the maximum value from a given window, whereas average-pooling will instead take the average of that window. After a series of these convolutional-pooling we then flatten our feature map into a 1-dimensional vector and pass it onto a regular feed forward neural network, leading us to predict the class label of the image.

Today's state of the art classification engines such as Xception [11] can easily differentiate between tens of thousands ambiguous classes. A network is therefore considered deep when it contains many layers, sometimes as many as 1000.

1.4 Reinforcement Learning

Reinforcement learning (RL) is a field of machine learning that aims to create artificial intelligence agents capable of learning from experiences. (Refer to 2.1 for more details on formulas and derivations.) Most RL problems are formulated as Markov Decision Processes (MDP) [12]. These problems have a state s which our agent can observe. This state is markovian in the sense that every state fully determines the problem at hand without requiring a memory of previous states. At each state our agent can choose a series of actions a, which then will lead it to a particular set of rewards as determined by the environment. This is similar to how animals learn from trial and error.

A policy in reinforcement learning is also defined as a function that maps states to a probability distribution of actions that should be undertaken. Our goal here is to find a policy π that will maximise these rewards obtained by the agent. The solution

we follow is to accurately estimating the rewards that will be obtained by taking a particular action at a given state, and choosing the action with the maximal value. This is an example of a greedy-policy [13]

The advantage of RL based solutions is that they can solve problems without knowing the problem before hand. Examples of recent successes in RL include Atari games [13] and AlphaGO [14]. While games have been the drivers of RL, it also been applied to other domains such as ad pricing [15] and even e-commerce [16].

Compared with deep learning, however, RL faces an entirely different set of challenges. While the labelled datasets used in classification or speech recognition are highly structured, the observations made by an RL agent heavily depend on its current exploration and policy. For example, an agent that immediately fails its stated task in the early rounds of a videogame can never hope to optimize for the final end game. A more explicit example could be a RL-agent that is always eaten by the ghost will never be able to find a robust enough policy to collect all the pellets on a map because it simply cannot explore enough of the game. The search space of state, action pairs also vast exceeds the data within object classification, requiring orders of magnitude higher computations in order to succeed.

1.5 Object Localization / Detection

Inspired by successes in classification, other researchers have applied these ideas to object localization and detection tasks. Localization here is defined as drawing a bounding box over a given image and predicting its class label. Detection however, involves drawing multiple boxes over multiple objects within the same image. This project focuses on the former.

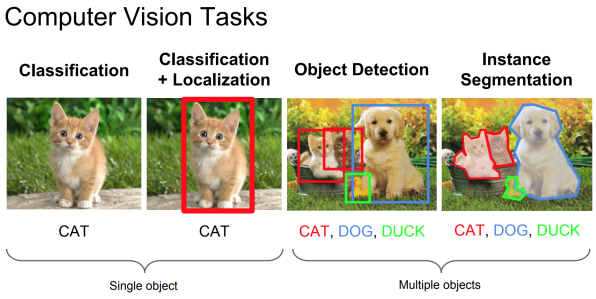

FIGURE 1.2: Overview of typical computer vision tasks [17]

Localization traditionally required an ensemble of techniques to be tackled and hand crafted features such as SIFT or HOG [18], but modern day deep learning based solutions can solve the entire problem end to end [19]. Through a series of convolutional networks and smart use of feed forward neural nets, object detection today can also be done in real time.

1.6 Contributions

The contributions of this capstone are as follows. The proposal of a bounding boxless method for object detection using reinforcement learning and a working implementation of the method. This capstone thus then presents evidence of the efficacy of such a method, proposing future developments that could potentially improve upon our current implementation. My advisor sent me a the following papers: Active Object Localization with Deep Reinforcement Learning[20] and Attention-Aware Deep Reinforcement Learning for Video Face Recognition[21] to survey.

A more robust implementation of this methodology can be used to train large scale object detection frameworks without the need for further hand annotated data. This would allow us to utilize the vast swaths of data that exists in satelite imagery or surveillance footage without the need to hand label each of these datasets ahead of time. This would also potentially allow us to implement object detection on specialized tasks which there exists little annotated data for.

Chapter 2

Existing Solutions

2.1 Reinforcement Learning

In reinforcement learning we observe a particular state, take some action and get a reward and new state in return.

$$s \xrightarrow{a} r, s' \tag{2.1}$$

More formally this can be illustrated by the Bellman equation below [13].

$$\begin{aligned} Q(s,a) &= r_t + \gamma r_{t+1} + \gamma^2 r_{t+2} + \cdots \\ Q(s,a) &= r_t + \gamma(r_{t+1} + \gamma r_{t+2} + \cdots) \\ Q(s,a) &= r_t + \gamma \max_a Q(s',a) \end{aligned} \tag{2.2}$$

Here Q is our computed table of all possible reward values for s, a state action pairs. The values stored within Q are also known as Q-values. The parameter γ is a discount factor less than 1 used to make sure the q-network accounts for future consequences. It is less than 1 to ensure q-values do not approach infinity. A policy $\pi(s)$ is defined as a probability distribution of actions at any given state. Storing such a table is computationally intractable for large problems, but it can be approximated using a neural network.

Traditional solutions simply use Equation 2.2 to assign values within a table. In deep reinforcement learning we instead use backpropagation to make our network tend towards the same output $Q(s,a) \rightarrow r_t + \gamma \max_a Q(s',a)$

2.1.1 Deep Q-Learner

The Deep Q-Network (DQN) [13] architecture is what laid most of the groundwork of recent deep learning based reinforcement learning solutions [22].

Architecture

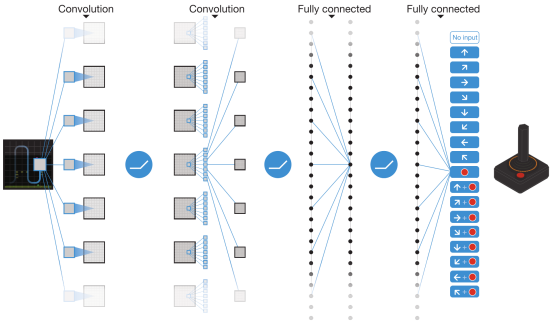

FIGURE 2.1: DQN architecture [13]

As presented in the original paper, the DQN architecture takes in a series of 4 atari game frames that are resized and grayscaled and estimates the rewards obtained by selecting a particular action using a neural network. It is also important to note that the DQN is an example of online-learning, in the sense that it learns as it experiences an environment rather than learning with respect to a history of labelled data.

During training this network uses what is known as an ϵ-greedy policy. At the beginning of training ϵ is set to be some parameter less than or equal to one. This determines with what probability our network chooses a random action. Over time, the value of ϵ is gradually decreased. When not choosing randomly our network will simply choose the action at a particular state with the highest estimated Q-value. This value of ϵ, however, is never set to 0 during training, ensuring that our network continues to have some degree of exploration. At inference time, we would of course only act with respect to the Q-values estimated by the network.

Training

Important training methods introduced by the DQN are *experience replay* and *target networks*. Experience replay aims to offset the short sightedness of our network by

letting it see previous actions sampled from a memory module. This is because if we only train our network with the current examples it sees, these tend to be highly correlated with one another and makes our network overfit.

Target networks are copies of the current estimate of the Q function that are updated at slower intervals. Since our Q-network is updated at every time step it has a tendency to fluctuate wildly. This means, between consecutive timesteps its estimates of q-values for the same input state may greatly change and potentially lead to feedback loops that we do not want. As a result, we use our target network as our estimate of $max_a Q(s', a)$ on the right hand side of Equation 2.2 during training instead.

In the initial phases of training our network's estimates of rewards may also greatly diverge. As a result the authors of the DQN also found that limiting the values of gradients that are backpropagated between $-1, 1$ reduces the variation of the network and allows it to converge faster.

All of these small improvements allowed the DQN to perform at above human levels on a series of 49 atari games [13].

Drawbacks

Drawbacks of the DQN are numerous and varied. It requires an immense amount of data from an environment, on the order in the tens of millions of frames to train a single agent. This translates to the network requiring nearly 50 hours of game time to learn to play a simple game such as pong or breakout [23]. The difficulty of these problems comes from the how diverse the states

Like many other neural network based reinforcement learning solutions, it is also highly sensitive to initial conditions and the parameters we set for our network such as its learning rate. For example even setting the paddle position differently can severly hamper its performance [24]. It also means that without the right set of hyper parameters, our model will fail to learn an appropriate policy in the first place [23]. More strangely, multiplying the rewards of our network by a scalar value can change it behaviour [23].

2.1.2 Alternatives to the DQN

Other methods that are now commonly used in deep reinforcement learning research include policy gradients, and actor-critic methods. Neither of these improvements are used within this capstone. Some improvements that were explored, such as prioritized experience replay and dueling q-networks, will be touched upon later.

Improvements that are utilized in this capstone are the ideas of the Double-DQN(DDQN)[25] and prioritized experience replay[26].

Prioritized experience replay improves on the original by looking only at the differences between the reward values our Q-network estimates for a given state versus the real obtained rewards; the idea being Q-value estimates that greatly diverge from what our agent observes should be trained on more than estimates that are correct. For each experience, we then calculate the error between the network and reality. This error is therefore used to balance a modified binary heap, allowing us to efficiently sample only experiences that have the highest error.

The DDQN aims to overcome systemic bias and value overestimation in the DQN. For example imagine a scenario in which the true Q-values for a given state are identical, but the network however is inherently noisy in its estimates. During an update step, because of the max in $\max_a Q(s,a)$, the action with the largest positive error will be selected. This, over time, can lead to that particular action to be favoured. The proposed solution is to instead use an alternative Q-network to find the index of action that is maximised, and another one with which to calculate actual Q-values.

$$Q_1(s,a) = r_t + \gamma Q_2(s', argmax_a Q_1(s',a)) \tag{2.3}$$

Here in this equation Q_1 represents one estimate of our Q-values while Q_2 represents the estimates from our secondary network. Since we utilize two Q-networks, hence the name of the algorithm. On atari this allows our network to achieve almost double the scores of the original DQN architecture. The target networks in the DQN can be used to estimate values of Q_2.

2.2 Object Detection

In order to understand the history of object detection and localization it is necessary to revisit the PASCAL VOC [27] challenge and ImageNet ILSVRC [28] of the early 2010s. The main metrics to watch out for in object detection are Intersection Over Union (IOU) scores, defined as the intersection between the proposed boxes and the actual ones [29]. The other metric is mAP or mean average precision. This measures that for every given proposed object, what percentage of the classes that are then predicted are correct. In this capstone as we are only concerned with drawing bounding boxes, we will focus mainly on the IOU scores of our method.

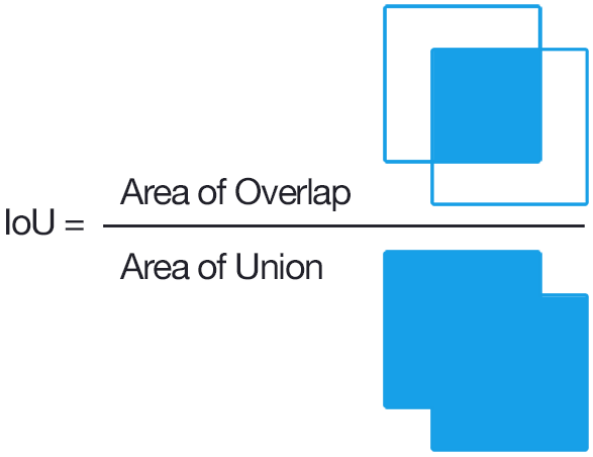

FIGURE 2.2: How IOU scores are calculated [29]

2.2.1 R-CNN

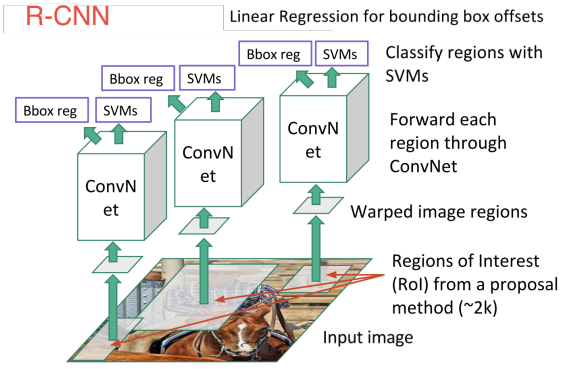

FIGURE 2.3: R-CNN Overview [30]

R-CNN was the first comprehensive solution to object detection that utilized deep learning [30]. The main insight was to use a pretrained CNN to extract features and to perform classification over smaller windows. Potential regions were calculated using selective search. Selective search groups together pixels which have similar colours and intensities. Running this several iterations generates 2000 regions per image after a minute of run time. Each proposed image is resized and run through our pretrained CNN. The extracted features are then classified via an ensemble of Support Vector Machines(SVM) which are a classicial machine learning algorithm used in classificaiton.

FIGURE 2.4: Selective search in action [30]

Drawbacks to this approach was the difficulty in training. As it was composed of multiple components, each segment had to be trained on its own. The significant run time of selective search also prevented this network from training quickly [31].

2.2.2 Fast R-CNN

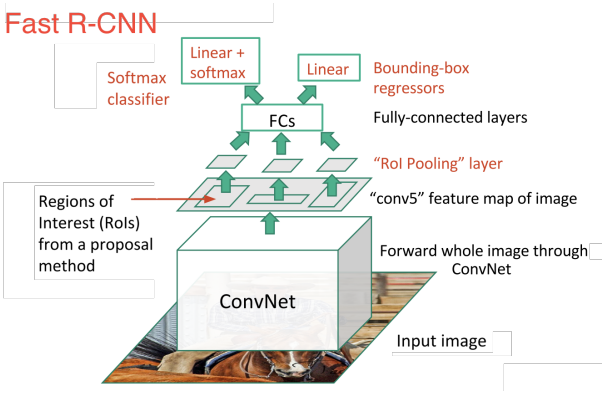

FIGURE 2.5: Fast R-CNN Overview [31]

Fast R-CNN attempted to improve things by sharing as many resources as possible. It does so by running the CNN only once and sharing that block of convolutional features [31]. The old SVMs were now also replaced with fully connected

neural network. This network however still relied upon selective search in the original image to find regions of interest. Each proposed region from search would then be projected onto a block from the convolutional block computed earlier.

An important concept that Fast R-CNN introduced was Region of Interest (ROI) Pooling [31]. This was a method used to ensure that proposed feature blocks would be of a certain size. ROI pooling works by subdividing a block into equal sized areas as best as it can, then finding the max value in each block. For each region that is proposed by selective search, we find the corresponding section of features on the convolutional block and ROI pool it into a fixed sized. This fixed sized vector is then passed onto our classication engine. As a result this method greatly improved the speed of detection by limiting the times the CNN is used.

2.2.3 Faster R-CNN

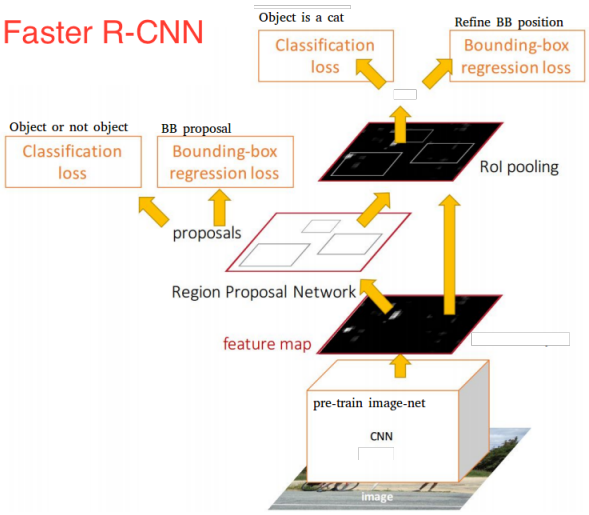

FIGURE 2.6: Faster R-CNN Overview [1]

Further developments sought to get rid of selective search entirely. In Faster-RCNN selective search is replaced by a region proposal network (RPN). The RPN acts as follows; we first preselect a series of k possible shapes with bounding boxes of varying sizes. The RPN will then scan through a window of our block of convolutional features, rating the likelihood there existed an object within one of the k possible bounding box shapes within the original image. The most likely features are then once again ROI pooled and passed unto a fully connected layer.

Faster-R-CNN remains relevant to our discussion because it serves as a baseline for most object detection tasks. While some newer developments may be faster, they rarely if ever outperform Faster-R-CNN's baseline performance [32]. Our proposed RL solution to object localization can be used to replace the RPN while limiting the number of candidate windows.

2.2.4 YOLO/SSD

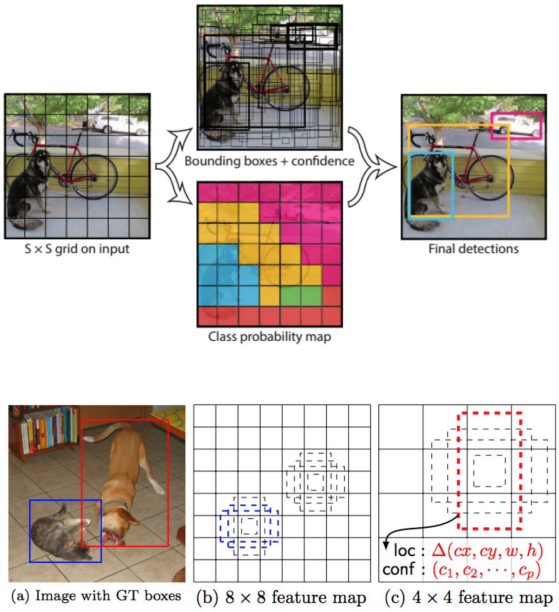

FIGURE 2.7: YOLO [19] and SSD [2] Overview

You Only Look Once (YOLO) and Single Shot Detector (SSD) are other methods of object detection. YOLO and SSD attempt to tackle the problem from an entirely different point of view. Previous systems would always generate proposed regions and then pass them into a classifier. YOLO and SSD attempt to do both steps simultaneously. YOLO does so by dividing our image into a large grid. It then predicts a set of proposed bounding boxes with coordinates for each grid, alongside a class prediction for the box as a whole. The system then intelligently combines all this information together, drawing a box over entire sets of grids and corrects them slightly in order to localize them.

SSD achieves similar results by modifying the RPN step of Faster R-CNN. It does so by not only proposing a series of bounding boxes directly from the block of convolutional features, but also running each box through a classifier. This skips the

need for ROI pooling layer. The main issue here is that there will be an excess of proposed boxes during training. Thus we only select the box with the highest IOU to be the correct one.

2.2.5 Limitations

As of 2018, state of the art models still only achieve unremarkable mAP scores on MS COCO object detction challenge (40%)[19]. This means that out of all the times the model was confident it detected a particular image, more than half the time it has actually detected the class wrongly.

2.3 Reinforcement Learning and Object Detection

The focus of this capstone is on the two papers *Active Object Localization* by Caicedo [20] and *Hierarchical Object Detection* by Bellver [33]. Both formulated the search for bounding boxes as a markov decision process and aimed at reducing the number of proposed boxes as compared to other object detection frameworks. While ultimately their performance falls short of other previously mentioned systems these are still worth revisiting for combining two diverging fields of machine learning. These models also recieve less study as compared to more generalized object detection framework, perhaps with further study they could exceed or reach parity in performance with other methods.

The main difference between the two papers are in the sets of actions their network can undertake. In Caicedo's model, the bounding box window is able to move vertically and horizontally across our canvas while also shrinking and growing if necessary. In Bellver's model, every action aims to shrink the bounding box, this leads it to be considered a form of hierarchical search.

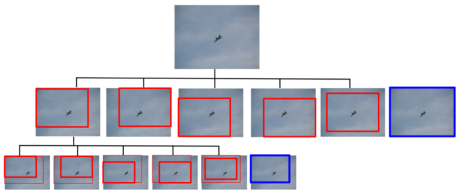

FIGURE 2.8: Sample of actions undertaken by Bellver [33]

The features of each network also slightly differ. Caicedo extracts a new set of features at each time step by resizing the current bounding box and running it through a pre trained CNN. Bellver on the other hand also gives the option of pre-computing a single block of convolutional features that are shared for each time step. This means for a proposed bounding box we have to extract the block of corresponding features from its computed convolutional block and use ROI pooling before passing it onto our Q-network. Otherwise there still is the option of computing a new set of features for each time step as well.

From empirical evidence it appears that computing a new set of convolutional features at each time step yields better performance at the cost of run time [33]. However as our RL agent reduces the search space for bounding boxes significantly this difference in compute is almost negligible. Both also differ from the DQN by only keeping a state vector of the previous four actions as integers, rather than keeping a feature representation of the previous bounding boxes.

Both also structure their environments in a similar fashion. Rewards are kept to be binary values to improve predictability and accuracy of the Q-network. This means whenever the Q-network proposes a bounding box that has higher IOU values it is rewarded the same amount regardless of the magnitude of change. Once a certain IOU threshold is met, both environments terminate and emit a significantly larger reward. Otherwise, both have a cut off number of timesteps, after which the environment will terminate on its own.

Overall Bellver's model is able to find the majority of objects within 10 time steps, two orders of magnitude reduction in bounding box proposals compared to frameworks such as R-CNN.

Chapter 3

Experiments and Methodology

Each experimental section delves deeper into the methods, results and discussions of each trial. However in general all three share a similar overview.

Additionally each experiment consisted of finding a suitable dataset, proposing a network that could potentially solve our problem and experimenting with its hyperparameters for several epochs. An epoch is defined as a single run through of the dataset, while hyperparameters are the values with which we have to determine for our network such as its learning rate.

Rather than rely on IOU scores or class labels from the training data we primarily rely on confidence signals from a pretrained CNN network. These are obtained by running a softmax layer over the output of the CNN.

$$\text{softmax}(x)_j = \frac{e^{x_j}}{\sum_i^K e^{x_i}}, j \in \{1, \ldots, K\} \tag{3.1}$$

Softmax aims to normalize a vector in an exponential fashion. This is because the values within a neural network output can vary dramatically. Normalizing these in a linear fashion would there lead us to always appear very confident in our network's output. Therefore by normalizing with respect to the exponential we can more accurately reflect the confidence of our network and have their intervals be more accurate. We use the highest value of the softmax as our confidence score, regardless of its corresponding label.

The Q-network functions similarly as to the previously discussed RL based object detection solutions, but instead used to maximise confidence scores.

Rewards were also kept consistent between experiments. Rewards can be obtained between each step of the Q-network or when it terminates.

$$R_{step} = \begin{cases} +1 & \text{if } confidence_{new} > confidence_{old} \\ -1 & \text{otherwise} \end{cases} \tag{3.2}$$

$$R_{trigger} = \begin{cases} +3, & \text{if confidence} \geq \eta \\ -3, & \text{otherwise} \end{cases} \tag{3.3}$$

Where η is a preset confidence threshold.

The actions taken by the Q-network are directly copied from Bellver. The scale which our network shrinks its bounding box estimates is also another hyperparameter that is empirically determined. All of these experiments used a scale of $\frac{3}{4}$ for their actions. This produces successive bounding boxes with some degree of overlap, which has shown to give better performance [33]. State history was also kept to a maximum of the immediate 4 previous frames or actions.

Like most reinforcement learning problems Huber Loss[34] is also used instead of either the more typical choices of cross entropy or mean squared error.

$$Loss_{Huber} = \begin{cases} 0.5 * x^2, & \text{if } |x| \leq \delta \\ 0.5 * \delta^2 + \delta * (|x| - \delta), & \text{otherwise} \end{cases} \tag{3.4}$$

Huber loss acts as linear loss function for small values, but a quadratic loss function for larger values. This is dependent on the value for δ, set to 1.0 in most cases. The choice of Huber allows to be more harsh on more wrong results, but less harsh on values which are less wrong. This in turn allows our network to adapt the rate at which it trains. This is because we want to perturb our network less if it is already reasonably accurate in its estimates. Unless otherwise stated each layer of all networks utilized the ReLU activation function.

Additionally none of the proposed bounding boxes are pased unto trained regressors. In all other object detection frameworks these coordinates are pased onto a regressor in order to correct them. However this is only possible given a ground truth of values from which we want the values to be corrected into.

However the bounding boxes of the altered images were never used during training.

3.1 MNIST DQN

The goal of this initial experiment is to draw the bounding boxes of an MNIST digit after it has been placed onto a larger canvas. This was chosen because

FIGURE 3.1: Sample images generated for the first experiment

To generate the data, a blank 75x75 canvas was generated. As each digit was of size 28x28, a random width and height position were chosen between $0 - 47$. Afterwards each image was copied over to that randomized coordinate.

The aim of this experiment was to create a Q-network capable of localizing to a single MNIST digit on a blank canvas. Using a basic CNN that is trained to recognize digits from the original MNIST dataset, we pass a collection of 4 image crops to a modified version of the original Atari DQN.

The confidence scores were obtained from a pre-trained classifier that was trained on the original unaltered MNIST data. For this experiment all numbers used regardless of what their value was.

3.1.1 Methods

Our experience replay module is created at a size of $100,000$ experiences. However in this example these were not populated ahead of time. The architecture of our q-network is as follows. Its input in this case is a stacked 4 frames of resized candidate bounding box images. This initial network also lacks a target network with which we calculate our q-values upon training.

Each layer was initialized using random uniform weights.

RMSProp was chosen as the optimizer in this case.

Each image is treated as an episode of the game, lasting at most 10 time steps. Training time was about 1 hour per 1000 episodes on a single GTX 1080 GPU with

Type	Size	Filters	Kernel Size	Stride	Padding
Input	4x28x28	N.A.	N.A	N.A	N.A
Conv1	32x21x21	32	8x8	1	0
Conv2	64x9x9	64	4x4	2	0
Conv3	32x7x7	32	3x3	1	0
fc1	512	N.A	N.A	N.A	N.A
fc2	5	N.A	N.A	N.A	N.A

TABLE 3.1: Overview of the q-network

Hyperparameter	Value
Learning Rate	0.0001
γ	0.99
ϵ_{start}	0.9
ϵ_{end}	0.05
ϵ_{decay}	60000
η	0.5
total moves	10
batch size	128

TABLE 3.2: Hyperparameters

PyTorch 0.3 and CudNN 7.0. The value for ϵ_{decay} was chosen as to allow our q-network to experience each image from the MNIST training dataset at least once.

3.1.2 Results

This network appears to perform no differently than a randomized agent after mild training. Both the number of actions taken per episode and total rewards earned are noisy graphs with no perceptiple trends.

3.1.3 Discussion

While this network performs poorly there are perhaps several reasons why. Firstly the features obtained by the q-network's internal CNN maybe insufficient to produce a localization policy. As modified version of this network was used to play Atari games, this is highly unlikely.

Additionally this network stores a relative abundance of negative experiences. During the random seeding of the memory module more than 90% of experiences did not lead to a positive reward. This served as the underlying motivation for using a prioritized experienced replay module the next experiment.

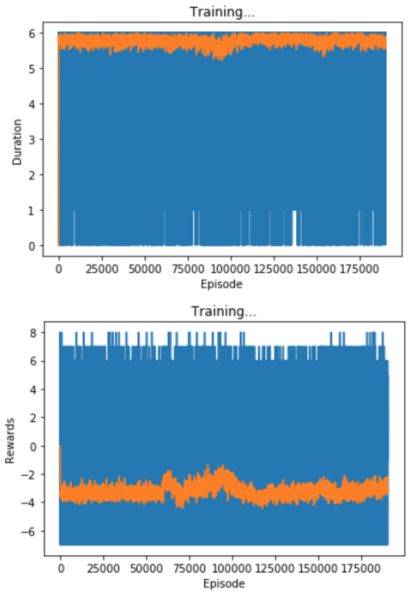

FIGURE 3.2: Length of actions and rewards per episode

A solution that would have made our training task perhaps easier would have placing multiple images onto our canvas. This would have meant that for any given random action the probability our network would see a image would increase. This would also allow us to experiment with the degree of overlap between images and see how that affects our detection network. However as our network was yet to solve this initial task, no further data was generated until this task was to be solved.

3.2 MNIST DDQN + Experience Replay

The goal of this experiment was to see whether alternative training methods would yield more conclusive results. An addendum was that the prioritized experience replay module would be seeded with actions made by a fully randomized agent before hand. Additionally by training using the DDQN methodology the hope was that the Q-value estimates would be more accurate.

3.2.1 Methods

The only change to our hyperparameters was the reduction of total time steps before termination to 5. This was motivated by observations of how an agent is able to localize to a digit in less than 3. This would also hopefully reduce the number of

negative experiences the Q-network will experience. The target network was also updated at a frequency of 1000 timesteps.

3.2.2 Results

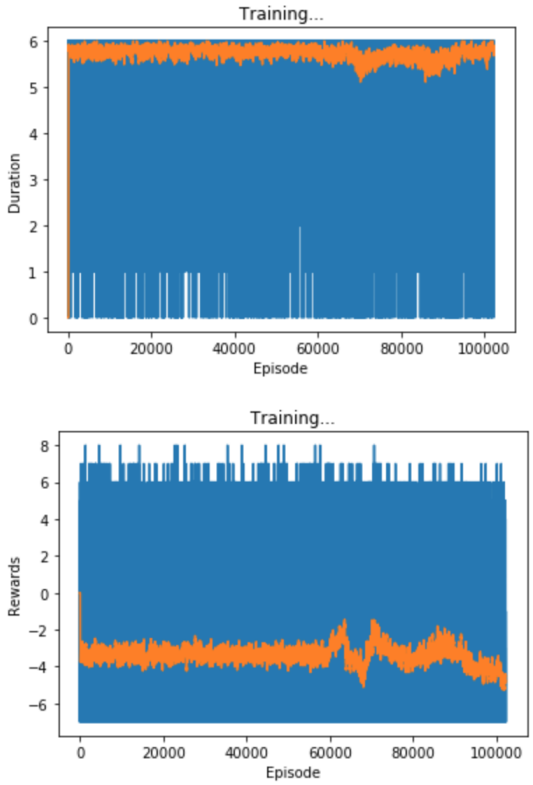

FIGURE 3.3: Length of actions and rewards per episode

As compared to the agent before, there appears to be some degree of improvement near episode 6000. This is because we reach the number of episodes as stated by ϵ_{decay}. However this quickly diminishes after more episodes. This is potentially indicative of a network that forgets its values due to new experiences, thus a lower learning rate and longer exploration period may have proved to be more useful.

3.2.3 Discussion

In both experiments so far, it was clear that the network simply had too many negative examples. Even with a prioritized experience replay module it was not clear that the network fully learnt to localize to anything of interest upon the canvas.

3.3 Pascal VOC 2012+2007

Inspired by Bellver's work this experiment attempted to find a network that would localize onto images which contained planes. The hope was that by only seeing a specific set of images our network would show promise, before we move the more complex task of localizing an image with respect to multiple classes.

Compared to the previous dataset, PASCAL VOC both contains richer information within each image and contains larger objects overall. This means a significant proportion of the images require little to no zooming in the first place for an object to be considered localized. Recognizing these factors, the following experiments adapts code from https://github.com/imatge-upc/detection-2016-nipsws/ which was the repository for the Bellver paper.

The main difference between the 2012 and 2007 dataset are the sizes of each image and the number of images for each class.

3.3.1 Methods

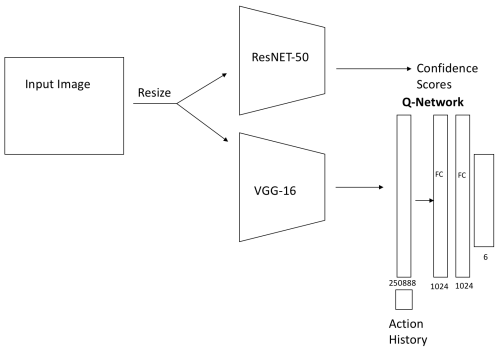

FIGURE 3.4: Architecture overview for this experiment

Confidence scores were obtained via ResNet-50 [8] pretrained on ImageNet. ResNet differs from other classification networks in that it aims to find what is termed the *residuals* between each layer of a neural network. The observation was that neural networks seemed unable to find an identity mapping between layers, if it could do so we could simply stack an infinite number of layers together without performance degradation. Therefore in ResNet we add the input from the previous layer to the

output of our step function, allowing us to model the differences between two layers rather than a direct mapping between them.

Empirically this yielded significantly better performance in classification and allowed for even deeper layers [8].

Since this network is trained only as a regular DQN, our experience replay module is only sampled randomly. Its size is also significantly smaller at only 1000 experiences.

For this experiment the proposed bounding box image was passed into VGG-16 for feature extraction, rather than reuse a single block convolutional features. This was motivated by the suggestions within the Bellver paper.

Our optimizer in this case was Adam with a learning rate of 0.001. As we were only testing the localization capability of the network rather than its general performance, we restricted to only images with planes. The model was trained for 20 epochs, taking around 20 hours to do so.

This model was created using Keras with a TensorFlow backend. Training time was significantly slower at around $2 - 5$ images per second.

γ was also reduced to 0.9, meaning our network accounts for less of its future rewards. η was increased to 0.8, accounting for the number of images in which our network appears to not take any action.

3.3.2 Results

FIGURE 3.5: IOU scores over time

From a few small epochs it appears that our IOU scores of proposed bounding boxes appears to increase. There appears to be some trendline upwards. This is

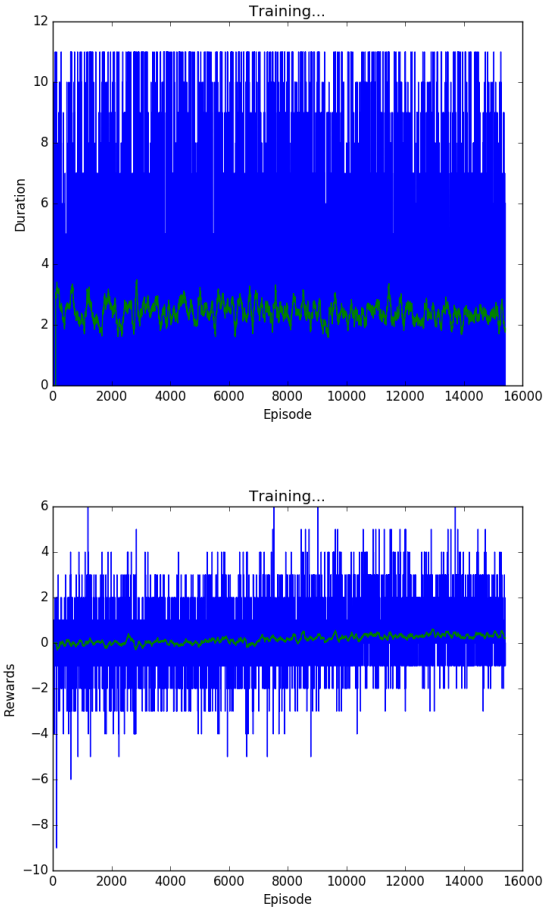

FIGURE 3.6: Rewards and Durations over training

inspite of the fact that this network was never told to optimize for this metric, nor did it ever recieve signals about the IOU scores of the bounding boxes it proposed.

3.3.3 Discussion

Qualitatively this network is largely a success. Looking at a few sample outputs it is clear the network has gained some ability to localize to what it believes to be a plane.

Here the proposed bounding boxes over the planes are of reasonable accuracy and do not ignore important components of the image.

The network is not without its faults. Often times our Q-network becomes distracted by other items in the scene. Objects in the foreground that are not planes occaisionally attracts its attention. This is perhaps because our confidence scores are generated indiscriminately by our classifier without regards to what object we actually want detected, so this result should be expected.

FIGURE 3.7: Examples of proposed bounding boxes

FIGURE 3.8: Examples of proposed bounding boxes

Compared to both Bellver and Caicedo this particular Q-network underperforms significantly. The Bellver paper did not include IOU performance of its model.

Model	Value
Ours	0.22
Caicedo	0.5

TABLE 3.3: Comparison of IOU Scores

Most of this performance difference arises because this Q-network tends to emit bounding boxes which are significantly larger. The boxes it proposes need only to be big enough for ResNet-50 to classify them. Depending on the intended usage of this object detection system, finding a slightly wider bounding box may not hamper its performance significantly.

As shown in our Section 3.3.2 the IOU score of our model also appears to increase with time. This shows that creating a network which optimizes for confidence in object classification has some correlation with proposes bounding boxes of increasing IOU.

Of note the category of planes in PASCAL VOC is also exceptionally broad. It includes airliners, fighter jets and even rotrary planes. More often than not the most

salient portion of the plane are its wheels. Thus our network occaisionally also localizes to only the wheels of a plane.

Improvements to this network would have involved a more rigorous hyperparameter search. As reinforcement learning problems are particularily sensitive to initial conditions and hyper parameters, values such as η and the learning rate could have been better tuned as to suite our needs.

While our network appears to perform well on planes, it is still unclear how it would perform on other classes within PASCAL VOC. This experiment also leaves it unclear whether our reinforcement learning method can be used to propose regions of multiple classes simultaneously.

Improvements to speed up the network could also be reusing VGG-16 features for the classification confidence. Since it is clear from Faster R-CNN that the objectness score can be directly estimated via convolutional feature maps, using these directly instead of a separate architecture could potentially lead to a significant speed up.

Other factors such as a prioritized experience replay module or dropout could have also been considered. Most importantly other reinforcement learning algorithms could have been employed to train our network.

Chapter 4

Conclusions

This capstone thesis explores the applications of Deep RL agents in partially observed markov decision processes outside of videogames. Our goal was to have Q-network look only at images and be able to localize to important objects, via the help of a confidence network that is trained on an entirely different set of data. The main contributions thus were the implementation of such a method and some evidence of its efficacy. This capstone illustrates that reinforcement learning algorithms have a much wider range of applications than just on videogames and can be applied to unsupervised machine learning tasks.

While the performance of this model may still leave much to be desired, there remains immense potential in this algorithm that is yet to be explored. This model still localizes to objects we may not necessarily care about currently, nor does it even exceed the performance of current state of the art models. This is because the model does not directly have access to IOU scores with which to optimize upon. Moreover, the bounding boxes it tends to produce are usually larger than the ground truth labels because this was deemed to be good enough for classification. The goal was to propose a system that could achieve some success in the domain of object detection and localization, not to neccessarily beat state of the art solutions to the problem. The fact that our model appears to improve its baseline IOU scores over time without directly optimizing the value is a success in and of itself. The hope is that with such a model, researchers can design object detection frameworks that no longer require vast amounts of labelled data in order to train their models. This opens up other avenues of research and data collection without the need for humans to manually label bounding boxes or classes ahead of time.

One contention that has arisen with this methodology is that neural networks do not work well with uncertainty. As illustrated by recent explorations of adversarial attacks [35], in uncertain situations a neural networks tend to appear more confident than they should have reason to. Taking into account adversarial examples, researchers have been able to convince a network that for an image which it originally classifies as a panda with 60% confidence to be a gibbon with 99% certainty [35]. As such regardless of what images and bounding boxes we feed to our confidence network it will tend to output a class with some degree of confidence. Neural networks are thus arrogant in that narrow sense. Moreover its not entirely certain whether showing half an image of a plane will lead our confidence network to be 50% certain it is seeing a car.

4.1 Frontiers

Other related works in the field include a tree based approach to tackling reinforcement learning and object detection [36]. This has allowed this particular reinforcement learning agent to consider multiple bounding boxes with different degrees of confidence simultaneously.

Another important field that this capstone did not touch upon was the task of image segmentation. Models such as Mask R-CNN [32] are able to more accurately label an object on a per pixel level. Whether a reinforcement learning approach that is unsupervised remains to be seen.

Bibliography

[1] S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 39, no. 6, pp. 1137–1149, 2017, ISSN: 01628828. DOI: 10.1109/TPAMI.2016.2577031. arXiv: 1506.01497.

[2] W. Liu, D. Anguelov, D. Erhan, C. Szegedy, S. Reed, C. Y. Fu, and A. C. Berg, "SSD: Single shot multibox detector", in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9905 LNCS, 2016, pp. 21–37, ISBN: 9783319464473. DOI: 10.1007/978-3-319-46448-0_2. arXiv: 1512.02325.

[3] T. Y. Lin, M. Maire, S. Belongie, J. Hays, P. Perona, D. Ramanan, P. Dollár, and C. L. Zitnick, "Microsoft COCO: Common objects in context", in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 8693 LNCS, 2014, pp. 740–755, ISBN: 978-3-319-10601-4. DOI: 10.1007/978-3-319-10602-1_48. arXiv: 1405.0312.

[4] R. Mundra, A. Ped-Dada, R. Socher, and Q. Yan, *Part 3: Neural Nets*, 2017. [Online]. Available: http://web.stanford.edu/class/cs224n/lecture{_}notes/cs224n-2017-notes3.pdf (visited on 09/24/2017).

[5] D. P. Kingma and J. L. Ba, "Adam: a Method for Stochastic Optimization", *International Conference on Learning Representations 2015*, pp. 1–15, 2015, ISSN: 09252312. DOI: http://doi.acm.org.ezproxy.lib.ucf.edu/10.1145/1830483.1830503. arXiv: 1412.6980.

[6] G. E. Hinton, N. Srivastava, and K. Swersky, "Lecture 6e- rmsprop: Divide the gradient by a running average of its recent magnitude", *COURSERA: Neural Networks for Machine Learning*, pp. 26–31, 2012. [Online]. Available: https://goo.gl/RsQeis.

[7] I. J. Goodfellow, D. Warde-Farley, M. Mirza, A. Courville, and Y. Bengio, "Maxout Networks", [Online]. Available: http://proceedings.mlr.press/v28/goodfellow13.pdf.

[8] K. He, X. Zhang, S. Ren, and J. Sun, "ResNet", *arXiv preprint arXiv:1512.03385v1*, vol. 7, no. 3, pp. 171–180, 2015, ISSN: 1664-1078. DOI: 10.3389/fpsyg.2013.00124. arXiv: 1512.03385. [Online]. Available: http://arxiv.org/pdf/1512.03385v1.pdf.

[9] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Alexnet", *Advances In Neural Information Processing Systems*, pp. 1–9, 2012, ISSN: 10495258. DOI: http://dx.doi.org/10.1016/j.protcy.2014.09.007. arXiv: 1102.0183.

[10] A. Karpathy and F. F. Li, *CS231n Convolutional Neural Networks for Visual Recognition*. [Online]. Available: https://cs231n.github.io/convolutional-networks/ (visited on 03/25/2018).

[11] F. Chollet, "Xception: Deep Learning with Separable Convolutions", *arXiv preprint arXiv:1610.02357*, pp. 1–14, 2016, ISSN: 1063-6919. DOI: 10.1109/CVPR.2017.195. arXiv: 1610.02357. [Online]. Available: https://arxiv.org/abs/1610.02357.

[12] C. Watkins, "Learning from Delayed Rewards", *Robotics and Autonomous Systems*, vol. 15, no. 4, pp. 233–235, 1995, ISSN: 09218890. DOI: 10.1016/0921-8890(95)00026-C. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/092188909500026C.

[13] V. M. Deepmind, "Human-level control through deep reinforcement learning", *IJCAI International Joint Conference on Artificial Intelligence*, vol. 2016-Janua, no. 7540, pp. 2315–2321, 2016, ISSN: 10450823. DOI: 10.1038/nature14236. arXiv: 1604.03986. [Online]. Available: http://www.nature.com/doifinder/10.1038/nature14236.

[14] D. Silver and D. Hassabis, *AlphaGo: Mastering the ancient game of Go with Machine Learning*, 2016. [Online]. Available: https://research.googleblog.com/2016/01/alphago-mastering-ancient-game-of-go.html.

[15] J. Zhao, G. Qiu, Z. Guan, W. Zhao, and X. He, "Deep Reinforcement Learning for Sponsored Search Real-time Bidding", 2018. arXiv: 1803.00259. [Online]. Available: https://arxiv.org/abs/1803.00259.

[16] Q. Cai, A. Filos-Ratsikas, P. Tang, and Y. Zhang, "Reinforcement Mechanism Design for e-commerce", 2017. arXiv: 1708.07607. [Online]. Available: http://arxiv.org/abs/1708.07607.

[17] F.-F. Li, A. Karpathy, and J. Johnson, "Lecture 8 - 1 Feb 2016 Lecture 8: Spatial Localization and Detection", [Online]. Available: http://cs231n.stanford.edu/slides/2016/winter1516{_}lecture8.pdf.

[18] A. Borji, M. M. Cheng, H. Jiang, and J. Li, "Salient Object Detection : A Survey", *eprint arXiv*, pp. 1–26, 2014, ISSN: 1941-0042. DOI: 10.1109/TIP.2015.2487833. arXiv: arXiv:1411.5878v1.

[19] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "(2016 YOLO)YOU ONLY LOOK ONCE: UNIFIED, REAL-TIME OBJECT DETECTION", *Cvpr 2016*, pp. 779–788, 2016, ISSN: 10636919. DOI: 10.1016/j.nima.2015.05.028. arXiv: 1506.02640v1.

[20] J. C. Caicedo and S. Lazebnik, "Active Object Localization with Deep Reinforcement Learning", [Online]. Available: https://www.cv-foundation.org/openaccess/content{_}iccv{_}2015/papers/Caicedo{_}Active{_}Object{_}Localization{_}ICCV{_}2015{_}paper.pdf.

[21] Y. Rao, J. Lu, and J. Zhou, "Attention-aware Deep Reinforcement Learning for Video Face Recognition", [Online]. Available: http://openaccess.thecvf.com/content{_}ICCV{_}2017/papers/Rao{_}Attention-Aware{_}Deep{_}Reinforcement{_}ICCV{_}2017{_}paper.pdf.

[22] R. Kaplan, C. Sauer, and A. Sosa, "Beating Atari with Natural Language Guided Reinforcement Learning", pp. 1–13, 2017. arXiv: 1704.05539. [Online]. Available: http://arxiv.org/abs/1704.05539.

[23] Alexirpan, *Deep Reinforcement Learning Doesn't Work Yet*. [Online]. Available: https://www.alexirpan.com/2018/02/14/rl-hard.html (visited on 03/26/2018).

[24] K. Kansky, T. Silver, D. A. Mély, M. Eldawy, M. Lázaro-Gredilla, X. Lou, N. Dorfman, S. Sidor, S. Phoenix, and D. George, "Schema Networks: Zero-shot Transfer with a Generative Causal Model of Intuitive Physics", [Online]. Available: https://www.vicarious.com/wp-content/uploads/2017/10/icml2017-schemas.pdf.

[25] H. V. Hasselt, A. C. Group, and C. Wiskunde, "Double Q-learning", *Nips*, pp. 1–9, 2010.

[26] V. Mnih, K. Kavukcuoglu, D. Silver, A. A. Rusu, and J. Veness, "Prioritized Experience Replay", *International Conference in Machine Learning*, vol. 4, no. 7540, p. 14, 2015, ISSN: 0028-0836. DOI: 10.1038/nature14236. arXiv: 1502.04623. [Online]. Available: http://arxiv.org/abs/1507.01526{\%}5Cnhttp://dx.doi.org/10.1007/978-3-642-27645-3{_}2{\%}5Cnhttp://arxiv.org/abs/1112.6209{\%}5Cnhttp://arxiv.org/abs/1509.06461{\%}5Cnhttp://www.arxiv.org/pdf/1509.06461.pdf{\%}5Cnhttp://arxiv.org/abs/1511.06295{\%}5Cnhttp://arxiv.org/abs/151.

[27] M. Everingham, L. Van Gool, C. K. Williams, J. Winn, and A. Zisserman, "The pascal visual object classes (VOC) challenge", *International Journal of Computer Vision*, vol. 88, no. 2, pp. 303–338, 2010, ISSN: 09205691. DOI: 10.1007/s11263-009-0275-4.

[28] Jia Deng, Wei Dong, R. Socher, Li-Jia Li, Kai Li, and Li Fei-Fei, "ImageNet: A large-scale hierarchical image database", in *2009 IEEE Conference on Computer Vision and Pattern Recognition*, 2009, pp. 248–255, ISBN: 978-1-4244-3992-8. DOI: 10.1109/CVPRW.2009.5206848. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5206848.

[29] A. Kovashka, *University of Pittsburgh: Error HTTP 404 - File not found*. [Online]. Available: https://people.cs.pitt.edu/{~}kovashka/cs1699/hw4.html (visited on 03/25/2018).

[30] R. Girshick, J. Donahue, T. Darrell, and J. Malik, "R-CNN", *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, pp. 580–587, 2014, ISSN: 10636919. DOI: 10.1109/CVPR.2014.81. arXiv: 1311.2524.

[31] R. Girshick, "Fast R-CNN", in *Proceedings of the IEEE International Conference on Computer Vision*, vol. 2015 Inter, 2015, pp. 1440–1448, ISBN: 9781467383912. DOI: 10.1109/ICCV.2015.169. arXiv: 1504.08083.

[32] K. He, G. Gkioxari, P. Dollar, and R. Girshick, "Mask R-CNN", in *Proceedings of the IEEE International Conference on Computer Vision*, vol. 2017-Octob, 2017, pp. 2980–2988, ISBN: 9781538610329. DOI: 10.1109/ICCV.2017.322. arXiv: 1703.06870.

[33] M. Bellver, X. Giro-i Nieto, F. Marques, and J. Torres, "Hierarchical Object Detection with Deep Reinforcement Learning", *Nips*, no. Nips, 2016. arXiv: 1611.03718. [Online]. Available: http://arxiv.org/abs/1611.03718.

[34] J. Cavazza and V. Murino, "Active Regression with Adaptive Huber Loss", *arXiv:1606.01568 [cs]*, pp. 1–14, 2016. arXiv: 1606.01568. [Online]. Available: http://arxiv.org/abs/1606.01568.

[35] X. Yuan, P. He, Q. Zhu, R. R. Bhat, and X. Li, "Adversarial Examples: Attacks and Defenses for Deep Learning", 2017. arXiv: 1712.07107. [Online]. Available: http://arxiv.org/abs/1712.07107.

[36] J. ZEQUN, "SCALE-ROBUST DEEP LEARNING FOR VISUAL RECOGNITION", [Online]. Available: http://scholarbank.nus.edu.sg/handle/10635/134430.