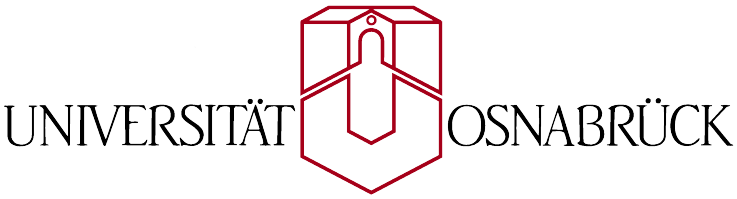

Controlling Self-Driving Race Cars with Deep Neural Networks

UNIVERSITY OF OSNABRÜCK

DEPARTMENT OF NEUROINFORMATICS

BACHELOR'S THESIS

Author:
Christoph Stenkamp

Supervisors:
Prof. Dr. Gordon Pipa
Leon Sütfeld

Osnabrück,
August 12, 2017

Abstract

This Thesis will be written in the next two months, and I'm pretty scared about that.
TODO: sobald der komplette text steht bei den Formeln auf die nicht referenziert wird die nummern weg machen (equation*)

Preface

This document was written as the author's bachelor thesis at the department of neuroinformatics at the University of Osnabrück during summer 2017 and is an original and independent work by the author Christoph Stenkamp.

Christoph Stenkamp
Osnabrück, August 12, 2017

Acknowledgements

Thanks to my parents, Marie, my supervisors, and my friends.. . .

"There are no surprising facts, only models that are surprised by facts; and if a model is surprised by the facts, it is no credit to that model."

Eliezer Yudkowsky

Contents

List of Figures

List of Tables

List of Algorithms

List of Abbreviations

The abbreviations used throughout the work are compiled in the following list below. Note that the abbreviations denote the singular form of the abbreviated words. Whenever the plural forms is needed, an s is added. Thus, for example, whereas ANN abbreviates *artificial neural network*, the abbreviation of *artificial neural networks* is written ANNs.

ANN	**A**rtificial **N**eural **N**etwork
CNN	**C**onvolutional (artificial) **N**eural **N**etwork
CPU	**C**entral **P**rocessing **U**nit
DDPG	**D**eep **D**eterministic **P**olicy **G**radient - Network
DQN	**D**eep-**Q**-**N**etwork
GUI	**G**raphical **U**ser **I**nterface

List of Symbols

For my friends, family, and especially Marie.

Chapter 1

Introduction

"sollte etwa 10% der Gesamtarbeit ausmachen"

1.1 Motivation

1.1.1 Problem Domain

1.1.2 Goal of this thesis

1.2 Research Questions

1.3 Reading Guidelines

Chapter 2

Reinforcement Learning

As the task as hand was not only to provide a reinforcement learning agent, but also to convert a game itself into something the agent can successfully play, I will in this chapter go into detail about Reinforcement Learning in general, to give insights into why I did what I did. Also, I will try to keep this stuff as general as possible, getting into detail when speaking about the used algorithms. [The sense of this chapter is to give an intro of MDPs and RL. It shall also go into enough details on how to specify an MDP such that an RL agent can learn on it, because a big part of the work was exactly that. It's supposed to end with SARSA and Q-learning as the two Ideas on how to perform RL]

2.1 Reinforcement Learning Problems

Machine Learning can mainly be subdivided into three main categories: Supervised Learning, Unsupervised Learning, and Semi-supervised learning. The first deals with direct classification or regression using labelled data (i.e. it uses pairs of datapoints with their corresponding category or value). In unsupervised learning, no such label exists, and the data must be clustered into meaningful parts without any knowledge, by for example grouping objects by similarity of their properties.
What will be mainly considered in this thesis will be a certain kind of semi-supervised learning: *Reinforcement learning*. In Reinforcement Learning (**RL**), instead of labels for the data, there is a *weak teacher*, which provides feedback to the actions the agent took.

Markov Decision Processes

The metaphor behind RL is that of a decision maker (*agent*) and an *environment*. The agent makes observations in the environment (its input), takes actions (output) and receives rewards. In contrast to the classical ML approaches, in RL the agent is also responsible for exploration, as he has to acquire his knowledge actively. Thus, a reinforcement learning problem is given if the only way to collect information about the *underlying model* (the environment) is by interacting with it. As the environment does not explicitly provide actions the agent has to perform, its goal is to figure out the actions maximizing its cumulative reward until a training episode ends.

In the classical RL approach, the environment is divided into discrete time steps. If that is the case, the environment corresponds to a *Markov Decision Process* (**MDP**). Formally, a MDP is a 5-tuple $\langle S, A, P, R, \gamma \rangle$, consisting of the following:

S – set of states $s \in S$
A – set of actions $a \in A$
$P_a(s, s')$ – transition probability function from state s to state s' under action a
$R_a(s, s')$ – reward function for action a in state s if the environment moves to s'
γ – discount factor for future rewards $0 \leq \gamma \leq 1$

Though in general both the state transition function and the reward function may be indeterministic (and thus not in complete control of the decision maker), I will refer to the result of a state transition at discrete point in time t as $s_{t+1} := P(s_t, a_t)$ and to the result of the reward function as $r_t := R(s_t, a_t, s_{t+1})$. If no point in time is explicitly specified, it is assumed that all variables use the same t.

While an *offline learner* gets as input the problem definition in the form of a complete MDP, where the only task left is to classify actions yielding high rewards from actions giving suboptimal results, the task for an *online reinforcement learning* agent is a lot harder, as it has to learn the MDP itself via trial and error. In the process of reinforcement learning, the agent will encounter states s of the environment, performing actions a. The future state s_{t+1} of the environment may be indeterministic, but depends on the history of previous states $s_0, .., s_t$ as well as the action of the agent a_t. It is assumed that the *Markov property* holds, which means that a state s_{t+1} depends only on the current state s_t and currenct action a_t.

Throughout interacting with the environment, the agent receives rewards r, depending on his action a as well as the state of the environment s. In many RL problems, the full state of the environment is not known to the agent, and it only perceives an observation depending on the environment: $o_t := o(s_t)$[1]. This is referred to as *partial observability*, and the corresponding decision process is a *partially observable MDP*. Additionally, the agent knows when a final state of the environment is reached, terminating the current training episode. An episode consists for the agent thus of a sequence of observations, actions and rewards until at time t_t some terminal state s_{t_t} is reached:

$$Episode := \big((s_0, a_0, r_0), (s_1, a_1, r_1), (s_2, a_2, r_2), .., (s_{t_t}, a_{t_t}, r_{t_t})\big)$$

Value of a state

In the process of reinforcement learning, the agent tries to perform as well as possible in the previously unknown environment. For that, it uses an action-policy π, mapping states to actions: $\pi(s) = a$.[2] In general, this policy may also be stochastic. As the agent does not have supervised data for what actions are the ground truth, it must learn some kind of measure for the value of being in a certain state or performing a certain action. The commonly used measure for the value of a state can be calculated by the immediate reward this state gives, summed with the discounted future reward the agent will archieve by continuing to follow his policy from this

[1] From now on, when I mean the state of the environment, I will explicitly refer to it as s_e, while reserving s for the agent's obvervation of the enviroment $o(s_e)$

[2] It is obvious, that the result of both the reward function and the state transition function depend on π. To be explicit about that, I will refer to a reward dependent on π as r^π and a state transition dependent on π as s^π. If state or reward depends on an explicit action instead, I refer to it as r^a and s^a.

state on:

$$V^{\pi}(s_t) := \sum_{t'=t}^{t_t} (\gamma^{t'-t} * r_{t'}^{\pi}) \tag{2.1}$$

Using the discounted future reward is useful because in an indeterministic environment it gets less likely that the agent actually reaches this state, and to make the agents perform good actions as quickly as possible.

The actual, underlying Value of a state s is defined as the value of the state when using the best possible policy, which corresponds to the maximally archievable reward starting in state s:

$$V^{*}(s_t) := max_{\pi} V^{\pi}(s_t^{\pi}) \tag{2.2}$$

While *passive reinforcement learning* simply tries to learn the Value-function without the need of action selection, an *active reinforcement learner* tries to estimate a good policy, using which those high-value states are actually reached. If the value of every state is known, then the optimal policy can be defined as the one archieving maximal value for every upcoming state: $\pi^{*} := argmax_{\pi} V^{\pi}(s) \forall s \in S$. Knowing what an optimal policy does, and using 2.1 and 2.2, it is possible to re-write the definition of the value of a state recursively as

$$V^{*}(s_t) = max_{\pi} \Big(\sum_{t'=t}^{t_t} (\gamma^{t'-t} * r_{t'}^{\pi}) \Big) \tag{2.3}$$

$$= max_{\pi} (r_t^{\pi} + \gamma * V^{\pi}(s_{t+1}^{\pi})) \tag{2.4}$$

This is known as the *Bellman Equation*, which allowed for the birth of dynamic programming. It rewrites the value of the decision problem at time t in terms of the immediate reward at t plus the value of the remaining decision problem at $t+1$, resulting from the initial choices.[3]

Value of an action

While the definition of a state-value is useful, it alone does not help an agent to perform optimally, as neither the successor function $P_a(s, s')$, nor the reward function $R_a(s)$ are known to the agent. While so-called *model-based* reinforcement learning tries to learn both of those explicitly to reconstruct the entire MDP, *model-free* agents use a different measure of quality: the *Q-value*. It represents the value of performing action a_t in a state s_t, afterwards following the policy π.

$$Q^{\pi}(s_t, a_t) := r_t^{a_t} + \gamma * V^{\pi}(s_{t+1}^{a_t}) \tag{2.5}$$

With the optimal, maximally archivable action-value Q^{*} being respectively

$$Q^{*}(s_t, a_t) = r_t^{a_t} + \gamma * V^{*}(s_{t+1}^{a_t}) \tag{2.6}$$

$$= max_{\pi} (r_t^{a_t} + \gamma * V^{\pi}(s_{t+1})) \tag{2.7}$$

[3] This is because of the definition of Bellman's *Principle of Optimality*, which states that "An optimal policy has the property that whatever the initial state and initial decision are, the remaining decisions must constitute an optimal policy with regard to the state resulting from the first decision[**Bellman1957**]"

As the Value of a state is defined as the maximally archievable reward from that state, the relation between Q and V can be expressed as

$$V(s_t) = max_{a_t} Q(s_t, a_t) \tag{2.8}$$

When an agent knows the Q-value for each action of a state, it can easily infer the optimal action in state s_t as $a_t^* := argmax_{a_t}(Q(s_t, a_t))$ and thus the optimal policy π^*, guaranteeing maximum future reward at every state. The goal of a model-free RL agent is thus to get a maximally precise estimate of Q^*, yielding maximal reward for every state. For that, it does not need to explicitly learn the reward- and transition function, but instead can model only the Q-function. Its policy is then to simply always take the action yielding the highest value for every state (a *greedy* policy). In RL settings with a highly limited amount of discrete states and actions, the respective Q-function estimate can be specified as a lookup table, whereas for areas of interest, the function is calculated using a kind of nonlinear function approximator.

Throughout exploration of the environment, the agent collects more information of it, continually updating its estimate Q^π. For that, it uses samples from its episodes of interacting with the environment.

2.2 Temporal difference Learning

Throughout the process of reinforcement learning, the agent continually improves its estimates $\hat{Q}$ of Q^*. An optimal solution would be to calculate the Loss of the current Q-estimate as the squared difference $(\hat{Q}\text{-}Q^*)^2$, to perform gradient descent in order to minimize that difference. However, as Q^* is unknown to the agent, that is not possible. Instead, a Q-learning agent performs *iterative approximation*, using the information about the environment, to continually update its estimates of Q^*. Using the recursive definition of a state-value given in the Bellman equation 2.4 allows for a technique called *temporal difference learning*[**sutton1988**]: At time $t+1$, the agent can compare its estimate of the Q-function of the last step, $\hat{Q}^\pi(s_t, a_t)$, with a new estimate using the new information it gained from the environment: r_{t+1} and s_{t+1}. Because of the newly gained information from the underlying model, the new estimate will be closer to the actual function Q^* than the original value:

$$Q^*(s_t, a_t) = r_t^{a_t} + \gamma * V^*(s_{t+1}^{a_t}) \tag{2.9}$$

$$\approx r_t^{a_t} + \gamma * V^\pi(s_{t+1}^{a_t}) = r_t^{a_t} + \gamma * \hat{Q}^\pi(s_{t+1}^{a_t}, a_{t+1}) \tag{2.10}$$

SARSA

The new knowledge about the environment can be incorporated in two different ways. For the first method, the agent samples a full tuple of $\langle s_t, a_t, r_t, s_{t+1}, a_{t+1} \rangle$ from the environment, to then calculate the temporal difference error in non-terminal states as $TD := (r_t + \gamma * \hat{Q}_i^\pi(s_{t+1}, a_{t+1})) - \hat{Q}_i^\pi(s_t, a_t)$. This algorithm of calculating the temporal difference error is known as SARSA, and it is an example of *on-policy* learning. In on-policy learning, the agent uses his own policy in every estimate of the Q-value.

Q-learning

In contrast to SARSA stands the *off-policy* algorithm *Q-learning*. This algorithm does not need to sample the action a_{t+1}, as it calculates the Q-update at iteration i using

the best possible action in state s_{t+1}[4]. As the previous definition of Q-values was only correct in non-terminal states, a case differentiation must be introduced for terminals and non-terminal states. In the following, y_t will stand for the updated estimate of the Q-value at t, sampling the necessary states, rewards and actions from the environment, almost resulting in the formula found in [3]:

$$y_t = \begin{cases} r_t & \text{if } t = t_t \\ r_t + \gamma * max_{a_{t+1}}(\hat{Q}^{\pi}(s_{t+1}, a_{t+1})) & \text{otherwise} \end{cases} \tag{2.11}$$

The temporal difference error is accordingly defined as

$$TD_t := y_t - \hat{Q}^{\pi}(s_t, a_t) \tag{2.12}$$

A Q-learning agent must thus for his learning step observe a snapshot of the environment, consisting of the following input: $\langle s_t, a_t, r_t, s_{t+1}, t+1 == t_t \rangle$, where the letter is the information if state s_{t+1} was a terminal state. Using the above error straight away allows for the update-rule of an agent in a very limited setting: Consider an agent, specifying his approximation of the Q-function (his *model*) with a lookup-table, initialized to all zeros. It is proven that for finite-state Markovian problems with nonnegative rewards the update-rule for the Q-table $\hat{Q}(s_t, a_t) \leftarrow r_t^{a_t} + \gamma * \hat{Q}^{\pi}(s_{t+1}^{a_t}, a_{t+1})$ converges to the optimal Q^*-function, making the greedy policy π^* optimal[5]. It is noteworthy, that each new temporal difference will affect not only the last prediction, but all previous predictions.

As however in practice the problems using a table as the Q-functions are only very limited scenarios, an update rule like this is irrelevant. Instead, a better idea is to use this definition of the temporal difference error for a loss function, which is to be minimized throughout the process of RL. A commonly used loss-function is the *L2-Loss*, which allows gradient descent, updating the parameters of the Q-function into the direction of the newly acquired knowledge. The L2-Loss at iteration i with model-parameters θ_i is thus defined as the following:

$$L_i(\theta_i) := \left(y_i(\theta_i) - \hat{Q}_i^{\pi}(s_t, a_t; \theta_i)\right)^2 \tag{2.13}$$

2.3 Q-Learning with Neural Networks

To understand this section, basic knowledge on how *Artificial Neural Networks* (**ANN**s) work and what they do is presupposed. A special focus must also lie on *Convolutional Neural Networks* (**CNN**s) [5], mainly used in image processing. As mentioned before, it is not only possible to use a Q-table to estimate the Q^*-function, but any kind of function approximator. Thanks to the universality theorem[6], it is known that ANNs are an example of such. The defining feature of ANNs in comparison to other Machine Learning techniques is their ability to store complex, abstract representations of their input when using a *deep* enough architecture.

2.3.1 Deep Q-learning

The reason to use neural function approximators instead of a simple Q-table approach for reinforcement learning problems is easy to see: While for a Q-table the

[4] A slight deviation from this *double-Q-learning*, an algorithm I will go into detail about lateron.
[5] Of course the agent will need some kind of exploration technique first, more on that later
[6] http://neuralnetworksanddeeplearning.com/chap4.html, I need a better source on this!

states and actions of the Markov Decision Process must be discrete and very limited, this is not the case when using higher-level representations. If the agent's observation of a state of the game is high-dimensional (like for example an image) the chance for an agent to re-visit a state it learned about is extremely slight. Instead, an Artificial Neural Network can learn a higher-level representation of the state which group conceptually similar states, and thus generalize to new, previously unseen, states. It is no surprise that the success of *Deep-Q-Networks* started its journey shortly after the introduction of CNNs, which are able to learn abstract representations of similar images, by now used in countless Computer Vision Applications.

Deep-Q-Network refers to a family of off-policy, online, active, model-free Q-learning algorithms using Deep Neural Networks. When using ANNs as function approximators for the model of the environment, it will result in a Loss function depending on the Neural Network parameters, specified by θ. The update rule in Deep Networks depends on the gradient with respect to the weights of this formula, $\Delta_{\theta_i} L(\theta_i)$.While there are attempts to use Artificial Neural Networks for Q-learning as early as 1993[SOURCE], some key components of modern Deep-Q-Networks (**DQN**s) were missing, leading to satisfactory performance only in very limited settings. In standard online RL tasks, the update step minimizing the loss specified in 2.13 is performed right after the observation occured to the agent. As consecutive steps of MDPs tend to be correlated, the update using gradient descent is prone to oscillation in its result, thus never converging to an optimal Q^*-function. It was not until *Deepmind*'s famous papers in 2013[2] and 2015[3], that those issues were successfully adressed. The two important innovations introduced in their DQN-architecture were the use of a *target network* as well as the technique of *experience replay*, which in combination successfully hindered the problem of oscillating and non-converging action-value function, even though still no formal mathematical proof of that is given.

Experience Replay

As mentioned above, learning only from the most recent experiences biases the policy towards those situations, limiting convergence of the Q-function. To adress this issue, the DQN uses an experience replay memory: Every percept of the environment (the $\langle s_t, a_t, r_t, s_{t+1}, t+1 == t_t \rangle$ - tuple) is added to a limited-size memory of the agent. When then performing the learning step, the agent samples random minibatches from this memory to perform learning on a maximally uncorrelated sample of experiences. In the original definition of DQN, those minibatches are drawn uniformely at random, while as of today, better techniques for sampling those minibatches are available[4], increasing the performance of the resulting algorithm significantly.

Target Networks

During the training procedure, the DQN-algorithm uses a separate network to generate the target-Q-values, used to compute the loss (2.13), necessary for the learning step of every iteration. The idea behind that is, that the Q-values of the *online network* shift in such a way, that a feedback loop can arise between the target- and estimated Q-values, shifting the Q-value more and more into a similar direction. To lessen the risk of such feedback loops, the DQN algorithm introduced the use of a second

network for calculating the loss: the target network. This is only periodically updated with the weights of the online network used for the policy, which reduces the risk of correlations in the action-value Q_t and the corresponding target-value y_t (see equation 2.11).

The use of this two techniques leads to the Q-learning update rule as used in [3]:

$$L_i(\theta_i) = \mathbb{E}_{\langle s_t, a_t, r_t, s_{t+1}\rangle \sim U(D)} \left[\left(r + \gamma * max_{a_{t+1}} \hat{Q}(s_{t+1}, a_{t+1}; \theta_i^-) - \hat{Q}(s_t, a_t; \theta_i) \right)^2 \right] \tag{2.14}$$

Where i stands for the current network update iteration, θ_i for the current weights of the target network (updated every C iterations to be equal to the weights of the online network θ_i), $Q(\cdot, \cdot; \theta)$ for the Q-value dependend on a ANN using the weights θ, $\mathbb{E}[\cdot]$ for the expected value in an indeterministic environment, D for the contents of the replay memory of length $|D|$ containing $\langle s_t, a_t, r_t, s_{t+1}\rangle$-tuples, and $U(\cdot)$ for a uniform distribution.

As is the case with the experience replay mechanism, the usage of a target network was improved as well by now - modern algorithms don't perform a hard update of the target network every C steps, but instead perform *soft target network update*, where every iteration, the weights of the target network are defined as $\theta_i^- := \theta_i * \tau + \theta_i^- * (1 - \tau)$ with $0 < \tau \ll 1$, first introduced in [DDPG-Paper]. This improves the stability of the algorithm even more.

Double-Q-Learning

In DoubleQ, we still use the greedy policy to select actions, however we evaluate how good it is with another set of weights

Dueling Q-Learning

Using Recurrent Networks

2.3.2 Deterministic Policy Gradient

2.3.3 Exploration techniques

Chapter 3

Related work

3.1 Reinforcement Learning Frameworks

Gym/Universe Torcs

3.2 Self-driving cars

Nvidias deep-drive RRT* Tensorkart Tesla Lidar hier in den fußnoten die ganzen non-scientific quellen wie tensorkart undso

Chapter 4

Program Architecture

The program was written by the author of this work and is licensed under the GNU General Public License (GNU GPLv3). Its source code is attached in the appendix of this work and additionally can be found digitally on the enclosed CD-ROM. The machine learning part was written in PYTHON, using the TENSORFLOW-library [1].

4.1 Design choices

4.1.1 The game as a reinforcement learning problem

-ungefähres UML-diagramm

4.1.2 The vectors

4.1.3 Exploration

4.1.4 Reward

4.1.5 Performance measure

4.2 Implementation

4.2.1 The game

What Leon did already

Communication

-den sockets post -das von leon gemalte ablaufdiagramm

4.2.2 The agent

Unbedingt auf jeden Fall UML-diagramm

Challenges and Solutions

DQN vs DDPG, sehend vs nicht-sehend, ...

Pretraining

The different agents

sehend vs nicht sehend, ...

Network architecture

1. dqn-algorithm - anzahl layer, Batchnorm, doubles dueling - MIT GRAFIK 2. ddpg - anzahl layer, Batchnorm - MIT GRAFIK

Chapter 5

Analysis, Results and open Questions

testing took place on a win10 machine, ... Answer all of the research questions explicitly!!!

Chapter 6

Discussion

"Fragestellung aus der Einleitung wird erneut aufgegriffen und die Arbeitsschritte werden resümiert" Zusammen mit der Conclusion 10% der Gesamtlänge

Chapter 7

Conclusion and future directions

Bibliography

[1] Martin Abadi, Ashish Agarwal, Paul Barham, Eugene Brevdo, Zhifeng Chen, et al. *TensorFlow: Large-scale machine learning on heterogeneous systems*. Software available from tensorflow.org. 2015. URL: http://tensorflow.org/.

[2] Volodymyr Mnih, Koray Kavukcuoglu, David Silver, Alex Graves, Ioannis Antonoglou, Daan Wierstra, and Martin Riedmiller. "Playing atari with deep reinforcement learning". In: *arXiv preprint arXiv:1312.5602* (2013). URL: https://arxiv.org/abs/1312.5602 (visited on 08/12/2017).

[3] Volodymyr Mnih, Koray Kavukcuoglu, David Silver, Andrei A. Rusu, Joel Veness, et al. "Human-level control through deep reinforcement learning". en. In: *Nature* 518.7540 (Feb. 2015), pp. 529–533. ISSN: 0028-0836. DOI: 10.1038/nature14236. URL: http://www.nature.com/nature/journal/v518/n7540/full/nature14236.html?foxtrotcallback=true.

[4] Tom Schaul, John Quan, Ioannis Antonoglou, and David Silver. "Prioritized Experience Replay". In: *arXiv:1511.05952 [cs]* (Nov. 2015). arXiv: 1511.05952. URL: http://arxiv.org/abs/1511.05952 (visited on 08/12/2017).

[5] Yann LeCun, Léon Bottou, Yoshua Bengio, and Patrick Haffner. "Gradient-based learning applied to document recognition". In: *Proceedings of the IEEE* 86.11 (1998), pp. 2278–2324. URL: http://yann.lecun.com/exdb/publis/pdf/lecun-01a.pdf (visited on 08/12/2017).

Declaration of Authorship

I, Christoph Stenkamp, hereby certify that the work presented here is, to the best of my knowledge and belief, original and the result of my own investigations, except as acknowledged, and has not been submitted, either in part or whole, for a degree at this or any other university.

_____

signature

_____

city, date