



POLITECNICO DI TORINO

Department of Control and Computer Engineering

Master of Science in Computer Engineering

Master Thesis

Deep Reinforcement Learning for Autonomous Systems

Designing a control system to exploit model-free deep reinforcement learning algorithms to solve a real-world autonomous driving task of a small robot.

Supervisors

Prof. Pietro MICHIARDI

Prof. Elena BARALIS

Candidate

Piero MACALUSO

s252894

ACADEMIC YEAR 2019-2020

This work is subject to the Creative Commons Licence

Abstract

Because of its potential to drastically change mobility and transport, autonomous systems and self-driving vehicles are attracting much attention from both the research community and industry. Recent work has demonstrated that it is possible to rely on a comprehensive understanding of the immediate environment while following simple high-level directions, to obtain a more scalable approach that can make autonomous driving a ubiquitous technology. However, to date, the majority of the methods concentrates on deterministic control optimisation algorithms to select the right action, while the usage of deep learning and machine learning is entirely dedicated to object detection and recognition.

Recently, we have witnessed a remarkable increase in interest in Reinforcement Learning (RL). It is a machine learning field focused on solving Markov Decision Processes (MDP), where an agent learns to make decisions by mapping situations and actions according to the information it gathers from the surrounding environment and from the reward it receives, trying to maximise it. As researchers discovered, reinforcement learning can be surprisingly useful to solve tasks in simulated environments like games and computer games, and RL showed encouraging performance in tasks with robotic manipulators. Furthermore, the great fervour produced by the widespread exploitation of deep learning opened the doors to function approximation with convolutional neural networks, developing what is nowadays known as deep reinforcement learning.

In this thesis, we argue that the generality of reinforcement learning makes it a useful framework where to apply autonomous driving to inject artificial intelligence not only in the detection component but also in the decision-making one. The focus of the majority of reinforcement learning projects is on a simulated environment. However, a more challenging approach of reinforcement learning consists of the application of this type of algorithms in the real world. For this reason, we designed and implemented a control system for Cozmo, a small toy robot developed by Anki company, by exploiting the Cozmo SDK, PyTorch and OpenAI Gym to build up a standardised environment in which to apply any reinforcement learning algorithm: it represents the first contribution of our thesis.

Furthermore, we designed a circuit where we were able to carry out experiments in the real world, the second contribution of our work. We started from a simplified environment where to test algorithm functionalities to motivate and discuss our implementation choices. Therefore, we implemented our version of Soft Actor-Critic (SAC), a model-free reinforcement learning algorithm suitable for real-world experiments, to solve the specific self-driving task with Cozmo. The agent managed to reach a maximum value of above 3.5 meters in the testing phase, which equals more than one complete tour of the track. Despite this significant result, it was not

able to learn how to drive securely and stably. Thus, we focused on the analysis of the strengths and weaknesses of this approach outlining what could be the next steps to make this cutting-edge technology concrete and efficient.

Acknowledgements

I would first like to thank my external thesis supervisor Prof. Pietro Michiardi for his guidance and support: he allowed me to autonomously work on a challenging and engaging project on an innovative research field, steering me in the right the direction whenever he thought I needed it. Furthermore, I would like to thank my internal supervisor Prof. Elena Baralis for her support.

A profound thank goes to my mother Francesca, my father Salvatore and my whole family: they have always supported me in every choice and interest by teaching me the meaning of sacrifice, commitment and constancy. I reserve a heartfelt thank to my brother Antonio for his steady presence and support, but also our mutual inspiration and constructive confrontation.

I would like to profoundly thank my Luisa for all her love, support and encouragement, despite our being so far away: she followed me in every choice by motivating and encouraging me in the face of every difficulty encountered during these years.

A special thank goes to every people I met during my stay on the second floor of "Collegio Einaudi" in Turin, where I have lived since 2014. Every person I met in my study path is essential, but I would like to particularly thank Giordano, Pierluigi, Stella, Alessio and Elvira for their support during my thesis work.

Finally, I would like to thank for their constant support my lifelong friends Federico, Davide, Christian, Michele, Jacopo and Pietro.

Piero Macaluso, Torino, March 2020

Contents

Contents	II
List of Tables	V
List of Figures	VI
List of Algorithms	VIII
1 Introduction	1
1.1 Structure of the thesis	3
1.2 Github repository	4
2 Reinforcement Learning	5
2.1 Fundamentals of reinforcement learning	5
2.1.1 The reinforcement learning problem	6
2.1.2 Bellman equations	9
2.1.3 Approaches to reinforcement learning	10
2.1.4 Dynamic programming	12
2.1.5 Model-free approach	14
2.1.6 Model-based approach	17
2.2 Deep reinforcement learning	18
2.2.1 Fundamentals of deep learning	19
2.2.2 Value-based methods	26
2.2.3 Policy gradient methods	28
2.2.4 Deep Deterministic Policy Gradient (DDPG)	30
2.2.5 Soft Actor-Critic (SAC)	34
2.3 Related work	38
3 Tools and Frameworks	42
3.1 OpenAI Gym	42
3.1.1 Environments	43
3.1.2 Observations	45
3.2 Anki Cozmo	46

3.2.1	Cozmo architecture	47
3.2.2	Why Cozmo?	51
3.3	PyTorch	54
3.3.1	TensorboardX	55
3.3.2	Comparison with TensorFlow	56
4	Design of the control system	59
4.1	Outline of the system	60
4.1.1	OpenAI Gym Cozmo environment	60
4.1.2	Human-Robot interaction	65
4.1.3	System flow	67
4.2	Algorithm setup	70
4.2.1	Neural networks design	71
4.2.2	Algorithms implementations and hyperparameters	73
4.3	Real-World experiments	75
4.3.1	Actions duration	75
4.3.2	Driving bias	76
4.3.3	Error management	76
4.3.4	Track design	77
5	Experimental results	80
5.1	Experimental methodology	81
5.1.1	Hardware and software details	81
5.1.2	Pendulum-v0 environment	82
5.1.3	CozmoDriver-v0 environment	84
5.1.4	Measuring performance	87
5.2	Pendulum-v0 experiments	88
5.2.1	DDPG hyperparameters	88
5.2.2	SAC hyperparameters	89
5.2.3	Comparative analysis	90
5.3	CozmoDriver-v0 experiments	96
5.3.1	The DDPG approach	96
5.3.2	The SAC approach	97
5.3.3	SAC hyperparameters	98
5.3.4	Results analysis	98
6	Conclusions	104
6.1	Future work	105
A	Reinforcement Learning	107
A.1	Bellman equation	107
A.2	Dynamic programming	108

List of Tables

5.1	Development Machine Hardware Specifications	81
5.2	Development Machine Software Specifications	82
5.3	Original Observation Pendulum-v0 environment	82
5.4	Pendulum-v0 Actions	83
5.5	CozmoDriver-v0 Actions	85
5.6	DDPG Hyper-parameter setup for Pendulum-v0 environment	89
5.7	SAC Hyper-parameter setup for Pendulum-v0 environment	90
5.8	SAC Hyper-parameter setup for CozmoDriver-v0 environment	98

List of Figures

2.1	Interaction loop between Agent and Environment	8
2.2	Overview of different components in reinforcement learning	12
2.3	Generalised Policy Iteration (GPI) schema	14
2.4	Comparison between Biological and Artificial Neuron	19
2.5	Fully-connected layer representation	20
2.6	LeNet Architecture Representation	24
2.7	Max-Pooling layer example	25
2.8	Dueling DQN	28
2.9	Actor-Critic architecture schema	30
2.10	Future transition in AI Applications	40
3.1	Anki Cozmo Robot	46
3.2	Interaction Robot / Mobile Application	48
3.3	Interaction Mobile Application / Computer	50
4.1	Outline of the control system	61
4.2	Web Application implemented to Control Cozmo	66
4.3	Cozmo algorithm flow chart	68
4.4	Convolutional Neural Network Architecture for Cozmo experiments	74
4.5	CozmoDriver Racing Track	78
5.1	Frame of Pendulum-v0 environment	83
5.2	Example of two subsequent frames of CozmoDriver-v0	85
5.3	DDPG Pendulum-v0 Reward Plot	92
5.4	SAC Pendulum-v0 Reward Plot	92
5.5	DDPG Pendulum-v0 Test Average Reward Plot	93
5.6	SAC Pendulum-v0 Test Average Reward Plot	93
5.7	DDPG Pendulum-v0 Last 100 Episode Average Reward Plot	94
5.8	SAC Pendulum-v0 Last 100 Episode Average Reward Plot	94
5.9	DDPG Pendulum-v0 Noise Epsilon Decay	95
5.10	SAC Pendulum-v0 auto-tuning temperature	95
5.11	SAC CozmoDriver-v0 auto-tuned temperature	101
5.12	SAC CozmoDriver-v0 Reward Plot	102
5.13	SAC CozmoDriver-v0 Last 100 Episode Average Reward Plot	102
5.14	SAC CozmoDriver-v0 Test Reward Plot	103

5.15 SAC CozmoDriver-v0 Test Average Reward Plot	103
--	-----

List of Algorithms

2.1	SARSA (on-policy TD control) for estimating $Q \approx q_*$	16
2.2	Q-learning (off-policy TD control) for estimating $\pi \approx \pi_*$	16
2.3	Batch normalisation	23
2.4	DDPG Algorithm [41]	33
2.5	Soft Actor-Critic [21]	37
4.1	CozmoDriver actions conversion from virtual to real	63
A.1	Policy Iteration for estimating $\pi \sim \pi^*$	108
A.2	Value Iteration, for estimating $\pi \sim \pi^*$	109

Chapter 1

Introduction

Autonomous systems and in particular self-driving for unsupervised robots and vehicles (e.g. self-driving cars) are becoming more and more an integral part of human lives. This topic attracted much attention from both the research community and industry, due to its potential to radically change mobility and transport. In general, most approaches to date focus on formal logic methods, which define driving behaviour in annotated geometric maps. These methods can be challenging to scale, as they rely heavily on an external mapping infrastructure rather than using and understanding the local scene, leaving fully autonomous driving in a real urban environment an essential but elusive goal.

However, recent work on autonomous driving has demonstrated that it is possible to exploit the knowledge about the surrounding environment to obtain a more scalable method for self-driving vehicles. The work in [49] demonstrated that this approach is feasible on rural country roads, using GPS for coarse localisation and LIDAR to understand the local scene. The ability to drive and navigate in the absence of maps and explicit rules, relying – just like humans do – on a comprehensive understanding of the immediate environment while following simple high-level directions (e.g. turn-by-turn route commands) may be the correct approach to revolutionise autonomous driving by making it a genuinely ubiquitous technology.

To date, the majority of the methods adopted to exploit the local scene and to learn how to drive concentrates on deterministic algorithms to recognise the surroundings and select the right action (e.g. lane following problem on well-marked structured highways). However, these methods, like the previous ones, are not able to generalise proficiently in a different environment because of their deterministic nature.

In this context, the usage of deep learning and machine learning is entirely dedicated to object detection and recognition, while the decision-making aspect is left to control optimisation algorithms [26].

Recently, we have witnessed a remarkable increase in interest in Reinforcement

Learning (RL). Reinforcement Learning is a machine learning field focused on solving Markov Decision Processes (MDP), where an agent learns to act in an environment by mapping situations and actions, trying to maximise some reward function. To date, it represents the closest example of a learning approach that mimics the ability of humans to learn from experiences. The agent, the brain of reinforcement learning, learns to make decisions according to the information it receives from the surrounding environment and from the positive (or negative) reward it receives. It represents a crucial step towards Artificial General Intelligence (AGI). This machine learning paradigm achieved super-human results at games such as Go [61] or chess [62]. Therefore, researchers found out that it can be surprisingly useful to solve tasks in simulated environments like computer games [44], and it possesses promising features to perform tasks with robotic manipulators [18]. Furthermore, the great fervour produced by the widespread exploitation of deep learning opened the doors to function approximation with neural networks and convolutional neural networks, developing what is nowadays known as Deep Reinforcement Learning.

In this thesis, we argue that the generality of reinforcement learning makes it a useful framework where to apply autonomous driving to inject artificial intelligence not only in the detection component but also in the decision-making one. The majority of the work in this research field are focused on simulated environments where experiments with a large number of iterations can be straightforwardly completed without direct human interaction. However, to date, the more challenging approach of reinforcement learning consists of the application of this type of algorithms in the real world [28]. In this context, the crucial challenges are the one related to hyper-parameters configurations that requires numerous and expensive iterations in order to obtain valuable results, but also the data noisiness and exploration. Despite these obstacles, the results that could derive from the application of these technologies to a real context could be compelling and revolutionary. For this reason, we accepted this challenge, and we decided to apply reinforcement learning algorithms to an autonomous driving problem, following the inspiring research of [29].

To develop our considerations about the particular application of this research field, we designed and implemented a control system to control Cozmo, a small toy robot developed by Anki company, by exploiting the Cozmo SDK and OpenAI Gym to build up a standardised environment in which to apply any reinforcement learning algorithm. This implementation represents the first contribution of our thesis. In the second contribution of our work, we aimed to implement state-of-the-art model-free deep reinforcement learning algorithms and discuss the result obtained. We opted for Soft Actor-Critic (SAC) [21, 20], a model-free reinforcement learning algorithm suitable for real-world experiments whose authors managed to overcome hyper-parameters configuration dependency of Deep Deterministic Policy Gradient (DDPG) [41], focusing on what could be next steps to make this cutting-edge technology concrete and efficient.

1.1 Structure of the thesis

This section aims to describe the main structure of the thesis.

Chapter 1 - Introduction

The current chapter contains the motivation underlying this work and the structure of the thesis.

Chapter 2 - Reinforcement Learning

This chapter aims to offer a description as detailed as possible about reinforcement learning state-of-the-art in order to provide the reader with useful tools to enter in this research field. The chapter consists of three principal parts. The first one aims to describe traditional reinforcement learning fundamentals. In contrast, the second one focuses reader's attention to the *deep* approach to reinforcement learning, providing an outline of deep learning and presenting Deep Deterministic Policy Gradient (DDPG) and Soft Actor-Critic (SAC) algorithms.

The last part of this chapter contains a related work review to introduce to the reader the problem we aimed to solve.

Chapter 3 - Tools and Frameworks

This chapter explains which are the primary tools, frameworks and languages that we used in this thesis. There will be a particular focus on *OpenAI Gym*, one of the most popular reinforcement learning framework nowadays, *Anki Cozmo*, the robot we used to carry out reinforcement learning experiments, and *PyTorch*, the deep learning framework we used to use convolutional neural networks in reinforcement learning.

Furthermore, we outlined the motivations behind the choices made through the analysis of the alternatives present at the time of the thesis development.

Chapter 4 - Design of the control system

The first contribution of our thesis was the implementation of a control system to perform reinforcement learning experiments in the real world, binding all the technologies presented in the previous chapter and focusing on reusability of this system to exploit other reinforcement learning algorithms.

The fourth chapter aims to present the whole set of features we implemented together with an analysis of the solutions we proposed to the problems we faced.

Chapter 5 - Experimental results

The second contribution of our thesis consists of the experiments we carried out with Soft Actor-Critic (SAC) algorithm to solve an autonomous driving task in the real world with Anki Cozmo robot. This chapter aims to present the results we obtained starting from the preliminary experiments on a modified environment to tests features and functionalities and concluding the chapter with the discussion about the learning process of the robot.

It also contains some considerations about the approach taken and a general discussion on how to measure performances in reinforcement learning algorithms.

Chapter 6 - Conclusions

This chapter provides a summary of the results obtained from experiments together with a specific critic part. Furthermore, the thesis will conclude with a specific part dedicated to possible future improvements to this work.

1.2 Github repository

The ideas and the source code of the work contained in this thesis is publicly available on Github at <https://github.com/pieromacaluso/Deep-RL-Autonomous-Systems>. The primary motivation behind this choice is allowing people to use, test, contribute and improve it even after the conclusion of this thesis work.

Chapter 2

Reinforcement Learning

Reinforcement learning (RL) is a field of machine learning that is experiencing a period of great fervour in the world of research, fomented by recent progress in deep learning (DL) which opened the doors to function approximation developing what is nowadays known as deep reinforcement learning. RL represents the third paradigm of machine learning alongside supervised and unsupervised learning. The idea underlying this research field is that the learning process to solve a decision-making problem consists in a sequence of trial and error where the *agent*, the protagonist of RL, could discover and discriminate valuable decisions from penalising ones exploiting information given by a *reward signal*. This interaction has a strong correlation with what human beings and animals do in the real world to forge their behaviour.

Before discussing the results of this thesis, it is good to delineate what today represents the state-of-the-art to understand the universe behind this paradigm better. Indeed, the exploration of this field of research is the main aim of this chapter. The first section begins with the definition of the notation used and with the theoretical foundations behind traditional RL. In the second section, it moves progressively towards what is deep RL through an introduction to the fundamentals of deep learning and a careful discussion of the essential algorithms paying more attention to those used during the thesis project. The last section aims to illustrate the starting point and ideas of the thesis, drawing what the scenario of deep RL applied to autonomous systems and real-world robotic tasks is today.

The elaboration of this chapter is inspired by [60], [66], [48], [37] and [15].

2.1 Fundamentals of reinforcement learning

Reinforcement learning is a computational approach to sequential decision making. It provides a framework that is exploitable with decision-making problems that are unsolvable with a single action and need a sequence of actions, a broader horizon, to

be solved. This section aims to present the fundamental ideas and notions behind this research field in order to help the reader to develop a baseline useful to approach section 2.2 on page 18 about deep reinforcement learning.

2.1.1 The reinforcement learning problem

Agent, environment and reward

The primary purpose of RL algorithms is to learn how to improve and maximise a future reward by relying on interactions between two main components: the *agent* and the *environment*.

The *agent* is the entity that interacts with the environment by making decisions based on what it can observe from the state of the surrounding situation. The decisions taken by the agent consist of *actions* (a_t). The agent has no control over the environment, but actions are the only means by which it can modify and influence the environment. Usually, the agent has a set of actions it can take, which is called *action space*. Some environments have *discrete* action spaces, where only a finite number of moves are available (e.g. $\mathcal{A} = [\text{North, South, East, West}]$ choosing the direction to take in a bidimensional maze). On the other side, there are *continuous* action spaces where actions are vectors of real values. This distinction is fundamental to choose the right algorithm to use because not all of them could be compatible with both types: according to the needs of the specific case, it may be necessary to modify the algorithm to make it compatible. The sequence of states and actions is named *trajectory* (τ): it is helpful to represent an episode in the RL framework.

The *environment* (E) represents all the things that are outside the agent. Whenever the agent takes an action, it emits a *reward* and an *observation* of the environment.

The *reward* r_t is a scalar feedback signal that defines the objective of the RL problem. This signal allows the agent to be able to distinguish positive actions from negative ones in order to reinforce and improve its behaviour. It is crucial to notice that the reward is local: it describes only the value of the latest action. Furthermore, actions may have long term consequences, delaying the reward. As it happens with human beings' decisions, receiving a conspicuous reward at a specific time step does not exclude the possibility to receive a small reward immediately afterwards and sometimes it may be better to sacrifice immediate reward to gain greater rewards later.

In this context, many features make reinforcement learning different from supervised and unsupervised learning. Firstly, there is no supervisor: when the agent has to decide what action to take, there is no entity that can determine what the optimal decision is in that specific moment. It does not learn from a set of labelled objects taken from a knowledge base as in supervised learning, but it exploits its

direct experience composed by observations and rewards as feedback. On the other hand, the presence of a mapping between input and output is the main difference from unsupervised learning, where the objective is to find underlying patterns rather than mappings.

The agent receives only a reward signal which may delay compared to the moment in which it has to perform the next action. This fact brings out another significant difference: the importance of time. The sequentiality links all actions taken by the agent, making resulting data no more independent and identically distributed (i.i.d).

The concept of return

Given these definitions, it is noticeable that the primary purpose of the agent is to maximise the cumulative reward called *return*.

The *return* g_t is the total discounted reward starting from timestep t defined by eq. (2.1) where γ is a *discount factor*.

$$g_t = r_{t+1} + \gamma r_{t+2} + \dots = \sum_{k=0}^{\infty} \gamma^k r_{t+k+1}, \quad \gamma \in [0,1) \quad (2.1)$$

Not only the fact that animal and human behaviour show a preference for immediate rewards rather than for the future ones motivates the presence of this factor, but it is also mathematically necessary: an infinite-horizon sum of rewards may not converge to a finite value. Indeed, the return function is a geometric series, so, if $\gamma \in [0,1)$, the series converges to a finite value equal to $1/(1 - \gamma)$. For the same convergence sake, the case with $\gamma = 1$ makes sense only with a finite-horizon cumulative discounted reward.

States and observations

The other data emitted by the environment is the *observation* (o_t) that is related to the *state* (s_t). It represents a summary of information that the agent uses to select the next action, while the *state* is a function of the *history*, the sequence of observation, actions and rewards at timestep t as shown in eq. (2.2).

$$h_t = o_1, r_1, a_1, \dots, a_{t-1}, o_t, r_t, \quad s_t = f(h_t) \quad (2.2)$$

The state described above is also called *agent state* s_t^a , while the private state of the environment is called *environment state* s_t^e . This distinction is useful for distinguishing fully observable environments where $o_t = s_t^e = s_t^a$, from partially observable environments where $s_t^e \neq s_t^a$. In the first case, the agent can observe the environment state directly, while in the second one, it has access to partial information about the state of the environment. Beyond the fact that this chapter

will focus on fully observable environments, the distinction between state and observation is often unclear and, conventionally, the input of the agent is composed by the reward and the state as shown in fig. 2.1.

Furthermore, a state is called *informational state* (or *Markov state*) when it contains all data and information about its history. Formally, a state is a Markov state if and only if satisfies eq. (2.3).

$$\mathbb{P}[s_{t+1}|s_t] = \mathbb{P}[s_{t+1}|s_1, \dots, s_t] \quad (2.3)$$

It means that the state contains all data and information the agent needs to know to make decisions: the whole history is not useful anymore because it is inside the state. The environment state s_t^e is a Markov state.

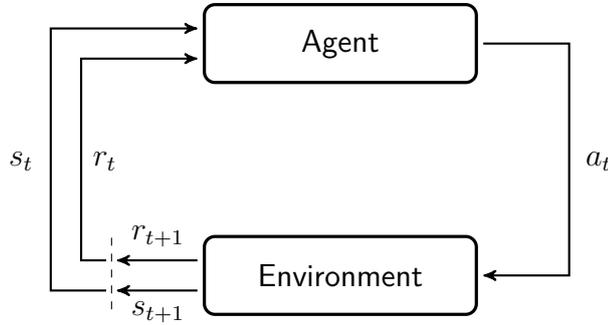


Figure 2.1. Interaction loop between Agent and Environment. The reward and the state resulting from taking an action become the input of the next iteration. [66]

The Markov decision problem

With all the definitions shown so far, it is possible to formalise the type of problems on which RL can unleash all its features: the Markov decision process (MDP), a mathematic framework to model decision processes. Its main application fields are optimisation and dynamic programming.

A MDP is defined by:

$$\langle \mathcal{S}, \mathcal{A}, \mathcal{P}, \mathcal{R}, \gamma \rangle$$

where \mathcal{S} is a finite set of states

\mathcal{A} a finite set of actions

\mathcal{P} a state transition probability matrix $\mathcal{P}_{ss'}^a = \mathbb{P}[s_{t+1} = s' | s_t = s, a_t = a]$

\mathcal{R} a reward function $\mathcal{R}_s^a = \mathbb{E}[r_{t+1} | s_t = s, a_t = a]$

γ a discount factor such that $\gamma \in [0,1]$

$$(2.4)$$

The main goal of an MDP is to select the best action to take, given a state, in order to collect the best reward achievable.

Policies, models and value functions

The components that may compose the agent, the brain of the reinforcement learning problem, can not be missing: they are the *model*, the *policy* and the *value function*.

A *model* consist of information about the environment. These data must not be confused with the ones provided by states and observations: they make it possible to infer prior knowledge about the environment, influencing the behaviour of the agent.

A *policy* is the representation of the agent's behaviour. It is a function that describes the mapping from states to actions. The policy is represented by π and it may be deterministic $a_t = \pi(s_t)$ or stochastic $\pi(a_t|s_t) = \mathbb{P}[a_t|s_t]$. In this perspective, it is evident that the central goal of RL is to learn an optimal policy π^* . The optimal policy is a policy which can show to the agent what the most profitable way to achieve the maximum return is, what is the best action to do in a specific situation. In order to learn the nature of the optimal policy, RL exploits value functions.

A *value function* represents what is the expected reward that the agent can presume to collect in the future, starting from the current state. The reward signal represents only a local value of the reward, while the value function provides a broader view of future rewards: it is a sort of prediction of rewards. It is possible to delineate two main value functions: the *state value* function and the *action value* function.

- The *State Value Function* $V^\pi(s)$ is the expected return starting from the state s and always acting according to policy π .

$$V^\pi(s) = \mathbb{E}_{\tau \sim \pi}[g_t | s_0 = s] \quad (2.5)$$

- The *Action Value Function* $Q^\pi(s)$ is the expected return starting from the state s , taking an action a and then always acting according to policy π .

$$Q^\pi(s, a) = \mathbb{E}_{\tau \sim \pi}[g_t | s_0 = s, a_0 = a] \quad (2.6)$$

2.1.2 Bellman equations

Both eqs. (2.5) and (2.6) satisfy recursive relationships between the value of a state and the values of its successor states. It is possible to see this property deriving *Bellman equations* [4] – shown in eq. (2.7) on the following page and demonstrated in appendix A.1 on page 107 – where $s_{t+1} \sim E$ means that the next state is sampled

from the environment E and $a_{t+1} \sim \pi$ shows that the policy π determines the next action.

$$\begin{aligned}
 V^\pi(s_t) &= \mathbb{E}_{a_t \sim \pi, s_{t+1} \sim E}[r(s_t, a_t) + \gamma V^\pi(s_{t+1})] \\
 &= \sum_{a \in \mathcal{A}} \pi(a|s) \sum_{s' \in \mathcal{S}, r \in \mathcal{R}} P(s', r|s, a) [r + \gamma V^\pi(s')] \\
 Q^\pi(s_t, a_t) &= \mathbb{E}_{s_{t+1} \sim E}[r(s_t, a_t) + \gamma \mathbb{E}_{a_{t+1} \sim \pi}[Q^\pi(s_{t+1}, a_{t+1})]] \\
 &= \sum_{a \in \mathcal{A}} \pi(a|s) \sum_{s' \in \mathcal{S}, r \in \mathcal{R}} P(s', r|s, a) [r + \gamma Q^\pi(s', a')]
 \end{aligned} \tag{2.7}$$

$r(s_t, a_t)$ is a placeholder function to represent the reward given the starting state and the action taken. As discussed above, the goal is to find the optimal policy π^* to exploit. It can be done using *Bellman optimality equations* defined in eq. (2.8).

$$\begin{aligned}
 V^*(s_t) &= \max_a \mathbb{E}_{s_{t+1} \sim E}[r(s_t, a) + \gamma V^*(s_{t+1})] \\
 &= \max_a \sum_{s' \in \mathcal{S}, r \in \mathcal{R}} P(s', r|s, a) [r + \gamma V^*(s')] \\
 Q^*(s_t, a_t) &= \mathbb{E}_{s_{t+1} \sim E}[r(s_t, a_t) + \gamma \max_{a'} [Q^*(s_{t+1}, a')]] \\
 &= \sum_{s' \in \mathcal{S}, r \in \mathcal{R}} P(s', r|s, a) [r + \gamma \max_{a'} Q^*(s', a')]
 \end{aligned} \tag{2.8}$$

Therefore, value functions allow defining a partial ordering over policies such that $\pi \geq \pi'$ if $V_\pi \geq V_{\pi'}, \forall s \in \mathcal{S}$. This definition is helpful to enounce the *sanity theorem*. It asserts that for any MDP there exists an optimal policy π^* that is better than or equal to all other policies, $\pi^* \geq \pi, \forall \pi$, but also that all optimal policies achieve the optimal state value function and the optimal action-value function.

The solution of the Bellman optimality equation is not linear and, in general, there is no closed-form solution. For this reason, there are many iterative methods: sections 2.1.4 and 2.1.5 on page 12 and on page 14 contain some of them.

2.1.3 Approaches to reinforcement learning

Every agent consists of an RL algorithm that it exploits to maximise the reward it receives from the environment. Every single algorithm has its singularity, and it could work with a specific application field which depends on the particular approach it supports. Understanding differences among these groups is useful to adequately understand what type of algorithm satisfies better the needs of a specific problem. Nowadays, RL algorithms are numerous, and drawing the complete picture behind them could be a complicated purpose. The distinctions presented in this section aims to describe the most crucial distinctions that are useful in the context of the thesis without claiming to be exhaustive.

Components of learning

The first worthy distinction between RL algorithms can be made analysing how the algorithms exploit the different components of the agent: indeed it is possible to explain the main strategies in RL using *policy*, *model* and *value function* defined in section 2.1.1 on page 9.

One of the most crucial aspects of an RL algorithm is the question of whether the agent has access to or learns the model of the environment: this element enables the agent to predict state transitions and rewards. A method is *model-free* when it does not exploit the model of the environment to solve the problem. All the actions made by the agent results from direct observation of the current situation in which the agent is. It takes the observation, does computations on them and then select the best action to take. This last representation is in contrast with *model-based* methods. In this case, the agent tries to build a model of the surrounding environment in order to infer information useful to predict what the next observation or reward would be. Both groups of methods have strong and weak sides. Ordinarily, *model-based* methods show their potential in a deterministic environment (e.g. board game with rules). In these contexts, the presence of the model enables the agent to plan by reasoning ahead, to recognise what would be the result of a specific decision before acting. The agent can extract all this knowledge and learn an optimal policy to follow. However, this opportunity is not always achievable: the model may be partially or entirely unavailable, and the agent would have to learn the model from its experience. Learning a model is radically complex and may lead to various hurdles to overcome: for instance, the agent can exploit the bias present in the model, producing an agent which is not able to generalise in real environments. On the other hand, model-free methods tend to be more straightforward to train and tune because it is usually hard to build models of a heterogeneous environment. Furthermore, model-free methods are more popular and have been more extensively developed and tested than model-based methods.

The use of policy or value function as the central part of the method represents another essential distinction between RL algorithms. The approximation of the policy of the agent is the base of *policy-based* methods. The representation of the policy is usually a probability distribution over available actions. This method points to optimise the behaviour of the agent directly and may ask manifold observations from the environment: this fact makes this method not so sample-efficient. On the opposite side, methods could be *value-based*. In this case, the agent is still involved in finding the optimal behaviour to follow, but indirectly. It is not interested anymore about the probability distribution of actions. Its main objective is to determine the value of all actions available, choosing the best one. The main difference from the policy-based method is that this method can benefit from other sources, such as old policy data or replay buffer.

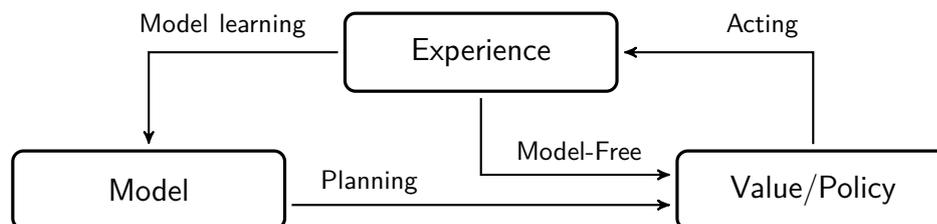


Figure 2.2. Overview of components of an agent with their relation in respect of different approaches of learning. Model-Free methods work with the experience, value functions and the policy, while model-based techniques try to build up a model to derive value functions and policy in order to act in the environment.

Learning settings

The learning setting could be *online* or *offline*. In the first case, the learning process is done in parallel or concurrently while the agent continues to gather new information to use, while the second one progresses toward learning using limited data. Generalisation becomes a critical problem in the latter approach because the agent is not able to interact anymore with the environment. In the context of this thesis, what matters is *online learning*: the learning phase is not bound to already gathered data, but the whole process goes on using both old data coming from replay buffers and brand new data obtained in the most recent episode.

Another significant difference in RL algorithms consists of the distinctive usage of the policy to learn. *On-policy* algorithms profoundly depend on the training data sampled according to the current policy because they are designed to use only data gathered with the last learned policy. On the other hand, an *off-policy* method can use a different source of valuable data for the learning process instead of direct experience. This feature allows the agent to use, for instance, large experience buffers of past episodes. In this context, these buffers are usually randomly sampled in order to make the data closer to being independent and identically distributed (i.i.d): the random extraction guarantees this fact.

2.1.4 Dynamic programming

Dynamic programming (DP) is one of the approaches used to resolve RL problems. Formally, it is a general method to explain complex problems by breaking them into more manageable sub-problems. After solving all sub-problems, it is possible to sum them up in order to obtain the final solution to the whole original problem. This technique provides a practical framework to solve MDP problems and to observe what is the best result achievable from them, but it assumes to have full knowledge about the specific problem. For this reason, it applies primarily to model-based problems.

Furthermore, dynamic programming methods *bootstrap*: it means that these strategies use one or more estimated values in the update step for the same kind of estimated value, leading to results more sensitive to initial values.

Policy Iteration

The *policy iteration* aims to find the optimal policy by directly manipulating the starting policy. However, before proceeding with this process, a proper evaluation of the current policy is essential. This procedure can be done iteratively following algorithm A.1 on page 108 where θ is the parameter that defines the accuracy: the more the value is closer to 0, the more the evaluation would be precise.

Policy improvement is the second step towards policy iteration. Intuitively, it is possible to find a more valuable policy than the starting one by changing the action to select in a specific state with a more rewarding one. The key to check if the new policy is better than the previous one is to use the action-value function $Q_\pi(s, a)$. This function returns the value of taking action a in the current state s and, after that, following the existing policy π . If $Q_\pi(s, a)$ is higher than $V_\pi(s)$, so the action selected is better than the action chosen by the current policy, and consequently, the new policy would be better overall.

Policy improvement theorem is the formalisation of this fact: appendix A.2 on page 108 shows its demonstration. Thanks to this theorem, it is reasonable to act greedily to find a better policy starting from the current one iteratively selecting the action that produces the higher $Q_\pi(s, a)$ for each state.

The iterative application of policy improvement stops after an improvement step that does not modify the initial policy, returning the optimal policy found.

Value Iteration

The second approach used by dynamic programming to solve Markov decision processes is *value iteration*. Policy iteration is an iterative technique that alternate evaluation and improvement until it converges to the optimal policy. On the other hand, value iteration uses a modified version of policy evaluation to determine $V(s)$ and then it calculates the policy. The pseudocode of this method is available in algorithm A.2 on page 109.

Generalised Policy Iteration

Generalised Iteration Policy (GPI) indicates the idea underlying the interaction between evaluation and improvement steps seen in value and policy iteration. Figure 2.3 on the next page reports how the two processes compete and cooperate to find the optimal value function and an optimal policy. The first step, known as policy evaluation step, exploits the current policy to build an approximation of the

value function. The second step, known as policy improvement step, tries to improve the policy starting from the current value function. This iterative scheme of dynamic programming can represent almost all reinforcement learning algorithms.

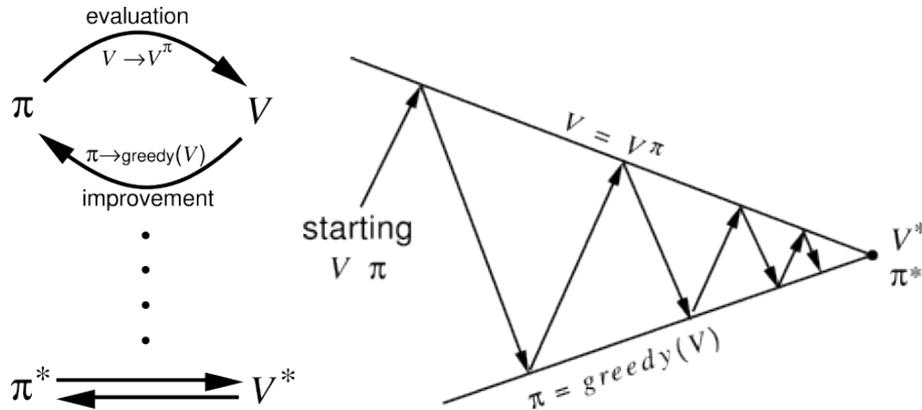


Figure 2.3. Generalised policy iteration (GPI) schema [66]. Value and policy functions compete and cooperate to reach the joint solution: the optimal value function and an optimal policy.

2.1.5 Model-free approach

As reported in the previous section, having a comprehensive knowledge of the environment is at the foundation of dynamic programming methods. However, this fact is not always accurate in practice, where it is infrequent to have a full understanding of how the world works. In these cases, the agent has to infer information using its experience, so it has to exploit model-free methods, based on the assumption that there is no prior knowledge about state transitions and rewards. This section intends to provide a brief description of two model-free approaches to prediction and control: *Monte Carlo* (MC) methods and *Temporal-Difference* (TD) ones.

Monte Carlo learning

Monte Carlo methods [66, Chapter 6] can learn from episodes of experience using the simple idea that averaging sample returns provide the value. This lead to the main caveat of these methods: they work only with episodic MDPs because the episode has to terminate before it is possible to calculate any returns. The total reward accumulated in an episode and the distribution of the visited states is used to calculate the value function while the improvement step is carried out by making the policy greedy concerning the value function.

This approach brings to light the exploration dilemma about how it is possible to guarantee that the algorithm will explore all the states without prior knowledge of the whole environment. ϵ -greedy policies are exploited instead of full greedy policy to solve this problem. An ϵ -greedy policy is a policy that acts randomly with probability ϵ and follows the policy learned with probability $(1 - \epsilon)$.

Unfortunately, even though Monte Carlo methods are simple to implement and they are unbiased because they do not bootstrap, they require a high number of iteration to converge. Furthermore, they have a wide variance in their value function estimation due to lots of random decisions within an episode.

Temporal Difference learning

Temporal Difference (TD) is an approach made combining ideas from both Monte Carlo methods and dynamic programming. TD is a model-free method like MC but uses bootstrapping to make updates as in dynamic programming. The central distinction from MC approaches is that TD methods calculate a *temporal error* instead of using the total accumulated reward. The temporal error is the difference between the new estimate of the value function and the old one. Furthermore, they calculate this error considering the reward received at the current time step and use it to update the value function: this means that these approaches can work with continuing (non-terminating) environments. This type of update reduces the variance compared to Monte Carlo one but increases the bias in the estimate of the value function because of bootstrapping.

The fundamental update equation for the value function is shown in eq. (2.9), where *TD error* and *TD target* are in evidence.

$$V(s_t) \leftarrow V(s_t) + \alpha \underbrace{\left(\overbrace{r_{t+1} + \gamma V(s_{t+1})}^{\text{TD target}} - V(s_t) \right)}_{\text{TD error } (\delta_t)} \quad (2.9)$$

Two TD algorithms for the control problem which are worth quoting because of their extensive use to solve RL problems are *SARSA* (*State-Action-Reward-State-Action*) and *Q-Learning*.

SARSA is an on-policy temporal difference algorithm whose first step is to learn an action-value function instead of a state-value function. This approach leads to focus not to estimate the specific value of each state, but to determine the value of transitions and state-action pairs. Equation (2.10) represents the update function of *SARSA*, while algorithm 2.1 on the following page summarise its pseudocode.

$$Q(s_t, a_t) \leftarrow Q(s_t, a_t) + \alpha [r_{t+1} + \gamma Q(s_{t+1}, a_{t+1}) - Q(s_t, a_t)] \quad (2.10)$$

Q-learning [74] is an off-policy TD control algorithm which represents one of the early revolution and advance in reinforcement learning. The main difference

Algorithm 2.1: SARSA (on-policy TD control) for estimating $Q \approx q_*$

Input: step size $\alpha \in (0,1]$, small $\epsilon > 0$

- 1 Initialise $Q(s, a) \forall s \in \mathcal{S}, a \in \mathcal{A}$ arbitrarily, except that $Q(\text{terminal}, \cdot) = 0$
- 2 **foreach** *episode* **do**
- 3 Initialise s_t
- 4 Choose a_t from s_t using policy derived from Q (e.g. ϵ -greedy)
- 5 **repeat**
- 6 Take action $a_t \rightarrow$ obtain r_{t+1} and s_{t+1}
- 7 Choose a_{t+1} from s_{t+1} using policy derived from Q (e.g. ϵ -greedy)
- 8 $Q(s_t, a_t) \leftarrow Q(s_t, a_t) + \alpha[r_{t+1} + \gamma Q(s_{t+1}, a_{t+1}) - Q(s_t, a_t)]$
- 9 $s_t \leftarrow s_{t+1} ; a_t \leftarrow a_{t+1}$
- 10 **until** s_t is terminal
- 11 **end**

from SARSA is the update rule for the Q-function: it selects the action in respect of an ϵ -greedy policy while the Q-function is refreshed using a greedy policy based on the current Q-function using a max function to select the best action to do in the current state with the current policy. Equation (2.11) represents the update function of *Q-learning*, while algorithm 2.2 summarise its pseudocode.

$$Q(s_t, a_t) \leftarrow Q(s_t, a_t) + \alpha[r_{t+1} + \gamma \max_a Q(s_{t+1}, a) - Q(s_t, a_t)] \quad (2.11)$$

Algorithm 2.2: Q-learning (off-policy TD control) for estimating $\pi \approx \pi_*$

Input: step size $\alpha \in (0,1]$, small $\epsilon > 0$

- 1 Initialise $Q(s, a) \forall s \in \mathcal{S}, a \in \mathcal{A}$ arbitrarily, except that $Q(\text{terminal}, \cdot) = 0$
- 2 **foreach** *episode* **do**
- 3 Initialise s_t
- 4 Choose a_t from s_t using policy derived from Q (e.g. ϵ -greedy)
- 5 **repeat**
- 6 Take action $a_t \rightarrow$ obtain r_{t+1} and s_{t+1}
- 7 Choose a_{t+1} from s_{t+1} using policy derived from Q (e.g. ϵ -greedy)
- 8 $Q(s_t, a_t) \leftarrow Q(s_t, a_t) + \alpha[r_{t+1} + \gamma \max_a Q(s_{t+1}, a) - Q(s_t, a_t)]$
- 9 $s_t \leftarrow s_{t+1} ; a_t \leftarrow a_{t+1}$
- 10 **until** s_t is terminal
- 11 **end**

Temporal Difference Lambda Learning

As reported previously, Monte Carlo and Temporal Difference learning perform updates in different ways. The first approach exploits the total reward to update the value function, while the second one, on the other hand, works with the reward of the current step. Temporal Difference Lambda, also known as TD(λ) [66, Chapter 7,12], represents a combination of these two procedures and it takes into account the results of each time step together with the weighted average of those returns. The idea of calculating TD target looking n-steps into the future instead of considering only a single step is the baseline of TD(λ). This lead to the formalisation of the λ -weighted return G_t^λ presented in eq. (2.12).

$$G_t^\lambda = (1 - \lambda) \sum_{n=1}^{\infty} \lambda^{n-1} G_t^{(n)} \quad (2.12)$$

TD(λ) implementation takes into account an additional variable called eligibility trace $e_t(s_t)$ which indicates how much learning should be carried out for each state for each timestep. It aims to describe how much the agent encountered a specific state recently and eq. (2.13) describes the updating rule of this value where the λ represents the trace-decay parameter.

$$e_t(s) = \gamma \lambda e_{t-1}(s) + \mathbb{1}(s = s_t) \quad (2.13)$$

2.1.6 Model-based approach

Heretofore, the focus of this section was on methods which have no prior knowledge of the environment, since this thesis grows on model-free foundations. Despite this point, it is worth to summarise the main concepts behind model-based approaches. Model-based methods gather information to enable the ability of planning, which can enhance the sample efficiency of the algorithm.

There are two primary principles to model-based learning. The first one implies to assemble a model starting from prior knowledge and to exploit it to calculate the policy and the value-function, while the second one is to infer the model from the environment by sampling experience. The central drawback of the first technique is that prior knowledge could be not as accurate as expected, leading to sub-optimal results. Consequently, the preferred way to learn is the second one.

The decisive point behind these approaches is that they are more sample-efficient concerning model-free ones: they require fewer data to learn a policy. On the other hand, the algorithm must learn the policy as well as the model: this translates to two different sources of approximation errors and an increase of computational complexity.

2.2 Deep reinforcement learning

The strategies shown so far works smoothly with systems with well-defined states and actions. In this context, it is reasonable to use lookup tables to describe the problem: state-value function V has an entry for each state while action-value function Q has an entry for each state-action pair. It is easy to understand how this setting cannot scale up with very large MDPs: problems regarding the availability of memory arise as it becomes difficult to manage the storage of a large number of states and actions. Also, there may be obstacles concerning the slowness of learning the value of each state individually. Furthermore, the tabular form could lead to expensive computation in linear lookup and can not work with continuous action and state spaces.

Function approximators represent the solution to overwhelm this problem. The underlying intention is to use a vector $\theta = (\theta_1, \theta_2 \dots, \theta_n)^T$ to estimate state-value and action-value function as shown in eq. (2.14), generalise from seen states to unseen states and finally update parameter θ using MC or TD Learning strategies.

$$\begin{aligned} V(s, \theta) &\approx V_\pi(s) \\ Q(s, a, \theta) &\approx Q_\pi(s, a) \end{aligned} \tag{2.14}$$

In these terms, function approximators can be considered as a mapping from the vector θ to the value function. This choice leads to a reduction in the number of parameters to learn and consequently to a system which can generalise better in fewer training samples.

Nowadays, since its widespread use in research, neural networks represent the most intuitive option to take as function approximator: it reduces the training time for high dimensional systems, and it requires less space in memory. This point represents the bridge between traditional reinforcement learning and recent discoveries in the theory of deep learning. Thanks to the last decade great fervour of deep learning, neural networks have become the fundamental tool to exploit as function approximator to develop deep reinforcement learning (Deep RL) which accomplished remarkable results. One of the first steps towards Deep RL and general artificial intelligence – an AI broadly applicable to a different set of various environments – was done by DeepMind with their pioneering paper [44] and the consequent [45].

Because of the nature of this work, the focus of this section will be on model-free algorithms. This section aims to explain the state-of-the-art and the leading theory behind Deep RL framework together with an overview about deep learning and the presentation of two deep actor-critic algorithms used in the experiments of this thesis: Deep Deterministic Policy Gradient (DDPG) and Soft Actor-Critic (SAC).

2.2.1 Fundamentals of deep learning

Artificial neural networks

Deep learning (DL) is an approach to learning based on a function $f : \mathcal{X} \rightarrow \mathcal{Y}$ parametrised with $w \in \mathbb{R}^{n_w} \mid n_w \in \mathbb{N}$ such that $y = f(x; w)$.

The starting point of this research field is the artificial neuron, inspired by the biological neuron from the brain of animals and human being. A neuron consists of numerous inputs called *dendrites* coming from preceding neurons. Therefore, the neuron elaborates the input and, only if the value reaches a specific potential, it *fires* through its single output called *axon*.

The neuron elaborates the inputs by taking the weighted sum, adding a bias b and applying an activation function f following the relation $y = f(\sum_n w x_i + b)$. Figure 2.4 shows the parallel comparison between the biological neuron and the artificial one. The set of parameter w needs to be adjusted to find a good parameter set: this process is called *learning*.

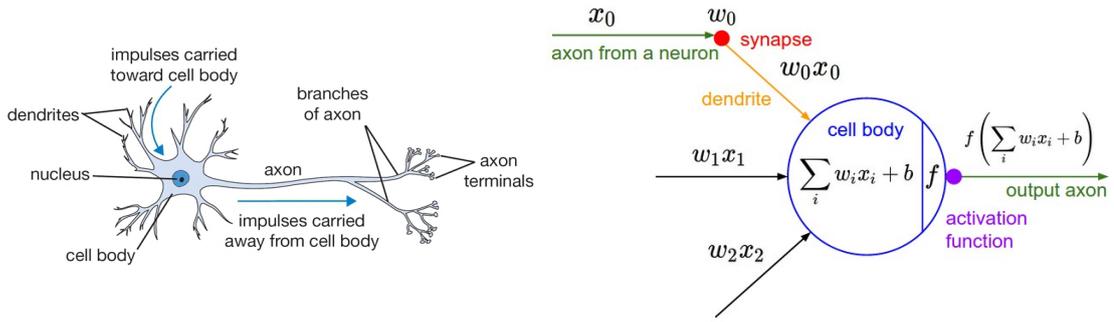


Figure 2.4. Comparison between biological neuron (left) and artificial neuron (right). The artificial neuron designs the dendrites as weighted inputs and returns the sum through an activation function. [65].

A deep neural network (NN) organises a set of artificial neurons in a series of processing layers to which correspond non-linear transformation. The whole sequence of these alterations directs the learning process through different levels of abstraction [13]. To better understand the nature of a deep neural network, it is convenient to describe a neural network with one fully-connected layer represented by fig. 2.5 on the next page.

$$\begin{aligned} h &= g(w_1 \cdot i + b_1) \\ o &= w_2 \cdot h + b_2 \end{aligned} \tag{2.15}$$

The input layer receives as input a column vector of input-features i of size $n \in \mathbb{N}$. Every value of the hidden-layer represented by a vector h of size $m \in \mathbb{N}$ is the result of a transformation of the input values given by eq. (2.15) where w_1 is a

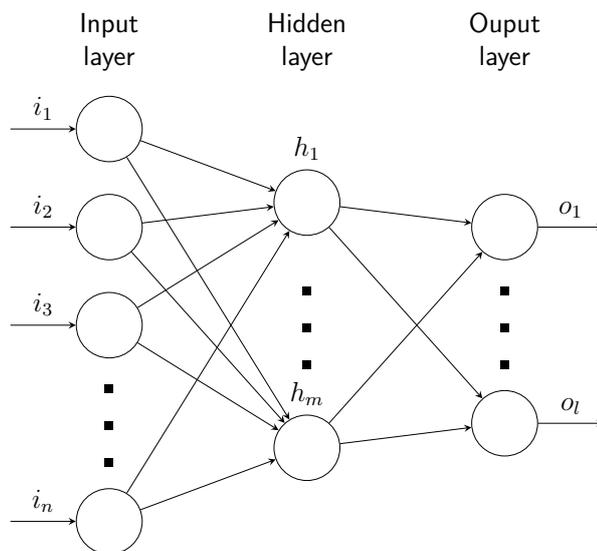


Figure 2.5. An example representation of a deep neural network with one fully-connected hidden layer.

matrix of size $m \times n$ and b_1 is a bias term of size m . g is a non-linear parametric function called activation function, which represents the core of neural networks. Subsequently, the second and last transformation manipulates the hidden layer h to produce the values of the output layer following eq. (2.15) on the previous page using w_2 with size $o \times m$ and b_2 with size o .

Learning process

The learning process aims to seek a set of parameters θ that results in the best possible function approximation for a specific objective. In supervised learning, the actual output Y is available for each particular input X , and it is used to update the parameters. The learning process can be carried out iteratively according to the following steps.

Forward pass The input X is forwarded through the neural network and the output $Y_{pred} = f(X, \theta)$ is gathered.

Loss The resulting predicted value Y_{pred} is compared with the actual value Y computing the loss function $L(\theta)$. There are a lot of loss functions available to satisfy the particular needs of specific learning tasks. The *error* is the difference between the output of the neural network for a specific input data and the actual value: it is essential to calculate the loss function. One of the most exploited loss

function is the *Mean-Squared Error* (MSE) [59] shown in eq. (2.16) which works with L2-distance.

$$\begin{aligned} L(y, \hat{y}) &= (y_{\theta} - y)^2 \\ J &= \frac{1}{n} \sum_{i=1}^n L(y_i, f(x_i)) \end{aligned} \tag{2.16}$$

Backpropagation The next step is the computation of the global gradient of the loss function $\nabla L(\theta)$, which is carried out together with its backpropagation through the network. The backpropagation algorithm [56] calculates the local gradient of loss for each neuron in the hidden layers. The concept underlying this procedure and shown in eq. (2.17) is the *chain rule* [39], which computes derivatives of composed functions by multiplying local derivatives.

$$y = g(x), \quad z = f(g(x)), \quad \frac{\partial z}{\partial x} = \frac{\partial z}{\partial y} \frac{\partial y}{\partial x} \tag{2.17}$$

Therefore, the chain rule is exploited to propagate the calculated global gradient loss $\frac{\partial L(\theta)}{\partial \theta}$ back through the network, in the opposite direction of the forward pass. The procedure calculates the local derivatives during the forward pass and estimates the local gradient of loss during backpropagation determining the multiplication between the local derivative and the local gradient of the loss of the connected neuron of the next layer: if the neuron has multiple connections neurons, the algorithms adds up all the gradients.

Update The final step consists in the update of the weights of all neurons. There are many ways developed through the years to carry out the update phase, but the most common one is the gradient descent. The objective of the gradient descent is to minimise the loss function by refreshing the internal parameters of the network in the negative direction of the gradient loss: this choice leads the function approximation process closer to the minimum at each iteration. Equation (2.18) describes the update rule presented by the gradient descent where α is the learning rate. The last-mentioned parameter determines how quickly the algorithm should approach the minimum. A higher learning rate leads to a more significant step towards the minimum, which threatens to overshoot the target.

$$\theta \leftarrow \theta - \alpha \nabla_{\theta} J \tag{2.18}$$

Nowadays, the technique applied in the majority of research projects is stochastic gradient descent (SGD) which combines batch learning [65] and gradient descent, but also its various improved extensions and variants, such as ADAM [31] and AdaGrad [12]: these extensions manage to improve the convergence of SGD thanks to the introduction of adaptive learning rates.

Regularisation

The final aim of the learning process is to obtain a function approximator capable of generalising over data. This fact means that a neural network should show performances on unseen data comparable to the one obtained from training data. For this reason, it is necessary an appropriate trade-off between underfitting and overfitting.

A shallow approximated function and insufficient training data with a lack of diversity are the leading cause to the first situation: the network generalises on the data, but the prediction error is always too high for all data points. The phenomenon of overfitting describes the exact contrary of underfitting. The leading cause is a too complex approximation function: this lead to a network which scores an excellent performance on training data, but poorly predicts unseen points.

Regularisation [5, 39] represents an approach to overcome and prevent the problem of overfitting. It works extending the loss function with a regularised term $\Omega(\theta)$ as shown in eq. (2.19) where λ is the regularisation factor.

$$L'(\theta) = L(\theta, Y, Y_{pred}) + \lambda\Omega(\theta) \quad (2.19)$$

Equations (2.20) and (2.21) show two examples of regularisation terms. The first is L^2 -regularisation which exploits the squared sum of the weights θ in order to keep the weights small. The second approach is known as L^1 -regularisation: in this case, large weights are less penalised, but this method leads to a sparser solution.

$$L'(\theta) = L(\theta, Y, Y_{pred}) + \lambda\frac{1}{2}\|\theta\|^2 \quad (2.20)$$

$$L'(\theta) = L(\theta, Y, Y_{pred}) + \lambda\frac{1}{2}\|\theta\| \quad (2.21)$$

Activation function

Equation (2.22) shows the most common activation functions: in general, *ReLU* achieves better performance over a wide variety of tasks, but usually, the selection of the best activation function has to be done starting from all information and requirements of the deep learning model.

$$\begin{aligned} \text{Sigmoid} &\rightarrow g(x) = \frac{1}{1 + e^{-x}} \\ \text{Hyperbolic Tangent} &\rightarrow g(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}} \\ \text{Rectified Linear Unit (ReLU)} &\rightarrow g(x) = \max(0, x) \end{aligned} \quad (2.22)$$

Batch Learning and Normalisation

The basic concept underlying *batch learning* [65] is to process a set of n training samples called also *mini-batches* in the place of a single one. This method works with the gradient averaged over all the samples in the mini-batch: it leads to a more accurate gradient reducing its variance and the training time.

Batch normalisation consists of zero-centring and rescaling all data in a specific batch, resulting in a mean of normalised data close to 0 and a variance close to 1. The algorithm presented in algorithm 2.3 is the one provided in [27]. This method computes the mean μ_β and the variance σ_β element-wise for each spatial position in the batch: $\epsilon > 0$ is a small value to avoid the division by zero. The batch normalisation layer then processes the resulting normalised value: γ and β are the parameters of this layer that are in addition to the original parameter set θ of the neural network in the learning process. The new learning dynamic provided by the addition of this class of layer increases the network expressivity: applying this method to the input data and the output of any hidden layer results in the reduction of the training time, better regularisation during learning and the reduction of the overfitting phenomenon.

Algorithm 2.3: Batch normalisation

Input: Mini-batch $\mathcal{B} = x_{1\dots m}$; γ and β parameters to be learned

Output: $y_i = \text{BN}_{\gamma,\beta}(x_i)$

- 1 $\mu_\beta \leftarrow \frac{1}{m} \sum_{i=1}^m x_i$ // Mini-batch mean
 - 2 $\sigma_\beta^2 \leftarrow \frac{1}{m} \sum_{i=1}^m (x_i - \mu_\beta)^2$ // Mini-batch variance
 - 3 $\hat{x}_i \leftarrow \frac{x_i - \mu_\beta}{\sqrt{\sigma_\beta^2 + \epsilon}}$ // Normalisation
 - 4 $y_i \leftarrow \gamma \hat{x}_i + \beta \equiv \text{BN}_{\gamma,\beta}(x_i)$ // Scale and shift
-

Convolutional Neural Networks

Sensory reception represents how humans and animals react to changes: it consists of sensors which process the input data and are sensitive to specific stimuli. This system inspired the architecture underlying Convolutional Neural Networks: they could efficiently handle significant input data with many applications in computer vision. Figure 2.6 on the next page displays the *LeNet-5* [40] which is capable to recognise digits in images. It represents a perfect example of a standard convolutional neural network architecture: it consists of a series of convolutional layers followed by a subsampling pooling layer. At the end of the convolutional stack, the values map into final hidden layers of the network to compute the final low-dimensional output of the network: fully-connected layers usually compose these

final layers. It is possible to suppose that the first layers have to learn low-level features of the input data while succeeding layers are responsible for combining the last-mentioned features in high-level ones.

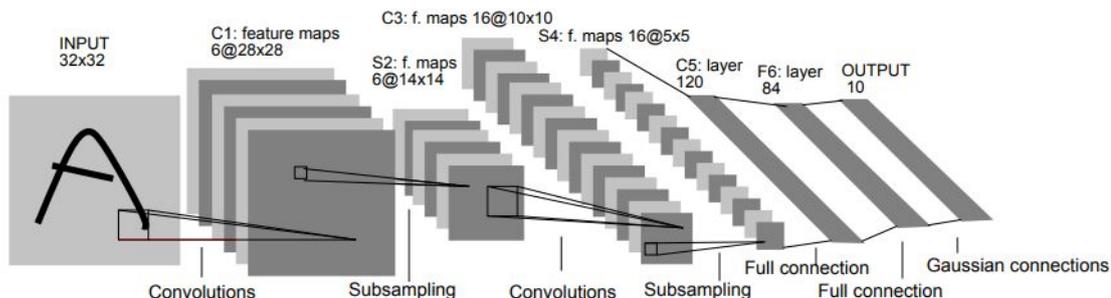


Figure 2.6. LeNet Architecture Representation. It consists of two distinct parts. The first one is composed of two stacks of convolutional and pooling layer. The last part is composed of two fully connected layers that produce the output. It represents the first compelling evidence showing the results of training convolutional neural networks by backpropagation. It was adopted to recognise digits for processing deposits in ATMs. [40]

Convolutional Layer Convolutional layers [38] operates with a set of learnable filters (called kernels) with dimensions $n \times m$ smaller than the whole input image. The convolution is the essential operation employed in these class of layer: it consists in convolving each filter across the width and height of the input data and computing dot products between the values in the filter and the ones in the input at any position. The result of this operation is a 2-dimensional activation map that contains the results of that filter at every spatial position. In this context, the network can learn filters that detect specific features in the image such as edges, textures and patterns [13].

It is possible to compute the output size $W_2 \times H_2 \times D_2$ of a convolutional layer starting from the input size $W_1 \times H_1 \times D_1$ and from the hyperparameters of this class of layer: the number of filters K , their spatial extent F , the stride S and the amount of padding P . The resulting volume size can be calculated using the relations reported in eq. (2.23).

$$\begin{aligned} W_2 &= (W_1 - F + 2P)/S + 1 \\ H_2 &= (H_1 - F + 2P)/S + 1 \\ D_2 &= K \end{aligned} \tag{2.23}$$

The number of parameters introduced by a single kernel is equal to $F \cdot F \cdot D_1$, so the convolutional layer has a total of $(F \cdot F \cdot D_1) \cdot K$ weights and K bias.

In a convolutional layer, the number of weights is kept small and then the computation is more efficient than the one of a fully-connected layer: small filters

need fewer parameters and less work in the convolutional operation. Besides this motivation, the filters are kept small also because it makes them capable of learning small and low-level features. The great innovation behind convolutional layers is that the same neuron can recognise the related learned features even if they emerge in different locations of the image: this is the property of translation invariance of feature detection.

Pooling Layer It is common to insert a pooling layer in-between successive convolutional layers. The main objective of this class of layers is to apply a down-sampling filter on the input: it progressively reduces the spatial size of the representation, decreasing the number of parameters and the computational cost in the network. It is also useful to control overfitting.

It is possible to compute the size of the output $W_2 \times H_2 \times D_2$ of a pooling layer using starting from the size of the input $W_1 \times H_1 \times D_1$ and from the hyperparameters of this class of layer: the spatial extent of the filter F , the stride S . The resulting volume size can be calculated using the relations reported in eq. (2.24).

$$\begin{aligned} W_2 &= (W_1 - F)/S + 1 \\ H_2 &= (H_1 - F)/S + 1 \\ D_2 &= D_1 \end{aligned} \tag{2.24}$$

The most common types of pooling layer are the *max-pooling* and the *average-pooling* layer. Both classes return a single value for each position of the filter: the first returns the maximum value, while the second returns the average among the values in the specific section of the input.

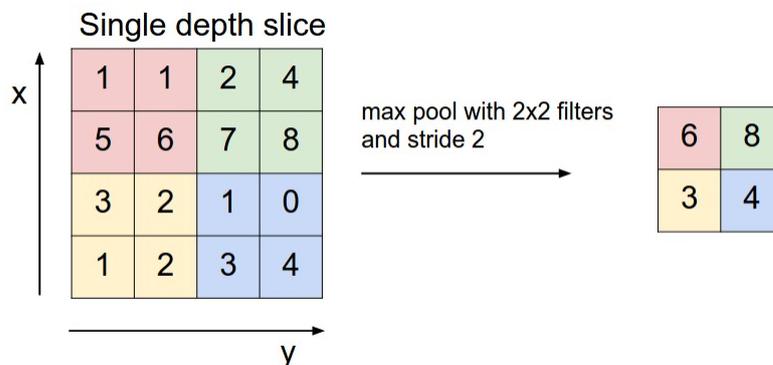


Figure 2.7. Example of a max-pooling operation with a stride of 2 and a spatial extent of 2. [65].

It is worthy of using a pooling layer in a situation where the exact feature position is not relevant but rather whether a particular feature exists in the input at all. Increasing the stride of convolutional layers represent an alternative approach to downsample without the usage of max-pooling layers [64].

2.2.2 Value-based methods

The first class of algorithms to explore is value-based one. They work learning an approximator $Q_\theta(s, a)$ to infer the optimal action-value function $Q^*(s, a)$ using an objective function based on Bellman equations. The preponderance of optimisations belonging to this category is *off-policy*: this means that the optimisation step is done using all data collected during the whole training, not only with the most recent policy available. In this configuration, the information used for the learning phase could also come from exploration decision, apart from ones obtained with the most recent policy. Indeed, value-based approaches are more sample efficient because they can reuse data more efficiently, but they are considered less stable than policy gradient ones. Thanks to the relation expressed by $a(s) = \operatorname{argmax}_a Q_\theta(s, a)$, it is possible to obtain the policy learned so far from the current action-value function.

Deep Q-Network (DQN)

This algorithm grows from the ideas underlying Q-Learning [74] shown previously in section 2.1.5 on page 15. The team of DeepMind introduced the Deep Q-Network (DQN) in [44] and in the next cutting-edge paper [45]: they managed to create an algorithm capable of learning to play ATARI video-games online using raw image and pixels. It works with neural networks as a function approximator, employing convolutional layers as first layers of the neural network and performing the optimisation with a variant of stochastic gradient descent called RMSprop [67]. The exploited neural network provides as output a probability distribution over all possible discrete actions to determine what is the best action to take.

To overcome the instability problem of value-based methods, DQN utilises two heuristics to narrow instabilities.

Target Network The presence of a second network, also called *target network*, enriches the update phase of this algorithm. Equation (2.25) defines the loss function of DQN where y_i value is computed using the target network instead of the local network. Therefore, the parameters of the target network are hard updated every $I \in \mathbb{N}$ iterations: this choice precludes instabilities and avoids divergence because of target networks parameters remain fixed for I iterations.

$$\begin{aligned} L_i(\theta_i) &= \mathbb{E}_{s,a \sim \pi} \left[(y_i - Q(s, a; \theta_i))^2 \right] \\ y_i &= \mathbb{E}_{s' \sim E} [r + \gamma \max_{a'} Q(s', a'; \theta_{i-1}) | s, a] \end{aligned} \tag{2.25}$$

Experience Memory Replay Another crucial introduction in this algorithm is *experience memory replay buffer* [42]. Trajectories sampled from the environment are temporally correlated, and this could lead to overfitting the parameters of the neural network because the data are not independent and identically distributed

(*i.i.d.*). The setting of this algorithm is *online* because the replay buffer stores $N_{\text{replay}} \in \mathbb{N}$ replacing old steps as new ones arrive. The experience is collected as tuples (s_t, a_t, r_t, s_{t+1}) using the ϵ -greedy policy. The learning phase samples a set of limited tuples called *mini-batch* allowing a wider set of state-action pair in the update of the network and improving the procedure in terms of variance in respect of single tuple update. Trajectories sampled from the environment are temporally correlated, and this could lead to overfitting the parameters of the neural network. Using a batch sample from the replay buffer makes the data *i.i.d.* and consequently improves the learning.

Improvements of DQN

Further investigation and speculation followed the publication of the thriving DQN. Summing up and comparing these new approaches to original DQN is the main aim of *Rainbow* [25]: it also introduces an algorithm called *Rainbow DQN* with all the techniques proposed. The following paragraphs will delineate three main improvements of DQN.

Double DQN The double DQN [22, 72] improvement can handle the intricacy of overestimation of Q-values caused by the maximisation step in eq. (2.25) on the preceding page. It works with two separate Q-Network with parameters θ and θ^- for estimating TD-target. It allows for removing the positive bias in estimating action values, leading to less overestimation of Q-learning values, improved stability and performance. In this context, the target y_i is replaced by eq. (2.26).

$$y_i = \mathbb{E}_{s' \sim E}[r + \gamma Q(s', \underset{a}{\operatorname{argmax}} Q(s', a; \theta_{i-1}); \theta_{i-1}^-) | s, a] \quad (2.26)$$

Prioritised Experience Replay The fundamental idea underlying *prioritised experience replay* [57] is precisely to prioritise experiences that contain more crucial information than other ones. An additional value that defines the priority of a specific transition joins each tuple stored in the replay buffer: thanks to this approach, experiences with higher priority has a higher sampling probability and are more likely to remain longer in the replay buffer. It is possible to use *TD-error* to measure the importance of each tuple in the experience. A high TD-error means that the agent behaved better or worse than expected in that particular moment, and therefore, it can learn more from that specific passage.

Dueling DQN The Dueling DQN architecture [73] presented in fig. 2.8 on the following page works decoupling the Q-value estimation in two distinct sequences of fully-connected layers right after convolutional layers.

These streams are capable of providing separate estimates of the state-value $V(s; \theta, \beta)$ and advantage $A(s, a; \theta, \alpha)$ functions exploited in the end to obtain the

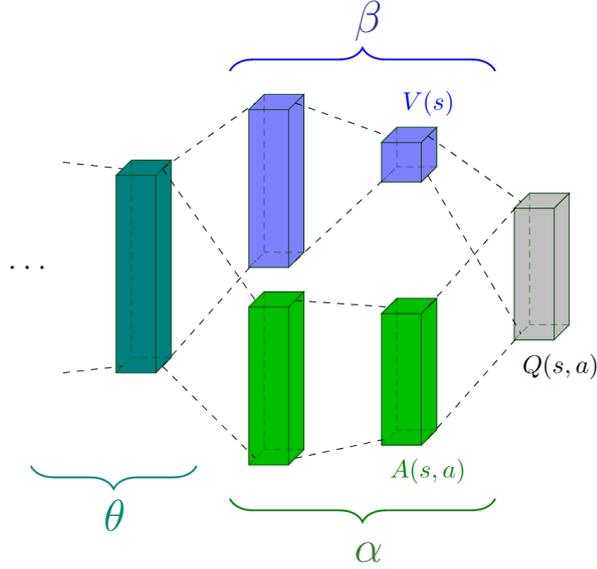


Figure 2.8. Dueling DQN architecture [73]: it consists in two stream to estimate state-value parametrised with β and advantages values parametrised with α for each action. The last layer represent the combination of these two types of values to obtain the Q-function. [15]

Q-value function $Q(s, a; \theta, \alpha, \beta)$ estimate where θ represents the parameters of convolutional layers while α and β the ones of state-value and advantage function respectively.

The first formalisation of the Q-value function is shown by eq. (2.27), but [73] also suggests a different approach shown in eq. (2.28) with increased stability in practice.

$$Q(s, a; \theta, \alpha, \beta) = V(s; \theta, \beta) + \left(A(s, a; \theta, \alpha) - \max_{a' \in \mathcal{A}} A(s, a'; \theta, \alpha) \right) \quad (2.27)$$

$$Q(s, a; \theta, \alpha, \beta) = V(s; \theta, \beta) + \left(A(s, a; \theta, \alpha) - \frac{1}{|\mathcal{A}|} \sum_{a' \in \mathcal{A}} A(s, a'; \theta, \alpha) \right) \quad (2.28)$$

2.2.3 Policy gradient methods

Policy gradient algorithms aim to optimise the policy performance measure in eq. (2.29) on the next page by finding a suitable policy $\pi_\theta(s|a)$ capable of generating a trajectory τ that maximises the expected rewards eq. (2.30) on the following page instead of learning a value function. Indeed the objective function in policy gradient methods consists of maximising $J(\theta)$ value by finding a proper policy by

updating θ parameters directly.

$$J(\theta) = \mathbb{E} \left[\sum_{t=0}^N r(s_t, a_t); \pi_\theta \right] = \sum_{\tau} P(\tau; \theta) r(\tau) \quad (2.29)$$

$$\theta^* = \underset{\theta}{\operatorname{argmax}} J(\theta) \quad (2.30)$$

Stochastic gradient ascent is used to refresh the parameters of the policy θ . Gradient ascent is the inverse of gradient descent and updates the parameters θ_t in the positive direction of the gradient of the policy's performance measure $\nabla_{\theta} J(\theta)$ following eq. (2.31) where α is the learning rate which defines the strength of the steps in the direction of the gradient.

$$\theta_{t+1} \leftarrow \theta_t + \alpha \nabla_{\theta} J(\theta_t) \quad (2.31)$$

The main advantage of policy gradient approaches consists in the stability of their convergence: these methods work updating their policy directly at each time step instead of renewing value function from which to derive the policy like value-based methods. Last-mentioned approaches can lead to a radical change in the policy output even for a small change in the value function: this event can cause prominent oscillation during training. Furthermore, policy gradient algorithms can face infinite and continuous action space because the agent estimates the action directly instead of calculating the Q-value for each possible discrete action. The third feature is their ability to learn stochastic policies, useful in uncertain contexts or partially observable environments. Despite the presence of the advantages just mentioned, policy gradient methods have a substantial disadvantage: they tend to converge to a local maximum instead of the global optimum.

Actor-Critic Architecture

Actor-critic architecture, shown in fig. 2.9 on the following page, represents the point of contact between value-based approaches and policy gradient methods. They are policy gradient methods basically but exploit value-function to learn the parameters θ of the policy. As its name suggests, these approaches work with two different parts called *actor* and *critic* [33]. The *actor* relates to the policy, while the *critic* deals with the estimation of a value function (e.g. Q-value function). In the context of deep reinforcement learning, they can be represented using neural networks function approximator [43]: the actor exploits gradients derived from the policy gradient theorem and adjusts the policy parameters, while the critic estimates the approximate value function for the current policy π .

Standard practice is to update both networks with the *TD-Error*, discussed in section 2.1.5 on page 15. Estimation made by the critic is useful to determine the contribution that expected values of the current and next state gives to the TD-error. Essentially, the output of the critic contributes to the update of the actor.

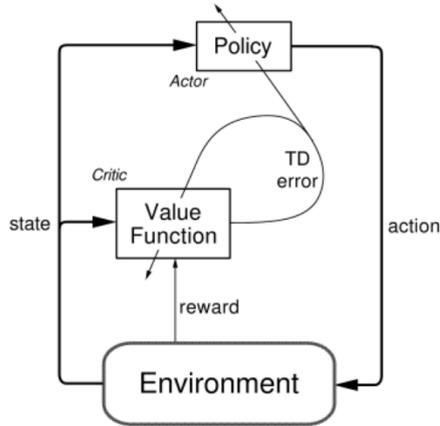


Figure 2.9. Actor-critic architecture schema: the actor represents the policy and maps the input state to an output action, while the critic represents the value function. Both networks can be updated using the contribution of the critic. It is noticeable that the actor uses the critic during the learning process [66].

2.2.4 Deep Deterministic Policy Gradient (DDPG)

Deep Deterministic Policy Gradient (DDPG) [41] is a policy gradient algorithm that works learning a Q-function and a policy, and that grows from the deterministic policy gradient algorithm (DPG) [63]. It is a model-free, off-policy, actor-critic algorithm which utilises deep function approximators to learn policies in high-dimensional, continuous action spaces. It can be applied to situations that can not be solved using *DQN* algorithm [45] because of the presence of continuous action spaces. A fine discretisation of the action space to adapt the situation to DQN would lead to an explosion in the number of discrete actions and the curse of dimensionality. *Bellman equation* and *Q-learning* are integral parts of this algorithm. The algorithm concurrently learns a Q-value function and a policy: it uses off-policy data and the Bellman equation to learn the Q-value function and uses the Q-value function to learn the policy.

Usually, in reinforcement learning, if the optimal action-value function $Q^*(s, a)$ is known, then in any given state, the optimal action $a^*(s)$ can be found by solving eq. (2.32).

$$a^*(s) = \arg \max_a Q^*(s, a) \quad (2.32)$$

When the number of discrete actions is finite, calculating the max poses no problem, because the Q-values can be calculated for each action separately, then directly compared. However, when the action space is continuous, this process becomes highly non-trivial: it would need to be run at every step of the episode, whenever the agent wants to take any action in the environment, and this can not work.

Because the action space is continuous, the function $Q^*(s, a)$ is presumed to

be differentiable concerning the action argument. For this reason, an efficient, gradient-based learning rule for a policy $\pi(s)$ which exploits that fact can be set up, approximating it with $\max_a Q(s, a) \approx Q(s, \pi(s))$.

Target networks

DDPG algorithm exploits 4 neural networks: the *local actor* π , the *local critic* Q , the *target actor* π' and the *target critic* Q' . Actor networks aim to approximate the policy using parameters θ while critic networks approximate the Q-Value function using parameters ϕ .

Initially, actor and critic networks have both randomly initialised parameters. Then the local actor – the current policy – starts to propose actions to the agent, given the current state, starting to populate the experience replay buffer.

When the replay buffer is big enough, the algorithm starts to sample randomly a mini-batch of experiences for each timestep t . This mini-batch is used to update the local critic minimising the Mean Squared Error (MSE) between the local Q-value and the target one shown in eq. (2.33) where $y_i = y_t$ given by eq. (2.36) on the following page and to update the actor policy using the sampled policy gradient defined in eq. (2.39) on the next page.

$$L = \frac{1}{N} \sum_i (y_i - Q(s_i, a_i | \phi))^2 \quad (2.33)$$

We can imagine the target networks as the *labels* of supervised learning.

Also, the target networks are updated in this *learning step*. A mere copy of the local weights is not an efficient solution because it is prone to divergence. For this reason, a *soft* target updates is used. It is given by eq. (2.34) where $\tau \ll 1$.

$$\theta' \leftarrow \tau\theta + (1 - \tau)\theta' \quad (2.34)$$

Learning equations

The two fundamental functions in reinforcement learning exploited in DDPG are the *action-value function* – see eq. (2.6) on page 9 – and the correspondent *Bellman equation* – see eq. (2.7) on page 10. If this policy is deterministic we can describe it as a function $\pi : \mathcal{S} \leftarrow \mathcal{A}$ obtaining eq. (2.35) which depends only on the environment.

$$Q^\pi(s_t, a_t) = \mathbb{E}_{r_t, s_{t+1} \sim E} [r(s_t, a_t) + \gamma Q^\pi(s_{t+1}, \pi(s_{t+1}))] \quad (2.35)$$

This means that it is possible to learn Q^π off-policy, using transition generated by a different stochastic behaviour policy β .

Focusing more and more on DDPG, the Bellman equation is the starting point for learning an approximator to $Q^*(s, a)$ of Q-Learning. The approximator is

parametrised by ϕ and the value network is updated and optimised by minimising the loss defined in eq. (2.36) where d_t is a flag which indicates whether the state s_{t+1} is terminal.

$$\begin{aligned} L(\phi) &= \mathbb{E}_{s_t \sim \rho^\beta, a_t \sim \beta, r_t \sim E} [(Q(s_t, a_t | \phi) - y_t)^2] \\ y_t &= r(s_t, a_t) + \gamma(1 - d_t)Q'(s_{t+1}, \pi'(s_t + 1 | \bar{\theta}) | \bar{\phi}) \end{aligned} \quad (2.36)$$

It is clear from the eq. (2.36) that the loss is calculated starting from the transitions generated by the policy β . For this reason a great importance in this algorithm is given to *replay buffer* – see section 2.2.2 on page 26 – and *target networks* – see section 2.2.4 on the previous page.

From the policy perspective, the objective is to maximise eq. (2.37) calculating the policy loss through the derivative of the objective function concerning the policy parameter eq. (2.38). However, since the algorithm is updating the policy in an off-policy way with batches of experience, it is possible to use the mean of the sum of gradients calculated from the mini-batch eq. (2.39).

$$J(\theta) = \mathbb{E}[Q(s, a)|_{s=s_t, a=\pi(s_t)}] \quad (2.37)$$

$$\nabla_\theta J(\theta) \approx \nabla_a Q(s, a) \nabla_\theta \pi(s | \theta) \quad (2.38)$$

$$\nabla_\theta J(\theta) \approx \frac{1}{N} \sum_i \left[\nabla_a Q(s, a | \phi) |_{s=s_i, a=\pi(s_i)} \nabla_\theta \pi(s | \theta) |_{s=s_i} \right] \quad (2.39)$$

Algorithm 2.4 on the next page shows the pseudocode of the DDPG algorithm.

Exploration vs. Exploitation

In reinforcement learning for discrete action spaces, exploration is done selecting a random action (e.g. epsilon-greedy). For continuous action spaces, exploration is done adding noise to the action itself. In [41], the authors use Ornstein-Uhlenbeck process [71] to add noise to the action output $a_t = \pi(s_t | \theta) + \mathcal{N}$. After that, the action is clipped in the correct range.

Hyperparameters

Exploration noise The exploration noise consists of two sets of parameters. The first set refers to the Ornstein-Uhlenbeck Process noise parameters π, σ, θ as reported in [71]. The second one consists of the parameters of ϵ , a small value to decrease the impact of the noise on the action. Equation (2.40) describes how the impact of the noise decreases in function of the current episode number e , where ϵ_{start} represent the starting value of the noise and ϵ_{end} the final one.

$$\epsilon = \epsilon_{\text{start}} - (\epsilon_{\text{start}} - \epsilon_{\text{end}}) \min \left(1.0, \frac{e}{\epsilon_{\text{decay}}} \right) \quad (2.40)$$

Replay buffer The parameters available for replay memory are its maximum size, its minimum size to start the learning phase and the mini-batch size to sample for each learning step.

Neural Network The neural network can be considered as a whole complex hyperparameter because it is possible to select among different layers to exploit for specific problems – e.g. the number of layers, the type of layers, the number of hidden features. Given the network architecture, the primary neural networks hyperparameters are the learning rate α and the update method – e.g. Adaptive Momentum Estimation (ADAM).

Learning Update The parameters of the learning phase of the algorithm are mainly two. The first one is γ , the main parameter in the reinforcement learning framework, which characterises the discounted return. The second is the soft target update parameter τ , which determinates the entity of the update of the network at each learning step.

Algorithm 2.4: DDPG Algorithm [41]

Input: Initial critic network Q with parameter ϕ and actor network π with parameter θ

- 1 Initialise target networks Q' and π' with weights $\bar{\phi} \leftarrow \phi, \bar{\theta} \leftarrow \theta$
- 2 Initialise replay buffer \mathcal{D}
- 3 **for** $episode = 1, M$ **do**
- 4 Initialise a random process \mathcal{N} for action exploration
- 5 Receive the initial observation state $s_t \leftarrow s_1$
- 6 **repeat**
- 7 Select action $a_t = \pi(s_t|\theta) + \mathcal{N}$ and *clip* results
- 8 Execute action a_t , obtain tuple $(s_t, a_t, r_t, s_{t+1}, d_t)$ and store in \mathcal{D}
- 9 **if** *it is time to update* **then**
- 10 Sample random minibatch of N transitions $(s_t, a_t, r_t, s_{t+1}, d_t)$ from \mathcal{D}
- 11 Compute the target $y_t = r_t + \gamma(1 - d_t)Q'(s_{t+1}, \pi'(s_{t+1}|\bar{\theta})|\bar{\phi})$
- 12 Update the critic by minimising the loss: $L = \frac{1}{N} \sum_i (y_i - Q(s_i, a_i|\phi))$
- 13 Update the policy using the sampled policy gradient:
 $\nabla_{\theta} J \approx \frac{1}{N} \sum_i \nabla_a Q(s, a|\phi)|_{s=s_i, a=\pi(s_i)} \nabla_{\theta} \pi(s|\theta)|_{s_i}$
- 14 Soft update Target Critic: $\bar{\phi} \leftarrow \tau\phi + (1 - \tau)\bar{\phi}$
- 15 Soft update Target Policy: $\bar{\theta} \leftarrow \tau\theta + (1 - \tau)\bar{\theta}$
- 16 **end**
- 17 $s_t \leftarrow s_{t+1}$
- 18 **until** s_t *is terminal*
- 19 **end**

2.2.5 Soft Actor-Critic (SAC)

Soft Actor-Critic (SAC) [20, 21] combines the off-policy actor-critic setup with a stochastic policy (actor), devising a bridge between stochastic policy optimisation and DDPG-style approaches. As DDPG, SAC can work in situations characterised by the presence of continuous action spaces, and it is model-free.

SAC algorithm can overcome some of the problems of DDPG. The latter can achieve excellent performance, but the interaction between the deterministic actor-network and the Q-function makes it difficult to stabilise and brittle concerning hyperparameters and other kinds of tuning [11, 24]. The learned Q-function begins to dramatically overestimate Q-values, which then leads to the policy breaking because it exploits the errors in the Q-function. For this reason, SAC exploits *Clipped Double-Q Learning* also used by Twin Delayed DDPG (TD3) [16]. It learns two Q-functions instead of one and uses the smaller of the two Q-values to form the targets in the Bellman error loss functions.

Another feature of SAC is *entropy regularisation* [77, 70, 53, 14, 19]. The policy is trained to maximise a trade-off between expected return and entropy, a measure of randomness in the policy. This peculiarity is strongly related to the exploration-exploitation trade-off: increasing entropy results in more exploration, which can accelerate learning later on, but it can also prevent the policy from prematurely converging to a local optimum.

Target networks

SAC algorithm exploits 5 neural networks: the local stochastic policy network with parameter θ , two local Q-Networks with parameters ϕ_1, ϕ_2 respectively, two target Q-Networks with parameters $\bar{\phi}_1$ and $\bar{\phi}_2$ respectively. Their behaviour is the same as the one of DDPG target network: the algorithm updates the target networks following eq. (2.34) on page 31.

Algorithm 2.5 on page 37 shows the pseudocode of the SAC algorithm.

Entropy-Regularised Reinforcement Learning

Entropy represents the average rate at which a stochastic source of data produces information. It is, in simple terms, a quantity which describes how random a random variable is. The motivation behind the use of entropy is that when the data source produces a low-probability value, the event carries more information than when the source data produces a high-probability value.

Let x be a random variable with probability mass or density function P . The entropy \mathcal{H} of x is computed from its distribution P according to eq. (2.41).

$$\mathcal{H}(P) = \mathbb{E}_{x \sim P}[-\log P(x)] \quad (2.41)$$

In *entropy-regularised* reinforcement learning the standard objective is generalised by augmenting it with entropy. The agent gets a bonus reward at each time step proportional to the entropy of the policy at that timestep. Assuming an infinite-horizon discounted setting, this changes the RL problem as shown in eq. (2.42) where $\alpha > 0$ is the temperature parameter that determines the relative importance of the entropy term controlling the stochasticity of the optimal policy.

$$\pi^* = \arg \max_{\pi} \mathbb{E}_{\tau \sim \pi} \left[\sum_{t=0}^{\infty} \gamma^t \left(R(s_t, a_t, s_{t+1}) + \alpha \mathcal{H}(\pi(\cdot|s_t)) \right) \right] \quad (2.42)$$

It is clear that the standard maximum expected return can be retrieved in the limit as $\alpha \rightarrow 0$.

From eq. (2.42) it is possible to derive *state-value function* $V^\pi(s)$ and *action-value function* $Q^\pi(s, a)$ as shown in eq. (2.43) and eq. (2.44).

$$V^\pi(s) = \mathbb{E}_{\tau \sim \pi} \left[\sum_{t=0}^{\infty} \gamma^t \left(R(s_t, a_t, s_{t+1}) + \alpha \mathcal{H}(\pi(\cdot|s_t)) \right) \middle| s_0 = s \right] \quad (2.43)$$

$$Q^\pi(s, a) = \mathbb{E}_{\tau \sim \pi} \left[\sum_{t=0}^{\infty} \gamma^t R(s_t, a_t, s_{t+1}) + \alpha \sum_{t=1}^{\infty} \gamma^t \mathcal{H}(\pi(\cdot|s_t)) \middle| s_0 = s, a_0 = a \right] \quad (2.44)$$

From these equations is possible to derive the connection between state-value and action-value function given by eq. (2.45) and the Bellman equation given by eq. (2.46).

$$V^\pi(s) = \mathbb{E}_{a \sim \pi} [Q^\pi(s, a)] + \alpha \mathcal{H}(\pi(\cdot|s)) \quad (2.45)$$

$$\begin{aligned} Q^\pi(s, a) &= \mathbb{E}_{s' \sim P, a' \sim \pi} [R(s, a, s') + \gamma(Q^\pi(s', a') + \alpha \mathcal{H}(\pi(\cdot|s')))] \\ &= \mathbb{E}_{s' \sim P} [R(s, a, s') + \gamma V^\pi(s')] \end{aligned} \quad (2.46)$$

Learning equations

SAC algorithm learns a policy π_θ with θ parameter set and two Q-functions Q_{ϕ_1}, Q_{ϕ_2} with ϕ_1 and ϕ_2 parameter sets respectively. The state-value function is implicitly parametrised through the soft Q-function parameters thanks to eq. (2.47). In [20] a function approximator for this function was introduced, but in [21] the authors found it to be unnecessary.

$$\begin{aligned} V^\pi(s) &= \mathbb{E}_{a \sim \pi} [Q^\pi(s, a)] + \alpha \mathcal{H}(\pi(\cdot|s)) \\ &= \mathbb{E}_{a \sim \pi} [Q^\pi(s, a) - \alpha \log \pi(a|s)] \\ &\approx Q^\pi(s, \tilde{a}) - \alpha \log \pi(\tilde{a}|s), \quad \tilde{a} \sim \pi(\cdot|s). \end{aligned} \quad (2.47)$$

Learning Q Q-functions are learned by Mean Squared Bellman Error (MSBE) minimisation, using a target value network to form the Bellman backups using eq. (2.48). Equation (2.47) on the preceding page implicitly parametrise the state-value function.

$$J_Q(\phi_i) = \mathbb{E}_{(s_t, a_t) \sim \mathcal{D}} \left[\frac{1}{2} \left(Q_{\phi_i}(s_t, a_t) - \left(r(s_t, a_t) + \gamma \mathbb{E}_{s_{t+1} \sim p} V_{\phi_i^-}(s_{t+1}) \right) \right)^2 \right] \quad (2.48)$$

The update shown makes use of target soft Q-function with parameters ϕ_i , which are calculated, like in the DDPG algorithm, as an exponentially moving average of the soft Q-function parameters [45]. It can be optimised using stochastic gradients.

Learning the Policy It is possible to derive SAC starting from the definition of soft policy iteration demonstrated in [21, Section 4]. In particular, the policy has to be learned starting from the minimisation of the expected KL-divergence [34, 35] and exploiting eq. (2.49).

$$J_\pi(\theta) = \mathbb{E}_{s_t \sim \mathcal{D}} [\mathbb{E}_{a_t \sim \pi_\theta} [\alpha \log \pi_\theta(a_t | s_t) - Q_\phi(s_t, a_t)]] \quad (2.49)$$

As [21] reports, there are several options for the minimisation of $J_\pi(\theta)$, but the most straightforward one using neural network as function approximator is to apply the *reparametrisation trick*. It works reparametrising the policy using a neural network transformation following eq. (2.50) where ϵ_t in a noise vector sampled from some fixed distribution.

$$a_t = f_\theta(\epsilon_t; s_t) \quad (2.50)$$

Therefore, it is possible to rewrite the expectation over actions in eq. (2.49) into an expectation over noise as in eq. (2.51).

$$J_\pi(\theta) = \mathbb{E}_{s_t \sim \mathcal{D}, \epsilon_t \sim \mathcal{N}} [\alpha \log \pi_\theta(f_\theta(\epsilon_t; s_t) | s_t) - Q_\phi(s_t, f_\theta(\epsilon_t; s_t))] \quad (2.51)$$

To get the policy loss, the final step is to substitute Q_ϕ with one of our function approximators: the choice falls on $\min_{i=1,2} Q_{\phi_i}(s_t, f_\theta(\epsilon_t; s_t))$, as the authors of [21] suggest.

Exploration vs. Exploitation

SAC algorithm trains a stochastic policy using *entropy regularisation*. α is the entropy regularisation coefficient which is the parameter that explicitly controls the exploration-exploitation trade-off. A higher α corresponds to more exploration, while a lower α corresponds to more exploitation.

This parameter has a fundamental importance in the algorithm, and it may vary from environment to environment. Choosing the optimal α parameter is a non-trivial task that could require careful tuning in order to find the one which leads to the stablest and highest-reward learning. In [21, Section 5], the authors formulated a different maximum entropy reinforcement learning algorithm to overcome this problem. Forcing the entropy to a fixed value is a weak solution because the policy should be free to explore more where the optimal action is uncertain, and to exploit the learned mapping in states with a more clear optimal action. The gradients are computed using eq. (2.52)

$$J(\alpha) = \mathbb{E}_{a_t \sim \pi}[-\alpha \log \pi(a_t | s_t) - \alpha \bar{\mathcal{H}}] \quad (2.52)$$

During the test phase, the algorithm uses the mean action instead of a sample from the distribution learned. This choice tends to improve performance over the original stochastic policy, allowing to see how well the policy exploits what it has learned.

Algorithm 2.5: Soft Actor-Critic [21]

Input: Initial policy parameter θ and Q-function parameters ϕ_1, ϕ_2

- 1 Initialise target network weights $\bar{\phi}_1 \leftarrow \phi_1, \bar{\phi}_2 \leftarrow \phi_2$
- 2 Initialise an empty replay buffer \mathcal{D}
- 3 **for** $episode = 1, M$ **do**
- 4 Receive initial state $s_t \leftarrow s_1$
- 5 **repeat**
- 6 Observe state s_t and select action $a_t \sim \pi_\theta(\cdot | s_t)$
- 7 Execute a_t and obtain tuple (r_t, s_{t+1}, d_t)
- 8 Store $(s_t, a_t, r_t, s_{t+1}, d_t)$ in replay buffer \mathcal{D}
- 9 $s_t \leftarrow s_{t+1}$
- 10 **until** s_t is terminal
- 11 **end**
- 12 **if** it is time to update **then**
- 13 Sample random minibatch of N transitions $(s_t, a_t, r_t, s_{t+1}, d_t)$ from \mathcal{D}
- 14 Calculate targets
- 15 Critics Update: $\phi_i \leftarrow \phi_i - \lambda_Q \nabla_{\phi_i} J_Q(\phi_i)$, for $i \in \{1, 2\}$
- 16 Actor Update: $\theta \leftarrow \theta - \lambda_\pi \nabla_\theta J_\pi(\theta)$
- 17 Temperature Update: $\alpha \leftarrow \alpha - \lambda \nabla_\alpha J(\alpha)$
- 18 Soft Critics Update: $\bar{\phi}_i \leftarrow \tau \phi_i + (1 - \tau) \bar{\phi}_i$, for $i \in \{1, 2\}$
- 19 **end**

Output: Optimised policy parameter θ and Q-function parameters ϕ_1, ϕ_2

Hyperparameters

Entropy regularisation parameter The only parameter of this section is α . It can be set as constant through all the training, or it can be learned thanks to the approach described in [21]. Further details in section 2.2.5 on page 36.

Replay buffer See section 2.2.4 on page 32.

Neural Network See section 2.2.4 on page 32.

Learning Update See section 2.2.4 on page 32.

2.3 Related work

A truly inspiring work for this thesis is [30] where the authors show, probably for the first time, that deep reinforcement learning is a viable approach to autonomous driving. Nowadays, most approaches focus on formal logic which determines driving behaviour using annotated 3D geometric maps: the external mapping infrastructure intuitively makes this approach limited to the models and the representation of the surroundings. This technique is not able to scale up efficiently because of last-mentioned strong dependencies.

The fundamental concept underlying [30] to make autonomous driving systems a ubiquitous technology is the design of a system which can drive relying - just like humans - on a comprehensive understanding of the immediate environment [2]. [49] is useful to motivate the research in this direction because it represents an example of autonomous vehicle navigation exploiting GPS for coarse localisation and LIDAR to understand the local scene instead of detailed prior maps. Many sensors have been developed through the years to gather information and observations increasingly sophisticated. However, the major problem is the massive budget needed to afford all these technologies. The extraordinary results obtained by [30] are not based on intelligent sensing techniques, but on the usage of a monocular camera image together with vehicle speed and steering angle. They decided to apply the model-free approach of reinforcement learning because it is exceptionally general and useful to solve tasks that are complex to model correctly. As discussed previously in this chapter, model-based algorithms tend to be more data-efficient than model-free ones; however, the quality of the adopted model limits the results [9].

The authors decided to exploit Deep Deterministic Policy Gradient (DDPG) [41]. Firstly, they developed a 3D driving simulator using Unreal Engine 4 to tune reinforcement learning hyperparameters such as learning rates and number of gradient steps to take after each training episode. Then, they tried to apply

the DDPG algorithm in the real world using the parameters learnt. They also did some experiments using a compressed state representation provided by a Variational Autoencoder [32, 55]. The excellent results obtained in [30] have been exceeded by the same authors in [76] that shows astonishing performances driving on narrow and crowded urban road never-seen during training.

Starting from all these outlined ideas, we decided to investigate ways and approach to autonomous driving with reinforcement learning without using simulators or prior data in order to make a step towards the so-called *reinforcement learning in the wild* [8]. The most popular and prominent achievements in reinforcement learning to date consist of experiments done using simulated environments or ones which exploit the knowledge acquired in simulated environments in real ones. The team of the DeepMind manages to develop smart agents capable of performing super-human results in numerous games and videogames such as *Go* [61, 62], while OpenAI engineers an agent capable of beating the world champion of the multi-player Dota 2 game [46, 47]. These problems are not easy to solve but have the benefit of having a training environment equal to the test one. This fact does not apply to the approach which exploits simulated experiments results in real environments.

The last-mentioned method encloses a critical caveat: the awareness that the simulator has limits. Unlike what happens in some environments where there are many similarities between the simulator and the environment – e.g. games and videogames –, in harder environments – e.g. autonomous vehicle on public roads, ads marketplaces, biology, and applications around human behaviour – is complicated to get a simulator capable of reproducing with high-fidelity the wild environment because of approximations that could mislead the learning. On the other hand, learning directly on the environment need a fast learning cycle because of the significant number of interaction with the environment and, above all, cheap or low-risk exploration cost: millions of self-driving episodes in simulator ending with a crash of the car has a small cost in respect of one episode with the same ending crash in the real world.

Despite all these problems, the introduction of reinforcement learning in future applications may revolutionise the actual learning approach, as shown in fig. 2.10 on the following page. Nowadays, deep learning is mainly focused on perception in autonomous driving and most artificial intelligence applications. Concrete decisions on what to do in specific situations are entrusted to hard-coded and human-designed rules through optimal control algorithms. Reinforcement learning aims to create a direct path from data to value to learn how to perceive data, but also how to make valuable decisions to perform a specific task. This cutting-edge approach brings out new questions like ethics that both research and industry are starting to discuss and address to understand and protect from data biases onto the algorithm behaviours.

Between the end of 2018 and the beginning of 2019, UC Berkeley and Google

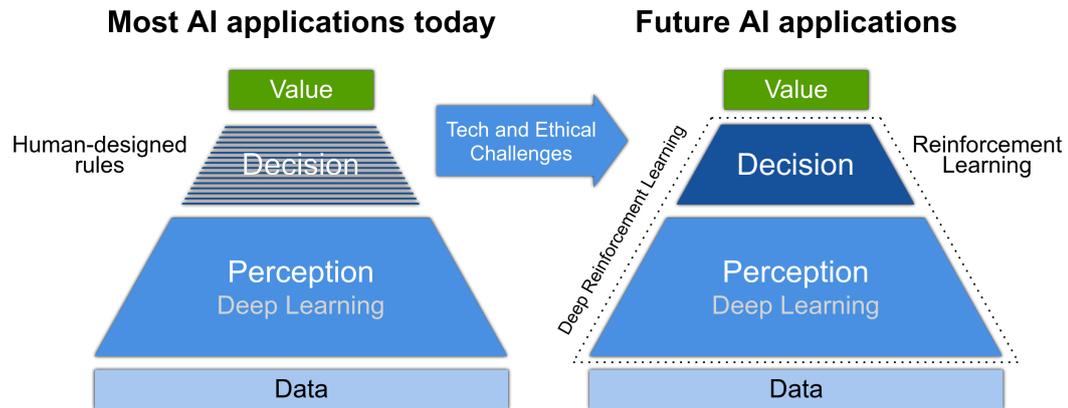


Figure 2.10. Most AI applications today exploit deep learning and machine learning for image detection and computer vision. Decisions are made by optimal control algorithms which are hard-coded and designed by humans. The reinforcement learning approach aims to inject machine learning algorithms in the decision component of the algorithm to make steps towards Artificial General Intelligence (AGI) [8].

jointly developed a state-of-the-art off-policy model-free reinforcement learning algorithm called soft actor-critic (SAC) (see section 2.2.5 on page 34). The critical goal is to provide a deep RL algorithm suitable for real-world problems and the related new challenges that they pose. They outlined the desired properties of the ideal deep reinforcement learning algorithm:

Sample Efficiency: the process of learning in the real world can be a very time-consuming task. For this reason, it is desirable a functional sample complexity to learn skills successfully.

No sensitive hyperparameters: as mentioned before, hyperparameter tuning could be a tough task to complete in real-world experiments as it could require numerous repetitions in situations where the cost in terms of time and money could be burdensome. The proposed solution of the authors is maximum entropy RL which provides a robust framework that minimises the need for hyperparameter tuning.

Off-policy learning: this learning approach allows the reuse of collected data for various tasks. This possibility helps the process of prototyping a new task when adjusting parameters or choosing a different reward function.

Soft actor-critic (SAC) represents a deep RL algorithm capable of satisfying the

previously mentioned requirements. The authors of [20, 21] revealed that the algorithm is capable of solving real-world robotic tasks in a conspicuous but acceptable number of hours, showing its robustness to hyperparameters and working on a large variety of simulated environments always using the same set of parameters. Not only it shows great performances in numerous challenging tasks compared to deep deterministic policy gradient (DDPG), twin delayed deep deterministic policy gradient (TD3) [16] and proximal policy optimisation (PPO) [58], but reveals its power by solving three tasks from scratch without relying on simulators or demonstrations [54].

The real-world robotic task involving a 3-finger dexterous robotic hand to manipulate an object similar to a sink faucet with a coloured end presented in [21, Section 7.3] shows similar concepts to the task analysed in this thesis for what concerns the framework of deep reinforcement learning exploited. The algorithm exploits raw RGB images and processes them through a convolutional neural network. The final goal of the robot is to rotate the valve into the correct position – with the coloured part pointing to the right – starting from a random position for each episode. The results obtained represents one of the most sophisticated real-world robotic manipulation tasks learned end-to-end with deep reinforcement learning, starting from raw images and without any previous simulation or pre-training phase.

Taking all arguments into account, we decided to follow [30] implementing a similar self-driving framework based on the design of a control system for a small toy robot called Anki Cozmo. Therefore, we formalised the autonomous driving learning problem as a Markov decision process to enable the application of reinforcement learning algorithms, taking into account the improvements mentioned in this section about model-free reinforcement learning algorithms applied to real-world robotic problems. Chapter 4 on page 59 provides a detailed description of the choice made and the system design. Chapter 5 on page 80 reports the experiment we carried out in the environment we designed.

Chapter 3

Tools and Frameworks

This chapter aims to describe the main tools and frameworks used to develop the project of this thesis. The first section will describe the OpenAI Gym framework, a central toolkit for developing and comparing reinforcement learning algorithms, and explain why this tool is essential for reinforcement learning research. The second part of this chapter will outline Cozmo, the powerful toy robot developed by Anki that we used as an agent in the reinforcement learning scenario to apply algorithms to try solving autonomous self-driving tasks: chapter 5 on page 80 will report the analysis and description of these experiments. This section will also report a set of available alternatives to Cozmo, explaining the motivations underlying the final choice. The description about PyTorch, an optimised tensor library for deep learning using GPUs and CPUs used to build up the convolutional neural network of this work, and the related comparison with TensorFlow will occupy the last part of this chapter.

3.1 OpenAI Gym

Nowadays, OpenAI Gym [6], released in 2016 with its public beta, is one of the most popular toolkits and frameworks in the reinforcement learning scenario. A brief analysis of reinforcement learning research could be useful to outline the motivations underlying the need for a reinforcement learning framework.

As reported previously in chapter 2 on page 5, reinforcement learning is a sub-field of machine learning dedicated to the world of decision making and motor control: researchers study how an agent can learn and improve to achieve a specific goal in a complex, usually unknown environment. This machine learning paradigm is becoming more and more attractive for both researchers and industries because of its visionary property of being very general. A reinforcement learning algorithm can be exploited to control a robot's motor in order to make it capable of running or jumping, play a videogame or a board game, make critical business decisions like

pricing and inventory management, but also learn how to invest in financial trading environments. The generality of reinforcement learning became engaging thanks to the remarkable results achieved in many challenging environments, as reported previously in chapter 2 on page 5.

Despite these appealing features, the research was slowed down by other circumstances, no less critical. The need for better benchmarks represents the first factor. As an example, the abundant availability of conspicuous datasets like *ImageNet* [10] has driven supervised learning improvement in the research. For what concerns reinforcement learning, the nearest equivalent to supervised learning datasets would be a broad collection of different environments in order to test various algorithms with different kinds of observations or rewards. The second withdraw of this approach to learning is the lack of standardisation of environments designed in publications. In reinforcement learning, subtle differences in problem definition, reward function design or action space typology could make the difficulty of the task grow. This fact threatens to slow down and corrupts experiments reproducibility making an objective comparison between the results of different papers almost impossible.

The need to fix both problems was the primary motivation behind the design and implementation of OpenAI Gym.

3.1.1 Environments

The agent and the environment represent the main components of reinforcement learning. The choice of OpenAI was to implement and provide the abstraction mainly for environments, not for agents. They decide to provide a standard environment interface instead of forcing the developer to use pre-defined agent interfaces: the motivation behind this choice was to leave developers independent in the design of the agent, the core of reinforcement learning, and facilitate the creation and usage of environments. Thanks to this approach, all agents implemented with OpenAI Gym can be used with the whole set of environments provided by the framework. Therefore, it is possible to create a personalised environment to suit the needs of a specific experiment that can be used by all agents exploiting OpenAI Gym environment interfaces.

In this scenario, we realised the first contribution to our thesis. Thanks to this framework features, we implemented an OpenAI Gym environment capable of interacting with Anki Cozmo by providing a binding between functions of Cozmo SDK and interfaces of the reinforcement learning framework. In chapter 4 on page 59 we will provide further information and details about our contribution.

The importance related to the high quantity of environment is fundamental to build a reliable and sustainable framework for reinforcement learning algorithms. For this reason, OpenAI Gym contains a various and heterogeneous environment database, ready to be used.

Interface functions

Exploring OpenAI Gym, it is essential to focus on the most crucial interface functions that the agent will exploit to interact with the environment. The functions which constitute the skeleton of an OpenAI Gym environment are the following:

- `def step(self, action)`: through this function, the agent can communicate the action it wants to take. The input data depends on the type and number of variables in the actions space (e.g. discrete or continuous). As will be discussed in section 3.1.2 on the following page, the values returned by this function represent the environment state after the manipulation caused by the agent action. Thanks to these data, the agent will be able to select the next action following the reinforcement learning loop.
- `def reset(self)`: during the episode, internal variables of the environment changes, influenced by the action taken previously. This function allows the agent to restart the initial situation of the environment. This procedure is particularly helpful when an episode finishes and the agent has to restart the next learning episode in a brand new copy of the environment.
- `def render(self, mode='human', close=False)`: this function is mainly used in simulated environments. It enables the visual render (if available) of the environment.
- `def close(self)`: the final function to close the environment after the end of all experiments and episodes.

Available environments

To date, OpenAI Gym includes the following environments:

- **Algorithms**: learning to imitate computations, such as copying or reversing symbols from the input tape, is the main aim of this typology. These environments might seem easy to be solved by a computer, but it is essential to remember that the objective here is to learn to solve these tasks purely from examples. Therefore, it is possible to vary the sequence length to increase or decrease task difficulties quickly.
- **Atari**: *Atari 2600* is a home video game console developed in 1977 which spread the use of general-purpose CPUs into gaming with game code distributed through cartridges. This environment section provides a database which contains more than 100 environments emulating Atari 2600 videogames. OpenAI Gym exploits *Arcade Learning Environment (ALE)* [3] providing RAW pixel images or RAM as observation of the environment.

- **Box2D**: in this group is possible to find some continuous control tasks in a simple 2D simulator such as *BipedalWalker*, *CarRacing* and *LunarLander*
- **Classic Control**: this class provides a set of problem borrowed by control theory and widely exploited in the classic reinforcement learning literature. Some task examples are balancing a pole on a cart or swing up a pendulum.
- **MuJoCo**: this collection contains continuous control tasks running in a fast physics three-dimensional simulator called *MuJoCo* which stands for *Multi-Joint dynamics with Contact*. This physics engine aims to facilitate research and development in robotics, biomechanics, graphics and animation. The simulator is particularly suitable for model-based optimisation allowing to scale up computationally-intensive techniques. Thanks to its features, it became useful as a source for reinforcement learning algorithms. [68]
- **Robotics**: OpenAI released this algorithm typology to provide eight robotics environments with manipulation tasks significantly more complicated than the MoJoCo ones. It contains *Fetch*, a robotic arm to move and grab objects, and *ShadowHand*, a robotic hand to manipulate and grab pens, cubes and balls. [51]

3.1.2 Observations

As previously reported, the `step(self, action)` environment interface is the most important one because it contains the behaviour definition of the environment that reacts to agent actions. Indeed, the agent has to know in which way its actions are influencing the environment in order to stop doing random actions and start making valuable decisions.

In order to provide this type of information to the agents, the `step` function returns four relevant values that reinforcement learning algorithms can exploit to determine the best action to do in the future. These values are:

- **observation (object)**: a specific object which represents the environment observation and shows the changes provoked by agent actions. Its structure and interpretation depend on the implementation of the specific environment. For example, it could represent the raw pixel data from a camera, the status of a board game or physics data of a robot (joint angles and velocities).
- **reward (float)**: this is the fuel of the reinforcement learning algorithms. This value represents the reward achieved thanks to the action taken by the agent. The reward for each action can change among environments, but this is the crucial information to enable the agent to learn.

- **done (boolean)**: this value is a simple boolean that signals the agent when the episode ended and it is time to reset the environment to start a brand new episode.
- **info (dict)**: a Python dictionary to monitor and show diagnostic information useful for debugging. The agent could use it as additional information in the learning process, but the documentation of OpenAI Gym does not recommend to use this data in the learning process to maintain the coherence with the reinforcement learning loop.

The last important thing to report about the OpenAI Gym framework is the definition of **Spaces**. As reported in the second chapter, an environment consists of the action space and the observation space. Both can provide discrete or continuous values: this distinction is fundamental to determine the usage of a specific algorithm rather than others to solve a given task better. For this reason, OpenAI Gym provides **Discrete** and **Box** to initialise discrete and continuous spaces, respectively. It allows the user to define a lot of features useful in the learning process, such as a maximum and minimum value setup or a default function to sample a random value from the defined space instantly.

3.2 Anki Cozmo



Figure 3.1. On the left there is a photo of Anki Cozmo in action, while on the right side there is a graphical reconstruction of the whole set of gears and hardware inside the robot.

Especially in the latest decades, human beings have started a complicated relationship with robots. They are very fascinated by the prospect of artificial intelligence offered by recent researches and applications. However, they are apprehensive and worried at the same time because of the apocalyptic plot that many sci-fi films

show and the significant promise of automation, capable of replacing human workers in the future. However, all these concerns disappear after meeting Cozmo, the palm-sized toy robot developed by the San Francisco-based company Anki and available on the market since 2016. On first glance, Cozmo might appear as one of the cutest toy robots: not surprisingly Anki employed the guidance of Carlos Baena, the former Pixar animator, to design this robot. Therefore, it can interact with people using a small display screen together with audio effects to mimic human emotional reactions and responses. The result is a toy robot WALL-E-inspired both aesthetically and personality-wise, powered up by artificial intelligence to move and discover the surrounding environment. Thanks to the built-in camera, Cozmo can remember faces and recite names, but also to plan paths and play various games with its three cubes that carry sensors and lighting.

Despite these entertaining, but not so technical facts, Cozmo hides a lot of powerful features under the hood. Anki developers produced a high-quality Python SDK that allows developers to take control of the whole set of Cozmo sensors and actuators thanks to the interaction granularity offered by functions and interfaces. This section aims to outline the hardware and software architecture hidden underneath the cute Cozmo bodyworks, together with a comparison with the alternatives available to design the reinforcement learning system of this thesis. An essential inspiration in the writing of this section came from [7], [69] and Anki Forums ¹.

3.2.1 Cozmo architecture

It is possible to define Cozmo as a vision-guided mobile manipulator, one of the first consumer robot which can boast vision among its features. However, as reported before, the features it shows during the normal toy usage, do not equal the number of interfaces and functions made available to developers. The hardware and the software developed for Cozmo makes it the right choice to fast prototyping computer science projects: it is the main reason why we decided to exploit Anki Cozmo instead of other alternatives. The SDK provided by Anki consists of a comprehensive set of low- and high-level functions which grants full access to sensor data providing the right flexibility, simplicity and granularity to satisfy every developer needs. It is versatile because it could be easily connected with hundreds of third-party libraries to augment Cozmo capabilities. Therefore, it is an entirely open-source SDK to give the community the freedom to customise and contribute.

Figures 3.2 and 3.3 on the next page and on page 50 shows technologies, the hardware and software involved in the production of Cozmo. The first image represents stacks and connections between the robot core and the mobile application

¹Anki Cozmo SDK Forums: <https://forums.anki.com/>

provided by Anki, while the second one shows the interaction between the last-mentioned application and the Python user program on the development machine. The reader can retrieve a global perspective about the whole Cozmo architecture by merging these two figures.

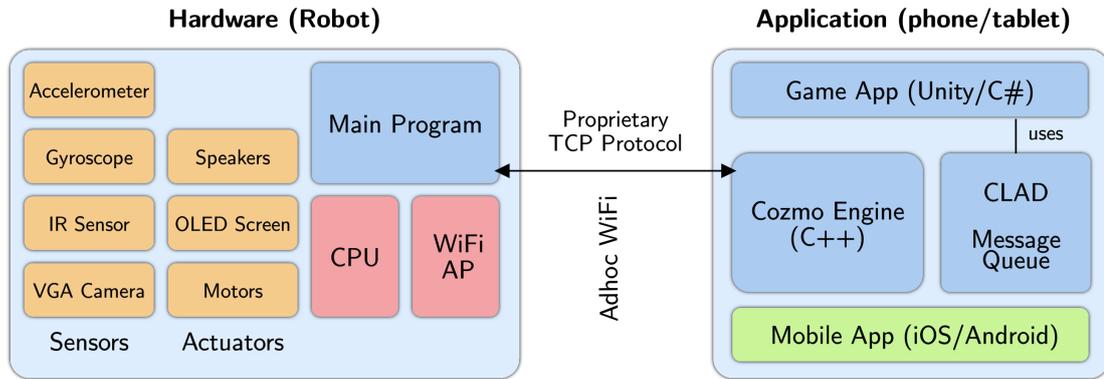


Figure 3.2. Interaction between the Robot and the mobile application stack. The main program of the robot interacts with the Cozmo Engine (C++) implemented in the mobile application through a proprietary TCP protocol established using an ad-hoc WiFi connection. [7]

Analysing fig. 3.2, it is noticeable that Cozmo has a lot of sensors and actuators, which enable it to move and understand the surrounding environment. For what concerns the sensor part, the VGA Camera is the crucial component exploited in the thesis. This camera provides a grayscale image with 320×240 . Anki reported a camera resolution equal to 640×480 , but the latest firmware version supports only the lower resolution. Furthermore, the camera can detect and acquire colours, but the firmware limits this feature to maintain the bandwidth stable and avoid overloads or slowdowns in the communication with the mobile application and subsequently, the user program running on the computer. The camera has approximately 60° field of view (FoV) and 290mm focal length.

As regards the actuators column, Cozmo can explore the world thanks to its four motors and over fifty gears. Instead of having wheels, this robot has two tracks to navigate: it can steer and move freely by controlling the speed of each track. Another moving part is the head that can move up or down to direct the camera and the display. It also has a forklift with which it can lift objects or the cubes available in the kit.

Cozmo can perform one single action at a time: if the current action is not yet complete and the request of a new action occurs, the new action fails with a *tracks locked* failure code. For this reason, the SDK does not allow the execution of multiple actions. Despite this fact, it is easy to notice that Cozmo animations

and behaviours typically use combinations of actions: indeed the user can send simultaneous actions to the robot by calling them using `in_parallel=True` in its script, but these actions have to belong to a different action track. This approach allows the parallel execution of actions, provided that they use different tracks. Cozmo software architecture holds seven independent action tracks:

- **HEAD**: raise/lower robot head.
- **LIFT**: raise/lower robot forklift.
- **BODY**: wheels or treads actions for driving and turning.
- **FACE_IMAGE**: actions with the OLED display such as animations or faces.
- **EVENT**: for this action type Anki does not release further information.
- **BACKPACK_LIGHTS**: actions or animations of lights on Cozmo back.
- **AUDIO**: speech or sound effects emitted by the robot.

The project of this thesis mainly exploited the body action track to move the robot in the environment: it also employed head and lift tracks, but only to position the robot head to provide images about the track to the main program and the reinforcement learning agent. The usage of parallel operations was not necessary.

The Cozmo hardware includes an on-board CPU and a WiFi access point, thanks to which the user can interact with the robot. However, to activate this communication, it is necessary to install the Cozmo Android/iOS application on a personal tablet or smartphone. This application is the same used to play with the toy-side of Cozmo, but in its settings, there is a function to enable Cozmo development mode. After connecting the chosen personal device to the robot through a simple WiFi connection, the application manages to create a proprietary TCP protocol to interact directly with the main robot program. The creators of Cozmo developed this mobile application using C++ to implement the *Cozmo Engine*, the component which shall be responsible for the TCP communication with the robot. To design and implement the game experience and the graphical user interface, they used Unity and C#.

This last-mentioned part utilises the component internally designed and implemented by Anki to provide a contact point between the Cozmo SDK installed in the development machine, as shown in fig. 3.3 on the following page: the C-like Abstract Data language (CLAD). The fundamental idea behind this tool is to make the process of serialisation, communication and deserialisation of data structures written in Python easier for the developer. In practice, for every data which has to pass over the wire, files with extension `.clad` to define enums, structures and

messages are generated: their syntax is similar to C struct one. After that phase, this tool auto-generates Python, C++ and C# code for each structure previously defined. This process allows the user to define a specific message in Python and to send it to the C++ engine where it will be deserialised automatically, avoiding problems and sources of bugs coming from intricate underlying details.

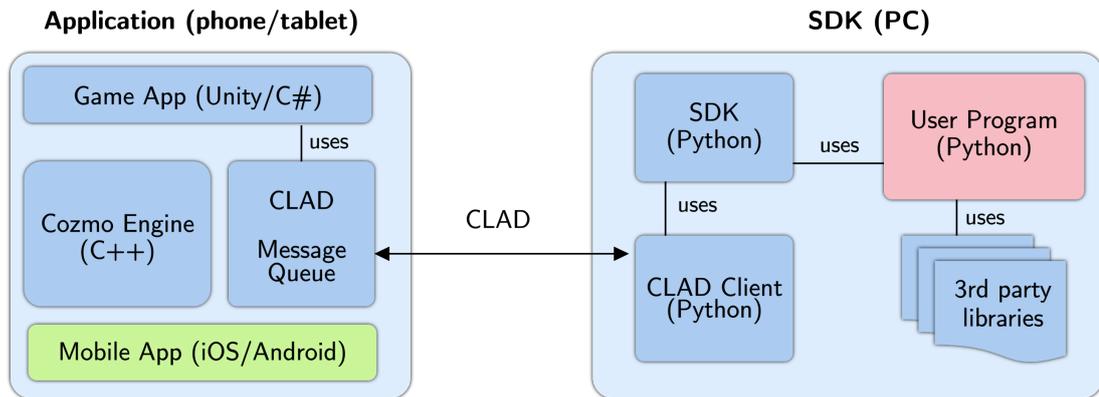


Figure 3.3. Interaction between the mobile application stack and the Python user program. Anki designed a C-like Abstract Data Language (CLAD) to implement the connection between the Cozmo SDK and the Cozmo Engine on the mobile application. This approach puts a decoupling layer between Python interfaces and low-level functions to make prototyping easier and fast-forwarding for developers. [7]

This approach results in a process method much lighter than the one provided by *Protocol Buffers (Protobuf)* by Google: even then, the main aim of this implementation choice was reducing the network bandwidth. Taking all arguments into account, CLAD is the protocol used for the interaction between the SDK and the C++ Engine that allows the developer to not care about the low-level part of the code and to focus on the high-level logic using Python. It is also useful to maintain the same interface for the user even if low-level logic changes occur.

In this case, the CLAD communication messages exploit a wired connection between the mobile device and the computer with a simple USB cable. In this thesis, we used an Android tablet to run the experiments, and for this reason, we used the *Android Debug Bridge (ADB)* to make this exchange possible. It is a command-line tool included in the *Android SDK Platform-Tools* package that allows the communication between the computer and Android devices. It facilitates many device actions such as installing, debugging apps or running a variety of commands on a device. It is a client-server program that consists of three components: it includes a *client* hosted in the development machine, a *daemon (adb)* which runs the commands on the device as a background process and finally a *server*, a background

process in the development machine that manages the communication between the two previous components.

The last step to start programming with Cozmo SDK is to install it in a development machine following the instruction provided by its documentation ².

3.2.2 Why Cozmo?

Before starting the development of this thesis project, we spent some time analysing the small car market situation in order to find out the right choice for our specific needs. In addition to Anki Cozmo, the ideal alternatives in the self-driving scenario when we started this thesis were *AWS DeepRacer Vehicle* and a customised vehicle implemented from scratch exploiting *Donkey @Car library*.

This section part aims to briefly describe the main alternatives to Anki Cozmo listing strengths and weaknesses for each approach to motivate the final choice made.

AWS DeepRacer

AWS DeepRacer is a platform developed by Amazon to learn and refine machine learning, reinforcement learning algorithms and techniques on AWS DeepRacer vehicle.

The whole ecosystem consists of two main part:

- **AWS DeepRacer Car.** It is a 1/18 scale race car developed and built to test reinforcement learning algorithms on a real track. It aims to show how the reinforcement learning model trained in a simulated environment can be conveyed to the real-world by using cameras to view the track and the model to control throttle and steering. It has a lot of impressive specifications under the hood such as Intel Atom[®] Processor, 4GB of RAM, an expandable 32GB of storage to accommodate the trained model and a 4-megapixel camera with MJPEG.
- **AWS DeepRacer Simulator.** The user can build his models in *Amazon SageMaker* and train, test and iterate the learning process using the racing simulator. It offers an integrated environment hosted on the AWS cloud to experiment and optimise algorithms to apply to the autonomous driving model.

There are many advantages in using the DeepRacer stack. It offers an integrated approach where the developer has to focus just on reinforcement learning: indeed, it abstracts a significant part of the software giving the developer the chance to

²Cozmo SDK Documentation: <http://cozmosdk.anki.com/docs/>

work almost exclusively on the model. It has a growing development community to confront ideas and find solutions through challenging competitions around the world. One of the fundamental aims behind this product is to build up a regulated environment where amateurs and researchers can compare and tests different approaches in solving the autonomous driving task. Therefore it provides a high-performance car where to store the trained model in order to make it independent to the training environment.

On the other hand, one of the main disadvantages of this approach is that it is an Amazon lock-in: the framework provided force developer to use the whole Amazon stack. This fact can be inconvenient economically-wise because of the rates of the Amazon platform that adds to the price of the car, but, above all, because Amazon may have access to all developer implementations and experiments.

Another not negligible factor was the product release date: Amazon had to release it in July, but, to date, it is not yet available in Italy. Therefore, because of this thesis is focused on the application of reinforcement learning algorithms directly in the real world without the aid of simulators and model, the absence of the physical car was crucial for the final decision.

Another important withdraw consists of the strict correlation between the simulator and the real system: the framework provided by Amazon seems to be suitable only to test reinforcement learning algorithms after the model training in the simulator, but not for the sake of this thesis.

Donkey@Car

The second important alternative to Cozmo was to develop a small car from scratch using integrated boards such as *RaspberryPi* or *NVIDIA Jetson Nano*, sensors and camera to personalise the device and satisfy specific project needs. *Donkey@Car*³ is the most popular choice to build a personal self driving toy car. It is an open-source community project powered by volunteers who are interested in build their own self-driving cars. They cooperated to build up a high-level self-driving library written in Python, focusing on enabling fast experimentation and contribution. They provide detailed instructions to build a personal Donkey vehicle, providing kits or lists of components to use: the whole kit costs among 250-300\$.

It is also possible to install the Donkey library on any RC car to make it self-driving and autonomous. Despite this fact, Donkey developers suggest building the *Donkey2* car, which is a tested hardware and software setup, to avoid problems such as incompatibilities or bugs and make the most out of the presence of a dense community.

³Donkey Car community website: <https://www.donkeycar.com>

The main strength of this choice is the freedom to develop a completely customised car to suit better the needs and requirements of a great set of autonomous driving projects. In the last releases of the library, Donkey developers released a complete sandbox simulator for training a self-driving car. The languages used to develop it are Unity for simulation and Python with Keras and Tensorflow for training. They also provide an OpenAI Gym environment to use with such simulator.

The main weakness of this method consists in the process of building a self-driving car system from scratch. It offers versatility and flexibility in components choice, but the time to devote to building a working system, free from as many bugs as possible would have slowed down the prototyping of the system itself and the whole thesis project. The duration of development is not associated with the process of physically assembling the car because Donkey developers estimate two hours to build the car. The real obstacle consists of the setup of a connection similar to the Cozmo one: it needs to be as stable as possible to make all stack working smoothly in real-time.

The final choice

As easily predictable, the final choice fell on Anki Cozmo. It provides a fast-forwarding SDK ready to be exploited in prototyping a brand new project together with the strictly necessary sensors to perform the reinforcement learning experiments in the real world. A crucial factor in reaching the final decision was the dimension of the car: Donkey and Amazon DeepRacer are 1/10 and 1/18 scale race cars respectively, while Cozmo is just 5.5cm wide, which results in a ratio of about 1/30. This fact not only makes Cozmo an easily transportable solution to speed up experiments and to restart episodes effortlessly but also a solution that supports the design of a track in a restrict space such as the one in the laboratory of Eurecom.

Therefore, the connection between the development machine and the robot is suitable for implementing an OpenAI Gym environment, and it is similar, at least in the premises, to the distributed off-board computation approach. The main algorithm, the neural network, the reinforcement learning framework and the other cognitive parts are computed and managed by the workstation, instead of being stored in the vehicle as happens in Amazon DeepRacer and Donkey car approaches.

Taking into account the perspective of autonomous cars in the real world, on-board and off-board computation approaches are still under research. With the on-board method, cars have much computational hardware inside in order to manage every aspect of autonomous driving by themselves, but it requires more powerful batteries to counterbalance energy consumption. On the other hand, the connection to off-board computer facilities or the clouds leads to new vectors of attack but also enables companies to monitor the behaviour of the vehicle fleet to identify malicious activities early. To date, both approaches are still under research, and

it is not possible to decree a legitimate winner. For what concerns the thesis, the designed system emulates an off-board approach.

In the end, Cozmo provides plain and straightforward control of the car, a rich Python SDK to use with OpenAI Gym, and it is the best trade-off between functionalities and fast-developing.

3.3 PyTorch

PyTorch ⁴ [50] is an open-source machine learning and deep learning library developed by Facebook's AI Research Lab and released to the public in October 2016. The main aim of PyTorch is to provide an intuitive and straightforward framework to develop artificial intelligence projects: two of the main applications to date are computer vision and natural language processing.

The programming languages utilised to develop PyTorch were Python, C++ and CUDA, the parallel computing and API model created by Nvidia to allow software developers and engineers to use CUDA-enabled GPU for general purpose processing. The primary interface provided by the library to the user employs Python, the project where Facebook developers mainly put their efforts. Despite this fact, it also offers a C++ interface.

PyTorch consists of the following components:

- **torch**: PyTorch Tensor library with strong GPU support. It implements interfaces similar to those of the NumPy library. It contains data structures for multi-dimensional tensors and mathematical operations, providing many utilities for efficient serialising tensors and arbitrary types.
- **torch.autograd**: the tape-based automatic differentiation library that supports every differentiable operation on tensors available in **torch**.
- **torch.jit**: this component is a compilation stack that uses TorchScript to create serializable and optimizable models from PyTorch code. This tool allows the user to train models in PyTorch using Python and then export the model in a production environment where Python may be disadvantageous for performance and multi-threading reasons.
- **torch.nn**: this component provides a neural networks library that is entirely compatible with **autograd** and designed for flexibility.
- **torch.multiprocessing**: this component is based on the Python multiprocessing library, but it implements memory sharing of torch tensors across processes.

⁴PyTorch Github Repository: <https://github.com/pytorch/pytorch>

- **torch.utils**: it contains many utility functions to better exploits the features of PyTorch.

PyTorch provides a NumPy-like experience to interact and manipulate data structures suitable for GPU computation, offering a deep learning research platform which can provide flexibility and speed. These data structures are called *Tensors* and they can be used both on the CPU and the GPU, accelerating the computation thanks to the whole set of functions and manipulators explicitly designed for every scientific computation need.

PyTorch is not a straightforward binding to an underlying complex C++ framework. The library design focused on establishing Python as the main priority, and for this reason, the user experience is very natural and similar to other important machine learning libraries already present in the package manager.

It is noticeable that PyTorch developers aimed to create an intuitive and linear product to use. To follow this idea, they decided to make PyTorch synchronous to permit the debugger to receive and understand messages and stack traces promptly. This feature translates in a better debugging experience for the end-user.

Beyond these features, one of the traits that distinguish PyTorch from other frameworks is its single way to build neural networks by using a tape-based automatic differentiation. The majority of deep learning frameworks available in the market, such as TensorFlow, Theano or Caffe, exploits a static approach in structure computation graph creation: they reuse the same layout in the whole program, therefore changing a simple component triggers the regeneration of the graph from scratch. PyTorch utilises an entirely different approach which is not unique to PyTorch, but it provides one of the fastest implementations: they call it *Tape-Based Autograd*. This term refers to the reverse-mode automatic differentiation exploited in the framework, which is a technique based on the properties of the chain rule: to calculate the derivative of an output variable w.r.t. any intermediate or input variable, the only requirement is to know the derivatives of its parents and the formula to calculate derivative of primitive expression. The main improvement that this approach brings is allowing the user to change the network structure on-the-fly without lag or overhead.

3.3.1 TensorboardX

One of the most crucial means that every machine learning researchers need is a tool to visualise and measure data efficiently: this fact is significant because we need to measure in order to improve models, projects and results. However, one of the main problem in PyTorch is the absence of such a tool, specifically designed for the Facebook framework. It can always use powerful tools such as *Matplotlib*, but it offers a synchronous approach that leads to slow down the main program since the primary process has to wait for the data rendering before starting next operations.

On the other hand, TensorFlow, the most important deep learning alternative to PyTorch developed by Google, provides in its package TensorBoard which is a webserver to serve visualisation of the training progress of the neural network. It can show to the user scalar values, images or text, and it is particularly useful to visualise experimental metrics such as loss and accuracy. The particularity of this tool consists in the fact that it stores these typologies of information asynchronously as events. The Python script calls specific functions to store information and goes on with the next operation without waiting for its render: that is possible thanks to the decoupling level inserted by this approach between the visualisation and the creation of data. Indeed, Tensorboard operates by opening and reading TensorFlow events files that contain the summary data generated during experiments. Therefore, it will be the webserver to take care of elaborate data for rendering without bothering the current Python script.

Fortunately, PyTorch can exploit the features of Tensorboard thanks to a library called *TensorboardX*⁵ that stands for *Tensorboard for X* to highlight developers aim to make Tensorboard available for all deep learning framework.

3.3.2 Comparison with TensorFlow

After the advent of deep learning, many companies decided to put their efforts to design architectures and frameworks to vehiculate this new technology. The two most popular frameworks in this research field are TensorFlow [1] by Google released in 2015 and PyTorch [50] by Facebook released in 2017.

Implementing the same neural network in these two frameworks will lead to different results because of the training process has many parameters that depend on the underlying technologies provided by the specific framework. For instance, the training process in PyTorch is enhanced by CUDA GPU usage, while TensorFlow can access to GPU through its GPU acceleration. The choice between these two frameworks is not straightforward because it depends on the perspective and the needs of the specific projects to develop. For this reason, this section aims to outline differences between these two libraries without aiming to decree the best one but to motivate the decision we made using PyTorch.

Dynamic versus Static

The first difference concerns the construction of the computational graph. A computational graph is an abstraction useful to represent the computation process through a direct graph.

In TensorFlow, computational graphs are defined statically, before running the code. The main advantage of this method is allowing parallelism and dependency

⁵TensorBoardX documentation: <https://tensorboardx.readthedocs.io/>

driving scheduling, features that boost the learning and make it more efficient. This framework communicates with the external world via specific tensors that will be substituted by input data at runtime. Only with TensorFlow 2.0, Google decided to implement dynamic computational graph in its product, but its stable version was released after the start of this thesis.

As mentioned above, PyTorch approach to computational graphs is dynamic. This characteristic means that the graph is built incrementally at runtime without using particular data structures as placeholders. This feature supports projects where the author needs to change the computational graph on-the-fly avoiding the application restart. In this sense, PyTorch is more pythonic than TensorFlow [36].

Distributed training

Another key feature is the distributed training and data parallelism. PyTorch offers native support for asynchronous execution from Python, and then it could improve performances. On the other hand, TensorFlow needs more efforts to allow distributed training: the developer must fine-tune every computation to make it running on a specific device. Both frameworks offer the same opportunities in these terms. However, TensorFlow needs more effort to make things work.

Visualisation

As discussed in the previous section, TensorFlow exploits TensorBoard to provide all tools that machine learning researcher needs to visualise learning and keep track of the training process. Facebook researchers developed *Visdom* for this purpose, but it provides very minimalistic and limited features compared to the ones offered by TensorBoard. As reported before, it is possible to use TensorBoard with PyTorch thanks to the library TensorBoardX.

Production deployment

For what concerns the deployment of trained models into production, TensorFlow offers the best service via *TensorFlow serving*, a framework that offers and uses REST Client API. The production deployment in PyTorch improved from its early releases, but, currently, it does not provide a framework to deploy the trained models on the web: the developers must use Flask or Django as backend server to provide the right environment to exploit the model.

Conclusions

Considering all the points explained in this section, we decided to utilise PyTorch for this project, but it is noticeable that there is no winner in this comparison.

Both frameworks have strengths and weaknesses that depends on the specific applications where we would use them. TensorFlow is a mature and robust tool, notably suggested for production and AI-related products. Although it needs some time to get the developer used to its programming approach and, at least at the start of this thesis project, it supports only static computational graph methods. On the other side, PyTorch is an efficient and young framework with a large community and which provides dynamic computational graphs and is more Python friendly. Therefore, it is especially recommended for research-oriented developers.

Chapter 4

Design of the control system

In the previous chapters, we outlined deep reinforcement learning fundamentals with its most critical underlying concepts, and then we discussed the choice made about the technologies to use as baselines for our experiments. The decision fell on Anki Cozmo because of the high-quality SDK provided to developers, its dimension and its features, while for what concerns the deep learning framework we opted for the versatility and flexibility provided by PyTorch, particularly suitable for a research context.

The following step in the path of this thesis consists of merging reinforcement learning theory with tools and frameworks presented previously to create the system in question. Indeed, this chapter aims to describe the design of the control system for reinforcement learning experiments with Anki Cozmo. The work presented in this part represents one of the contributions of our thesis and the necessary step towards reinforcement learning experiments.

The outline of the whole ecosystem with the description of interfaces, frameworks and technologies used occupies the first section of the chapter. This part also comprehends the description about the implementation of the OpenAI Gym environment to make reinforcement learning algorithms interact with Cozmo, emphasising its differences from a typical simulated environment: we will start from the problem formalisation as Markov Decision Process (MDP) to conclude with the implementation of human-robot interaction.

We already presented the theory underlying DDPG [41] and SAC [20, 21] algorithms in sections 2.2.4 and 2.2.5 on page 30 and on page 34 respectively. For this reason, the second section consists of a discussion about the specificities of reinforcement learning implementations we built with references to the choice we made in terms of hyper-parameters and neural network design in a real-world application. In the final section of this chapter, we will present some relevant problems we faced in the design and setup of the real-world track together with the decision we made to overcome them.

4.1 Outline of the system

The development of the control system for Anki Cozmo was the main contribution of the thesis, together with the experiments carried on with the robot in the real world. The main aim of this work was to create an OpenAI Gym environment capable of interacting with a robot in the real world without any interaction, fine-tuning or prior knowledge obtained through the use of a simulator. OpenAI Gym usually provides plain and straightforward interfaces to interact with simulated environments: we decided to exploit these functions to allow the application of reinforcement learning algorithm directly in the real-world decision of the robot.

The fundamental source of inspiration to develop this control system was [29, 30]. This publication represents, as its authors reported, the first reinforcement learning self-driving experiment where a car learned to drive through the application of a reinforcement learning algorithm, by trial and error. They first trained the model exploiting Deep Deterministic Policy Gradient (DDPG) in a simulator for many epochs to find the most suitable hyper-parameters to use. After this simulated learning process, they started their experiments in the real world using the set of parameters obtained from preceding experiments. Unfortunately, the authors did not describe in details the fine-tuning process in the simulation and did not provide the results of these experiments in order to allow a weighted comparison with the real-world experiment. They revealed only a table with a report of the best performance for each model. This fact, accompanied by the challenging prerogatives of this type of experimentation, was the propulsive thrust that led us to attempt to implement a similar reinforcement learning configuration without any prior help from simulations.

We decided to export and implement these ideas in our project, adapting them to the specificities and particularities of the Cozmo setup. Figure 4.1 on the next page summarises the resulting system providing a schematic overview of every technology employed and interactions among them. This section aims to describe as clearly as possible all the components of the control system we designed.

4.1.1 OpenAI Gym Cozmo environment

Before starting the description of the system we designed to carry out reinforcement learning experiments it is necessary to outline the decisions we made about what to implement in *CozmoDriver*, the OpenAI Gym environment we developed to apply, train and test reinforcement learning algorithms with Cozmo.

The path of this section will follow the steps of a typical formalisation of the Markov Decision Process (MDP), bringing out the problems encountered, the reasoning behind them and solutions proposed as they go.

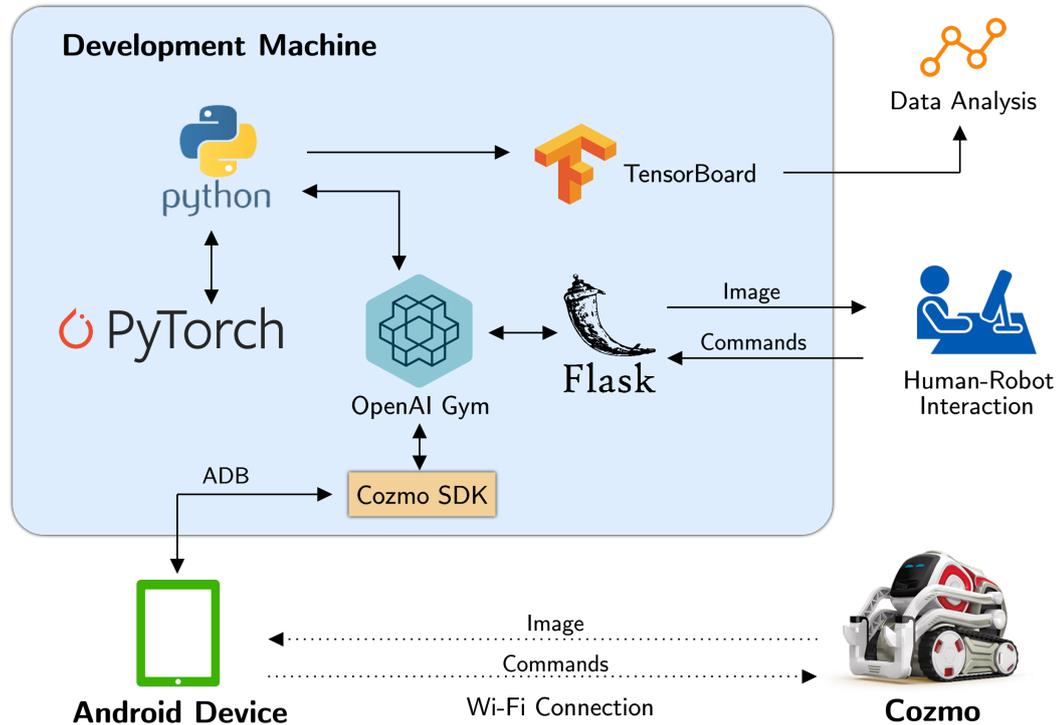


Figure 4.1. The interaction between the user and Anki Cozmo has a crucial role in this system. The main Python script utilises OpenAI Gym for the reinforcement learning component and PyTorch for the deep learning one. The user can interact with the flow of the system through a simple web app that uses OpenAI Gym and the Cozmo SDK directly to provide information for the user (e.g. images, learning information) and the robot (e.g. commands). The last component consists of TensorBoard thanks to which the script can store results that can be retrieved later by the user.

Markov Decision Process formalisation

Starting from the definition of MDP that we already reported in eq. (2.4) on page 8, we studied and investigated the best configuration to provide an acceptable trade-off between performance and memory consumption, capable of making the system work on the development machine we used for our experiments. In the following paragraphs, we will analyse each MDP aspects paying particular attention to the problems we faced and the motivations behind every decision made to overcome them.

State/Observation space The environment observation is the group of information that the reinforcement learning agent can see and obtain from the interaction

with the real world. Current autonomous driving technology usually works thanks to the presence of various sensor positioned in different points of the car body as we discussed in section 2.3 on page 38. However, this approach is quite different from what human beings use to guide every day: the only input that the human receives is what he sees. Taking this fact into account, in the self-driving tasks in question, we thought that the most reasonable way to obtain knowledge about the surrounding environment as similar as possible to how humans do was to exploit front camera images provided by Cozmo SDK. However, it is essential to remember that, by definition, the state must satisfy the Markov property. According to this definition, *the state must be independent of the past given the present*. For this reason, using a single image to describe the current state may be an oversimplification of the problem. Even a human would not be able to determine the best action to take starting from a single frame. That is because it is difficult to infer or determine the current direction of the car, speed or steering wheel position. Merely adding another image can intuitively improve the human perception of the scene: as an example, the first intuition this introduction could reveal is where the car is going, allowing the user to decide more accurately about the trajectory to follow.

To verify this fact before starting the experiments with the application of the reinforcement learning algorithms to Cozmo, we firstly analysed the results of some experiments on the environment of the classic control problem of trying to keep a frictionless pendulum standing up (*Pendulum-v0*). The original version of this environment utilises angle position and trigonometric results as observation to return to the agent. However, this environment offers to the user the access to the images provided by the OpenAI Gym `render` interface. It represents an entirely different kind of experiment from Cozmo driving task, but they have in common the improvement in trajectory inference brought by the presence of a number of pictures higher than one. In order to make this environment suitable for convolutional neural networks, we decided to appropriately modify it to exploit raw images as observations instead of the original information. Therefore, we noticed that the usage of a single picture as observation led to unstable and worse results than the ones obtained by combining two subsequential images to feed the algorithm. For this reason, we decided to use two consecutive raw images provided by Cozmo by using a queue data structure with size two. In the code flow, the developer merely has to push the next image obtained from the robot and use the specific queue function implemented to obtain the concatenation of the last two images, only when necessary.

Therefore, we decided to reduce the original size of the input Cozmo image to 64×64 . We made this decision as a trade-off between performance, learning phase duration and space available in the central memory to store the replay memory.

In conclusion, the observation provided to the agent is the concatenation of two grayscale images with dimension 64×64 pixels.

Action Space Another essential part that we needed to formalise is the action space, how the agent can interact and influence the surrounding environment. In the car scenario, the two main components of driving are the speed of the vehicle and the position of the steering wheel. To straightforwardly formalise these two parts, we decided to use two simple real values.

We chose to define the desired speed value in a range of 0 to 1, while we opted for a range of -1 to 1 for the steering wheel position. These limits allow the agent to manipulate simple values in the decision-making process and to facilitate the manipulation of neural network results. At the same time, the underlying logic of the environment takes care to translate these values into a compatible format for the Cozmo SDK. Indeed, as reported in section 4.1.2 on page 65, the Cozmo SDK function exploited to manoeuvre the robot needs at least the speed of each tread. Algorithm 4.1 reports key steps of this translation. Therefore we decided to raise acceleration parameters by setting them equal to 4 times the velocity of each thread to reach the desired speed as fast as possible.

Algorithm 4.1: CozmoDriver actions conversion from virtual to real

Input: Desired speed $s_t \in \{x \in \mathbb{R} | 0 \leq x \leq 1\}$
 Steering wheel position $w_t \in \{x \in \mathbb{R} | -1 \leq x \leq 1\}$
 Maximum forward speed $s_{\max}^{\text{forward}} = 150\text{mm/s}$
 Maximum turning speed $s_{\max}^{\text{turning}} = 100\text{mm/s}$

- 1 Left tread speed: $ts_{\text{left}} = s_t \cdot s_{\max}^{\text{forward}} + w_t \cdot s_{\max}^{\text{turning}}$
- 2 Right tread speed: $ts_{\text{right}} = s_t \cdot s_{\max}^{\text{forward}} - w_t \cdot s_{\max}^{\text{turning}}$

Output: Left tread speed ts_{left}
 Right tread speed: ts_{right}

Reward Function The reward function is the crucial feature to define in the formalisation of the MDP. After a review of the available literature and the analysis of the problem, we obtained a list of ideas and concepts to model the reward function:

- **Lane Distance:** this model calculates the reward of each action by calculating the distance between the car and the centre of the lane. The main aim is to prioritise the correct positioning of the car on the lane, crucial for driving safety. However, it is noticeable that this value can be easily calculated in a simulated environment, while it needs a lot of sensors and calculations to obtain a good estimation in a real-world environment. Beyond this problem, this approach has difficulties in scaling to varying environments where road typology and dimension is not a pre-configured constant. Therefore, it is a limited approach because human beings do not always drive the car in the

perfect centre of the lane: for instance, when approaching a curve, it could be more convenient to move the car slightly away from the perfect centre.

This fact reveals the shortcomings of this approach: the system can perform only as good as the human intuition underlying the hand-crafted lane reward.

- **Distance Covered:** the second approach we investigated was the one suggested by [29, 30], where the reward of a specific action consists of the total distance covered by the car for each specific action taken. Approaching the problems with this method leads to results that can be easily understandable for humans: indeed, the total reward of each episode represents the total distance travelled by the robot.

In the car scenario of the previously mentioned publication, it is possible to use the car odometry device to quickly retrieve this value after each action and calculate the reward of a specific decision obtaining the difference with the previous value. Cozmo does not have such kind of sensor on board. Therefore it is necessary to calculate this value manually. The intuition behind a reasonable estimation of the distance covered by Cozmo consists of using the fundamental formula of kinematics: the speed. Indeed, in the designed system, we have direct access to the aspired speed because it is a parameter that the agents decide at each iteration, and it is possible to derive the time elapsed between one action and its following one by manually calculating them inside the OpenAI Gym environment.

- **Speed Crash Penalty:** the third typology of reward we investigated consists of a sort of life bonus reward. The robot receives a reward (e.g. 1 point) for each timestep of correct decisions and a negative reward (e.g. -10 points) every time the user stops the robot preventing the crash. Therefore we added to the positive reward a small quantity that depends on the current speed to encourage the robot to stay on track and increase its speed. Consequently, we decided to add a penalty in faulty time step proportional to the robot crash speed to entice the robot in avoiding high speed when close to critical points. Equation (4.1) formalises the reward used in this approach: p_1 and p_2 are two parameters that determine how much the speed influence the reward and their module must be much less than the constant value in the equation to highlight the fact that they represent a secondary objective [52].

$$r_t = \begin{cases} +1 + p_1 \cdot s_t, & \text{if Cozmo on the track} \\ -10 - p_2 \cdot s_t, & \text{if Cozmo off the track} \end{cases} \quad (4.1)$$

After the analysis of these three reward design proposal, we decided to select the second one to pursue our experiments in the real world. As previously reported, the first option would have been hard to carry on and to scale up. The third option

hints intriguing facts that a reinforcement learning agent could take into account to better solve the driving task of our experiments. The only withdrawal of this approach is related to the correlation between reward and distance covered: this correspondence is significant for the developer to have a more transparent overview of what is happening and how the algorithm is learning, at least in the early stages of development. In the second option, the distance covered by the robot is equal to the reward, while this conformity is lacking in the third option. For this reason, we decided to take the second reward proposal for this time. We noticed that it could be an exciting future development trying to merge the second alternative with the third one to obtain a brand new reward function that both penalises bad decisions proportionally to speed and maintain its correspondence with the track crossed.

4.1.2 Human-Robot interaction

It is noticeable that the simulator can undoubtedly be programmed to understand whenever the car is going outside the track, crossing the roadside. In a reinforcement learning scenario, this fact facilitates the restarting procedure for an episode: the developer has to bind some events or actions to a process that stops the current episode, put the car on the road again and starts the next experiment. In the real world, the situation is more complicated not only because of the need of the human intervention to relocate the car in a safe place but also because there are more variables to take into account. The most critical factor is that the failure of an episode in the simulator has no threats or costs, while real-world experiments failures could lead to high costs and severe damage to the car and equipment. Despite this point, the application of such experiment typology in a real environment instead of a mere simulation represents an exciting challenge that could bring reinforcement learning to the next level. In order to make experiments as safe as possible, the authors of [29, 30] implemented a self-driving system designed explicitly for self-driving reinforcement learning experiments where the car driver has the faculty of stopping the car when it is going to run off the road or in a dangerous situation and relocating it in the nearest safe position to start the next learning episode. By simply pressing a button, the logic of the car disables reinforcement learning algorithm decisions and gives full control to the real driver of the car.

We aimed to implement this kind of user-robot interaction also in our setup. The requirements were almost the same as the ones described in the paper, but this case could not rely on steering wheel, brakes and accelerator as in the car scenario where they are directly accessible by the user. The system needed an interface to allow the developer to stop the robot whenever it is approaching the side of the road and manoeuvre the robot just like a car. For this reason, we firstly implemented a straightforward interface using a web app implemented using



Figure 4.2. This image shows the web application we implemented to control Cozmo during reinforcement learning experiments. The focus is on the first two columns of the application since they provide the essential tools. The first one is entirely dedicated to the list of key the user can use to drive the robot or control the reinforcement learning algorithm flow. The second column consists of the live image coming from Cozmo front camera and some information about the current state of the RL system.

plain HTML5, CSS3 and Javascript for the frontend and Flask ¹, a lightweight Web Server Gateway Interface (WSGI) web application framework, as backend. Therefore, we designed the web-app interface by using the Bootstrap framework ² to offer an easy-understandable and appealing user experience. A screenshot of the

¹Flask Github Repository: <https://github.com/pallets/flask>

²Bootstrap documentation: <https://getbootstrap.com/>

dashboard is available in fig. 4.2 on the previous page.

The aim of this application is allowing user interaction with Cozmo and Flask represented the right choice to allow the communication between this interface and the OpenAI Gym environment. The Flask backend interacts directly with the functions offered by Cozmo SDK to allow the user to see the live streaming from Cozmo camera directly in the web app. Therefore it can receive, convert and forward commands from the robot to the SDK. These commands consist of the pressure of both single or combination of buttons: Flask decides the action to trigger programmatically with hard-coded conditions and calculates speeds and accelerations of both right and left treads.

The SDK function we utilised to control Cozmo is `drive_wheels()`. The parameters of this function are the following:

- **l_wheel_speed** (*float*): mandatory parameter that specifies the speed of the left tread (in millimeters per second).
- **r_wheel_speed** (*float*): mandatory parameter that specifies the speed of the right tread (in millimeters per second).
- **l_wheel_acc** (*float*): optional parameter that specifies the acceleration of the left tread (in millimeters per second squared). The default value is the equal to `l_wheel_speed`.
- **r_wheel_acc** (*float*): optional parameter that specifies the acceleration of the right tread (in millimeters per second squared). The default value is the equal to `r_wheel_speed`.
- **duration** (*float*): it specifies the duration of the driving action of the robot. It calls `stop_all_motors()` after this duration has passed. The default value is `None`. In this case, the behaviour of this function is equivalent to the non-async `drive_wheel_motors()` one: the wheels will continue to move at that speed until commanded to drive at a new speed.

This method is the same we used to implement the OpenAI Gym environment, allowing the algorithm to interact with the robot just like a human in the driving seat. Just as examples, the user can start and stop the episode using the enter button, forget the previous episode with backspace and relocate the robot on the track using W, A, S and D buttons.

4.1.3 System flow

The implementation of an algorithm flow to sustain the specific experimental need was necessary due to the continuous interactions between the human and the robot.

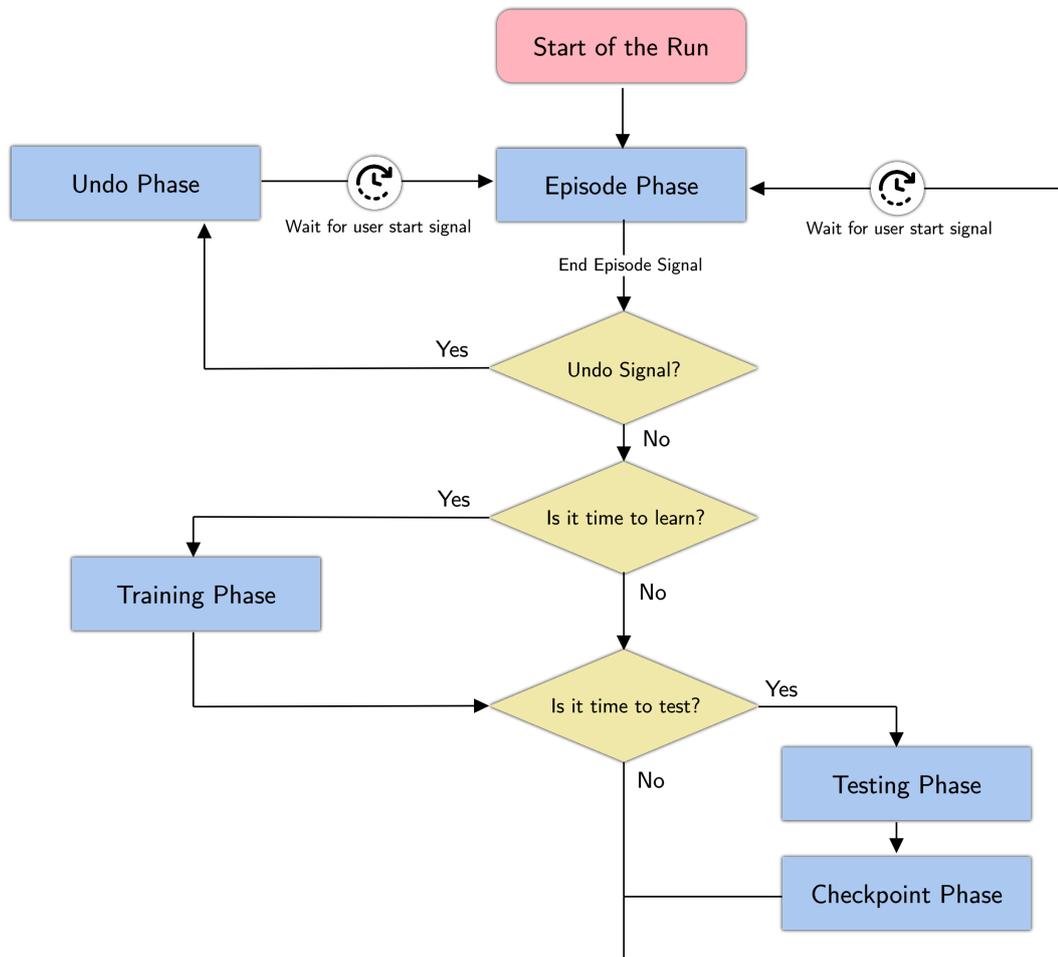


Figure 4.3. This image shows the flow chart of the system we implemented. The most crucial phases are highlighted in blue. This chart is deliberately drawn without an end, because, although there was the possibility, we never set a fixed maximum limit of experiments in Cozmo scenario. It is possible to retrieve the warm-up procedure by answering no to the last two decision branch.

Starting from the ideas of [29, 30], we decided to divide the learning process in a series of phases highlighted in blue in fig. 4.3.

The phases we defined are the following:

- **Episode phase.** This phase consists of a single episode take. It represents the results of a series of action taken from the agent to solve the task. In the early part of the experiment, the algorithm has to perform a warm-up, a procedure where the agent makes random actions to explore the environment randomly and obtains an initial set of entries for experience replay memory.

After the agent gathered the minimum amount of entries, which is usually equal to the batch size or a multiple thereof, the agent starts to exploit the neural network to act using a noisy policy for exploration purpose. This last-mentioned part is still an episode phase, but testing or checkpoint phase never follows it. As reported in section 4.3.1 on page 75, the time between two subsequent actions is a parameter we set according to limitations of Cozmo SDK to avoid problems in the learning process.

The user is the main responsible for this phase. It can interact by toggling enter button on the keyboard. The first hit starts the episode, while the second one determines the end of the episode and attributes zero rewards to the last action taken.

- **Undo phase.** As described in section 4.3.3 on page 76, it is possible to invalidate experiments due to a human or a system error. For this reason, we implemented a procedure that the user can trigger to delete the knowledge acquired in the last training episode and restore the previous state. We positioned it right after the episode phase to delete faulty episodes as soon as possible.

In this case, the user has two possibilities to undo the last episode. The user can either hit the backspace button in substitution of the second enter button hit to stop the episode and start the undo phase or pressing it after the end of the episode and before the next one. Initially, the first choice led to a direct restore of the previous situation without executing the training phase, while the second one executed the training phase and only afterwards the undo phase. After some tests, we decided to set the first behaviour as unique for both possibilities. This choice led to a delay increase between two consecutive episodes because of the addition of an indirect confirmation of the current episode before starting the training phase. However, thanks to the careful design of the network, the waiting time remained manageable.

- **Training phase.** This section starts its execution after the initial warm-up phase, and it is located after each Cozmo episode. It manages all neural networks updates with several optimisation steps, also known as epochs: the number of optimisation steps is set as a parameter by the developer.
- **Testing phase.** This phase disables noisy policies from the algorithm to allow the agent to take the action that the neural network decree as best in that specific iteration. It consists of a repetition of a finite set of episodes that triggers after every specified number of epochs, given as parameter of the system: the average reward calculated by the rewards obtained from each testing episode is the result of this phase. This value is crucial for the reinforcement learning experiments because we used them to build the

average reward performance graph that shows how much the agent learned in the graphs of chapter 5 on page 80 and determines the quality of the learning process itself.

- **Checkpoint phase.** This phase is described in section 4.3.3 on page 76. It consists of saving all data to make the developer able to restart the experiment from the last available checkpoint. It is usually located right after the testing phase in order to save all values together with network weights and biases.

The user can also trigger this phase manually by toggling the C button before starting the next episode by hitting the enter button. It allows to virtually pause experiments, like the one with Cozmo, that could last tens of hours, and that can need multiple days to complete.

4.2 Algorithm setup

Another crucial step in the design of the system is the setup of reinforcement learning algorithms we exploited. This thesis aims to show results and challenges of the implementation of SAC algorithm to solve a real-world driving task, so it is essential to include in this document ideas and implemented choices we used to develop our system.

Given the fervour that has led to an impressive development of reinforcement learning in recent years, numerous repositories were born to be able to offer ready-made implementations of these algorithms in order to speed up the implementation process in the most suitable experiments. Nowadays, the most famous and exploited reinforcement learning repository available for developers is *OpenAI Baselines*³ which provides a set of high-quality implementations of reinforcement learning algorithms realised using *Tensorflow* deep learning library. In addition to this last-mentioned project, there are many new forks of this project which offers improvements, refactorings or additional implementations of the latest algorithms offered by the continuous scientific research in this field.

Despite this fact, we decided to implement our versions of reinforcement learning algorithms from scratch taking the last-mentioned implementations as guidelines to follow in the developing process instead of exploiting them directly. We chose to follow this workflow primarily for didactical reasons. Implementing an algorithm from scratch, starting from the theory provided by the related paper escorted by the numerous implementations available is probably the best way to understand the whole set of ideas underlying algorithms properly. Furthermore, we made this decision to have the opportunity to manage and implement architectural choices to

³OpenAI Baselines Github Repository: <https://github.com/openai/baselines>

create a suitable workflow for the episodes carried out in Cozmo experiments that could be compatible with the human-robot interaction of Cozmo.

This section contains the choices we made in the design of the neural network and a reflection about the selections made for the hyper-parameters of reinforcement learning algorithms.

4.2.1 Neural networks design

Another essential component in the developing of the control system is the convolutional neural network we designed. As already reported in chapter 3, we opted using PyTorch as deep learning framework. To choose the neural network that could better meet the requirements, we analysed the models used in [41, 29, 20, 21].

The author in [41] presented two types of neural networks, but the model we are interested in is the convolutional one, used to learn from pixels. It consists of 3 convolutional layers without pooling with 32 filters at each layer. Therefore, the authors added two fully connected layers with 200 units. The paper also contains information about the initialisation of network weights and biases: they set final layer ones from a uniform distribution of $[-3 \times 10^{-3}, 3 \times 10^{-3}]$ and $[-3 \times 10^{-4}, 3 \times 10^{-4}]$ respectively in order to ensure the initial outputs for the policy and value estimates were near zero. They used uniform distributions $[\frac{-1}{f^{0.5}}, \frac{1}{f^{0.5}}]$ where f is the layer fan-in. The actions were concatenated just before fully connected layers.

In [29], the authors used a convolutional neural network with four convolutional layers, with 3×3 kernels, a stride of 2 and 16 feature dimensions, shared between the actor and critic models. Therefore, the flattened encoded state obtained from convolutional operations were used as input for fully connected layers of both actor and critic: in the last case, it was concatenated with the actions. In this architecture, there was only a single fully-connected layer of 8 features. They conducted the experiments using a modified Renault Twizy vehicle with a single forward-facing video camera situated in the centre of the roof at the front of the car, carrying out their experiments on-board using a single NVIDIA Drive PX2. They managed to solve their self-driving task in a handful of trials using 250 optimisation steps with a batch size of 64. They managed to make the experiment very manageable with an optimisation phase that took approximatively 25 seconds, which is a reasonable amount of time considering that the driver must reposition the car at the centre of the lane before restarting the procedure. As stated in the paper, their agent was able to cover a distance of about 300 metres in 37 minutes of training time within just 35 episodes. In the real world, the environment is much more complicated than the simulated one, and then they decided to implement the logic of the agent through the usage of a Variational Autoencoder (VAE). This decision led to an improvement in the reliability of the algorithm.

In [21], the authors reported the training of a real-world robotic task with a 3-finger dexterous robotic hand. The objective of the agent is to position a sink faucet

in a specific position highlighted by a coloured end. The neural network exploited on this occasion consisted of two convolutional layers with four 3×3 filters and max-pool layers, followed by two fully connected layers with 256 units. Even in this case, the authors exploited RGB images to carry out real-world training of the agent. Therefore, they included some information about training time: the agent needed 300k environment interaction steps with an equivalent of 20 hours of training.

The problems just outlined have relative differences, but the varying durations of the experiments are truly impressive. This fact underlines how the training duration depends not only on the data quality but also on hyper-parameters used, on the complexity of the problem and the available computational power. It is the primary motivation behind the elaborateness of an experiment carried out entirely in the real-world.

After the analysis of the neural network used in the last-mentioned papers, we tried to modify these models after testing them on a modified version of the *Pendulum-v0* environment, provided by the OpenAI Gym framework, with a variety of architectures. We exploited the network architectures that passed this selection to made experiments with *Pendulum-v0* and, consequently, with the environment we designed with Cozmo. Chapter 5 on page 80 will show the results in question.

However, before finding a good architecture to exploit, we started little experiments with Cozmo to analyse changes in the behaviour policy of the robot. There we noticed a crucial factor to take into account to decide what network to use for our experiment: the optimisation phase duration. It is a vital parameter to make the experiment manageable for the user: in this thesis work, the agent is not in a simulation where the computer automatically decides when to restart the episode so that the human can let the experiment running by itself. In this context, the user must be ready to stop, reposition and restart the car at any moment. Given the evidence that an experiment like this could last thousands of episodes, we aimed to reduce the waiting time for the user to make the experiments last less, or, at least, obtain a good relationship between the duration of the episode and that of the optimisation steps. To avoid a long waiting time after each episode, we tried to spread the optimisation phase inserting a single learning step after each action taken by the agent. We found out this approach in some implementation of DDPG algorithm mainly applied to simulated environments. This choice seemed working with the *Pendulum-v0* task because, in a simulated context, the environment stops itself waiting for the next action taken by the agent during the optimisation phase: the system flow is independent of the duration of the last-mentioned phase. It is noticeable that this fact does not apply to a real-world scenario like the one we implemented with Cozmo. As discussed in section 4.3.1 on page 75, the robot continues to drive even during the learning process. Therefore the system is highly unstable because this process not always has the same length and every action lasts differently: it depends on the specific network topology. After the analysis of this

behaviour, we decided to maintain the optimisation phase among episodes and to fix a specific duration for each action of Cozmo.

The architecture we selected was a sort of merge of the ones we found in [29, 30, 21]. We opted for a neural network with three convolutional layers with 16 filters of 3×3 dimension. We decided to use a stride of 2 instead of using pooling layers with a stride of 1, following ideas of the authors of [29, 30]. This decision aims to shorten the optimisation phase and obtain more manageable experiments without impacting performance excessively [64]. We applied batch normalisation after each convolutional level to improve the speed, performance, and stability of neural networks [27]. Finally, we flattened the results and used them as input for the last part of the architecture, which consists of two fully-connected layers with a hidden size of 256 features. We decided to implement the network using the Rectified Linear Unit function (ReLU) as non-linearity, to initialise all network biases to 0 and all weights using Xavier initialisation [17].

In the Q-Network implementation, the outputs of the convolutional section were concatenated with actions, and there is one single output value after the fully-connected part, which represents the value of the action-value function Q . In the policy scenario, as shown in fig. 4.4 on the next page, there is no concatenation at the end of the convolutional layers stack, and the output size depends on the dimensionality of the specific action space which, in the Cozmo scenario, is equal to 2.

4.2.2 Algorithms implementations and hyperparameters

As already mentioned in this section, the experiments we made in this thesis were carried out in a real-world environment. At the beginning of this thesis work, we implemented the DDPG algorithm following the theory of the related paper and the hyperparameters suggested in [41, 29, 30]. This process was carried out in parallel with the implementation of the same algorithms for a simulated environment offered by the OpenAI Gym framework, *Pendulum-v0*. This decision was useful to check the correctness of the architectural decisions we made step by step. Despite this fact, the learning context of Cozmo showed its complexity since the first experiments bringing out differences from *Pendulum-v0* environment. We found out that, in order to obtain results that could show as clearly as possible whether the algorithm is working and improving with the selected set of parameters, it was necessary to wait for a large number of epochs corresponding to tens of hours or few days depending on the neural network architecture and the hyper-parameters.

Furthermore, these experiments can not exploit the advantages of the simulated environment in which the researcher can set the parameter ranges at the beginning, leaving the computer to start and complete the search for each combination of the available parameters. The real-world approach we described in this chapter needs the constant presence of a human to carry out the learning process, and the whole

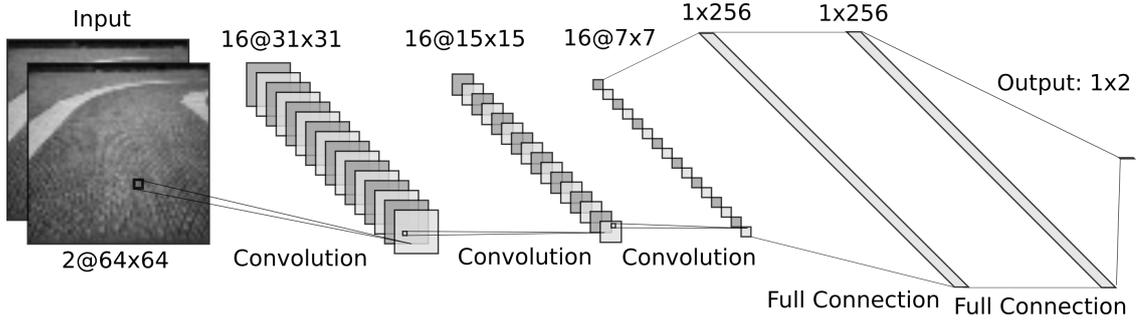


Figure 4.4. Convolutional Neural Network Architecture for Cozmo experiments. This particular example shows the model exploited as the Policy with a tensor with dimension equal to the action space size as output and two consecutive grayscale images which represents the state of the environment as input. The first part of the network consists of three convolutional layers with 16 filters of 3×3 dimensions. Each level is supplemented by a batch normalisation one. The results are then flattened and concatenated with the vector of actions before entering the second part. This section consists of two fully-connected layers with 256 features. The output of this particular network represent the action to take, given the input state. This network uses ReLu as non-linearity. Before starting experiments, the network is initialised with biases equal to zero and weights set utilising Xavier initialisation [17].

procedure is further slowed down by the Cozmo battery lifetime and its charging time: both take about 30 minutes. It is noticeable that, in a real-world scenario like this, it is almost impossible to make a humanly manageable workflow capable of doing a sustainable grid search. For this reason, we decided to initialise these parameters following the guidelines provided by the DDPG paper. The results, in this case, were not as good as we expected: the robot showed no tangible progress even after numerous episodes. The policy learned led to strange behaviour with sharp turns in a direction and episodes that ended almost immediately.

After this implementation, we started a search for a reinforcement learning algorithm more suitable for real-world problems. The ideal objective would be to find a hyperparameter agnostic algorithm capable of performing well regardless of algorithm configuration and ensuring the absence of unfairness introduced from external sources [24]. The last-mentioned aim is still being researched today by the scientific community. Despite this fact, we found out an algorithm capable of automatically adapt itself to reduce the hyper-parameter dependency: SAC, an algorithm which was born precisely as an evolution of the DDPG approach to improve its performance in real-world applications and overcome hyper-parameters dependencies. Therefore, we also implemented this algorithm from scratch by using the implementation of the so-called *parameter auto-tuning* proposed in [20, 21].

Chapters 5 and 6 on page 80 and on page 104 will present the performance comparison between these two algorithms in a *Pendulum-v0* simulated environment and the performance of SAC in the real-world Cozmo one.

4.3 Real-World experiments

The real-world nature of the approach we followed in the work of this thesis revealed more questions and problem than the corresponding simulated environment. This fact happens because executing a self-driving task in the real world is meaningfully more challenging. There are plenty of factors that inevitably emerge, and that can not be monitored and audited appropriately if not after making a large number of attempts.

This section aims to describe the most crucial and interesting problems we faced in the development of this control system together with a debate on possible countermeasures.

4.3.1 Actions duration

In the first implementation of the environment, the agent was able to make decisions without a specific timing between actions. This fact led to different problems in the implementation of reinforcement learning agents. The first problem was related to experience memory gathering also caused by the limitation of Cozmo Camera: it is a 30fps camera but, as reported in the documentation of Cozmo SDK, the Cozmo framework emits a new camera image generally up to 15 times per second. Therefore, the frequency of image requests was very high because the system did not contain timing implementation constraints in the control of operations. These two factors led the system to retrieve the same image both before and after taking the current action.

Consequently, the state of each environment step consisted of the concatenation of two images that were often the same picture. This consequence led to a conceptual error that may influence the process of learning if we observe that with a human perspective: a state of this kind represents an action that does not impact the environment of the system while it is modifying it.

We noticed this problem because, in the first part of the experiments, where the agent takes random action to explore the surrounding environment, the robot continued to drive a straight path, even if shaky, without taking a definite step in a specific direction and with an almost constant speed. This symptom was strictly related to the robot's inability to have the right time to carry out a specific action before interacting with the environment with the next one. Accordingly, the robot ends up navigating with an average speed close to the half of the maximum speed and always going in a straight line only with small and temporary slopes to the right

or left. After noting this problem, we fixed it by hard-coding a minimum interval between the execution of a specific action and the beginning of the next one in the OpenAI Gym environment: we selected this value according to the constraint given by the Cozmo SDK about robot camera device.

4.3.2 Driving bias

As we reported in section 4.1.2 on page 65, the user has to interact with the robot to indicate how valuable is the last action taken by the robot agent. It is noticeable that, in this context, human-robot interaction has a crucial role in the learning process. As the sole source of information for the algorithm, it is responsible for all improvements and imperfections of learning process results: the robot learns which actions are valuable and which are unprofitable or disadvantageous, but it is essential to remember that the human is the one who decides the correctness of each action by stopping the car in a dangerous situation. This fact inevitably leads to the introduction of unconscious bias in the algorithm that could affect final results.

It emerged after many episodes, where the robot started to learn how to steer near a curve: sometimes the robot managed to make the curve correctly, without going out of the road line, other times it was able to steer with a tread slightly out of the track, then continuing to drive correctly in the next straight section. Since the reinforcement learning agent uses the reward received and the stack of images that represent the previous and next state in order to understand the value of a given action, the algorithm considers the last-mentioned approaches to the curve equally valuable. From a human perspective, imperfectly executing a curve can still be considered correct, but the risk is that experiences of this type may influence the experience replay memory and then the learning process in the long term. This factor is accentuated by the fact that, as the algorithm improves, borderline cases of this type tend to increase more and more, and the user is more and more inclined to accept them.

However subjective the error may be, we have always tried in our experiments to be as severe as possible in accepting episodes to the limit of acceptability. We will discuss the experiments and their results thoroughly in chapters 5 and 6 on page 80 and on page 104.

4.3.3 Error management

Despite the care taken in the design of the reinforcement learning system covered by this chapter, many factors sometimes invalidated the experiments launched. Just to cite a few of them as an example, we can report the instability in the Cozmo connection with its SDK caused by cable failure or the discharge of the robot battery in the middle of an experiment without any warning signal.

These events can also be added to those caused directly by the distraction of the user who guides the learning process: sometimes it happened that the user sent the episode end signal when the error was already made and over. The agent had already started to insert wrong and off-road experiences in the replay memory, invalidating the experiment carried out up to that moment.

To try to solve the problem, we have implemented two types of rescue systems. The first is a volatile backup system for every single episode that is discarded after the start of the next one. Once the episode has ended, if the user believes that it has not been carried out correctly or a factor has occurred that risks compromising the entire learning process, there is the possibility to restore the previous state of the episode and start the process again from that point.

We implemented the second type of rescue as soon as the experiments proved to last longer than expected. Because the experiments could take many hours or even days, it was necessary to implement a checkpoint system to save the state of the experiment and to restore it in the following days. We decided to insert this process at the end of the periodic test phase: it serialises and stores in the secondary memory storage the values of the neural network and the data of the reinforcement learning algorithm.

4.3.4 Track design

In order to carry out real-world experiments with Cozmo, we need to build a track specifically designed for robot dimensions. For this reason, we spent some time to search for the most reliable way to build a path where to train Cozmo efficiently.

Firstly, we opted for an easily transportable track to allow various attempt with different locations and environmental conditions that could affect the training phase. Furthermore, we noticed that the presence of reflections might influence the learning process, then it was necessary to use a material to use as terrain for the track that was less reflective as possible to avoid such kind of problems. The first choice was the black floor of the Data Science laboratory of Eurecom. It was useful only during the initial design and development of the control system to build small pieces of track in which testing functionalities. This solution had numerous drawbacks such as the impracticality to transport and high light reflection.

After this first try, we analysed different solution to design the track. The following list provides a brief report of the various solutions taken into account during the thesis, together with a brief analysis of advantages and drawbacks.

- *Covering fabric*: this material is easily transportable, but it has a high light reflection, and its structure is prone to make wrinkles and dunes particularly challenging to remove.
- *Tar paper*: this solution slightly diminished the reflection problem compared



Figure 4.5. Picture from above of the track we designed and build to carry out experiments with Anki Cozmo robot. The route is a mixed track that includes two straights, a narrow hairpin and a wide one that, united by a curve elbow, make up a serpentine. The track length is about 3 metres.

to the previous choice, but the material was fragile and with the same drawbacks of the covering fabric.

- *Cotton fabric*: this solution offers an easily transportable material with reduced light reflection where it is easy to remove wrinkles and dunes.

Summing up, it is noticeable that the cotton fabric provides the right trade-off among all requirements reported before.

Another crucial factor was the dimension of the lane, which must reproduce an environment similar to real driving. We opted for analysing the ratio of the size of a vehicle to the width of a road. In our study, we utilised the width of a typical family car and utilised the average width of a typical Italian motorway for the lane dimension: we found out a value of about 160-170cm for the first one and between 275cm and 375cm for the second one. Therefore, we measured the Cozmo width that was about 5.5cm for a resulting ratio of $\frac{1}{30}$. Accordingly, the scaled lane width obtained was between 9cm and 12.5cm. The other component to take into account was the material to use to draw the lane. In this case, we used a simple paper tape of width equal to 2.5cm. Because of the narrow and limited angle of vision provided

by Cozmo camera, we opted for a total width of about 10cm: the size of the road changes slightly throughout the path emulating what can happen in a hypothetical real road. Therefore, we chose this dimension because positioning the tape with a distance greater than 10cm would result in a significant part of the tape outside the view of the camera. A track picture is available in fig. 4.5 on the previous page.

Chapter 5

Experimental results

In the previous chapters, we described the reinforcement learning control system we designed, together with an analysis of the solutions we proposed for the problems we faced during the development process. Indeed, this process has not been free from difficulties, both of implementation level and parameter optimisation. After completing the design of this architecture, our second goal was to look for an algorithm that could better adapt to a real context, exceeding the limits set by DDPG in hyper-parameter tuning. The ideal would have been to find a parameter agnostic algorithm: an enabling feature to achieve excellent performance regardless of the specific configuration and hyper-parameter selection. During our research, we came across the SAC algorithm and, after a careful analysis of the paper and having understood the considerations made by the authors about SAC real-world applications, we thought it might be the right choice to get better performance than the DDPG experiments. For this reason, this chapter aims to present a detailed comparison between DDPG and SAC experiments carried out with *Pendulum-v0* environment and show the performance achieved by SAC with the experiments with Cozmo.

The first section of this chapter focuses on the experimental methodology. It will be an opportunity to describe the hardware of the development machine we used for the experiments and present in a more schematic and precise way the OpenAI Gym environments on which we will apply the algorithms. We speak in the plural, because we have decided to report both the experiments performed on *Pendulum-v0* environment, and those carried out with Anki Cozmo in the real world using the architecture we built. This part will also contain a brief analysis of how reinforcement learning experiments are assessed to date. For this segment, we took inspiration by [24], an exciting publication where the authors investigated reproducibility challenges, proper experimental techniques, and reporting procedures of modern deep reinforcement learning to draw up guidelines from which to start in order to obtain better reports, not so much from the result perspective, but from how they are reported.

The second and third sections of this chapter will, therefore, be devoted respectively to the two types of environments used. We will show all the useful graphs in order to analyse and to comment on the obtained results.

5.1 Experimental methodology

This preliminary section is essential to understand better the tasks we tried to solve through the usage of reinforcement learning algorithms and what approach we used to evaluate experiments results.

5.1.1 Hardware and software details

In order to carry out the experiments contained in this chapter, we used a personal laptop. We chose this solution because the machine has excellent specifications to support the computational power required by the machine learning experiments both in terms of GPU and RAM.

Despite these initial considerations, we still had problems in terms of RAM. This type of experiment requires an extensive experience memory replay to allow optimal batch extraction. Despite the large RAM present and the reduction of the size of the input image, we were still forced to reduce the maximum size of the replay memory to complete the experiments.

We collected the essential information about hardware and software that we have used to perform experiments in tables 5.1 and 5.2 on this page and on the next page.

Table 5.1. Development Machine Hardware Specifications

Component	Details
Laptop	Dell Inspiron 15 7559
CPU	Intel® Core™ i7-6700HQ # of Cores: 4 # of Threads: 8 Processor Base Frequency: 2.60 GHz Max Turbo Frequency: 3.50 GHz
GPU	NVIDIA GeForce GTX 960M CUDA Cores: 640 Memory: 4GB GDDR5, 2500 MHz
RAM	12GB DDR3L, 1600 MHz

Table 5.2. Development Machine Software Specifications

Component	Details
Operating System	Ubuntu 18.04.3 LTS (Bionic Beaver)
Python	v.3.6.8
PyTorch	v.1.4.0
OpenAI Gym	v.0.15.4

5.1.2 Pendulum-v0 environment

OpenAI Gym *Pendulum-v0* environment formalises the inverted pendulum swing-up problem, a classic problem in the control literature. In this version of the problem, the pendulum starts in a random position, and the goal is to swing it up, so it stays upright.

We have also decided to include in this thesis the experiments we have carried out on this simulated environment because the results obtained and the problems faced were essential to have a more prepared approach to deal with the real-world experiment and the environment we designed for Cozmo.

Observation

The original implementation of this environment is based on a state represented by a `Box(3)` type, a data structure defined by OpenAI Gym that extends functionalities of a standard array. It contains values related to the current angle of the pendulum as described in table 5.3.

Table 5.3. Original Observation Pendulum-v0 environment

Index	Observation	Min	Max
0	$\cos(\theta)$	-1.0	+1.0
1	$\sin(\theta)$	-1.0	+1.0
2	$\dot{\theta}$	-8.0	+8.0

Since the goal of our thesis was to apply deep reinforcement learning algorithms to a problem such as the autonomous driving one where input data is composed of images, we decided to build a wrapper (`gym.ObservationWrapper`) for the original environment in order to receive observations as raw pixels. Thanks to this approach, we were able to apply the same considerations and the same convolutional neural networks that we used in the Cozmo environment.

We have started many experiments on this environment to find the most suitable number of images to use as a state, looking for a trade-off between the algorithm’s needs and the memory constraints imposed by the hardware we used. The agent revealed instability using a single frame, while it led to excellent results using two images. In the end, we decided to resize the image to 64×64 pixels to overcome hardware limitations.

A sample screenshot of the environment in action is shown in fig. 5.1.

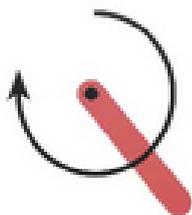


Figure 5.1. Frame of Pendulum-v0 environment. We decided to use a set of two subsequent 64×64 images.

Actions

The actions that the agent can perform within this environment are described through a `Box(1)` object containing only one element. This value corresponds to the joint effort, which allows the agent to swing the pendulum. The action space has also been maintained in the modified environment.

Table 5.4. Pendulum-v0 Actions

Index	Action	Min	Max
0	Joint effort	-2.0	+2.0

Reward

The reward for each timestep t is given by

$$r_t = -(\theta_t^2 + 0.1\dot{\theta}^2 + 0.001a_t^2)$$

where θ is normalized between $-\pi$ and π . Therefore, the lowest cost is $-(\pi^2 + 0.1 * 8^2 + 0.001 * 2^2) = -16.2736044$, and the highest cost is 0. In essence, the goal is to remain at zero angles (vertical), with the least rotational velocity, and the least effort. The reward design has also been maintained in the modified environment.

Starting state

The initial state of the environment in question is chosen randomly. Two values are extracted: the first is an angle between $-\pi$ to π , the second is a speed between -1 and 1. A zero angle corresponds to the standing pendulum.

Episode termination

OpenAI Gym documentation does not specify a particular episode termination for this environment: the choice is left to the user. In our case, after some attempts, we decided to set a limit value of 200 steps for each episode.

Solved requirements

Even in this case, OpenAI Gym documentation does not specify any indications to understand whether an episode has been solved. Indeed, *Pendulum-v0* is an unsolved environment, which means it does not have a specified reward threshold at which it is considered correctly completed.

5.1.3 CozmoDriver-v0 environment

CozmoDriver-v0, the reinforcement learning environment we implemented, is one of the contributions of this thesis. This section aims to present as schematically as possible the basic parameters that characterise the environment we have designed. Further details on the implementation choices, problems encountered, and solutions we have adopted to solve them are available in chapter 4 on page 59.

Observation

The observations we decided to use in *CozmoDriver-v0* are the same as those we exploited in the *Pendulum-v0* environment. Indeed, our agent will obtain, for each action carried out, a queue composed of two images from the front camera of Cozmo resized to 64x64 pixels. As in the previous environment, we decided to resize the images obtained in order to remain within limits placed by the RAM available in the development machine.

The first image represents the state before the action, while the second represents the consequences of the action taken. The number of images was set to two after performing some experiments on *Pendulum-v0* environment that revealed instability in the use of a single image. We decided to limit ourselves to two images, as we would increase the size of a single entry in replay memory by adding more of them. This choice would have required a counterbalance such as the decrease of the maximum size of replay memory.

As we mentioned in chapter 3 on page 42, Anki Cozmo has a front camera inserted inside its tilting head and one forklift. To obtain more valuable images for our experiments, we decided to tilt the head as much as possible down and raise the forklift: in this way, the image is focused on the lane, leaving everything that could distract the learning process outside the view.

An example of two subsequent frames received by Cozmo is available in fig. 5.2.

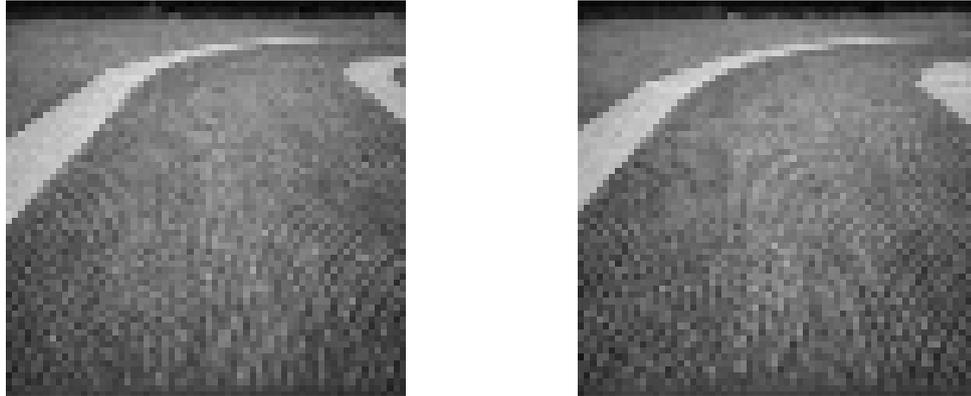


Figure 5.2. An example of a two subsequent frame of CozmoDriver-v0 environment. We decided to resize the image returned by Cozmo to 64×64 for memory consumption reason: a higher resolution would lead to a further decrease in experience replay memory.

Actions

We have already discussed in section 4.1.1 on page 61 the decisions taken to implement the management of actions within the environment that we have built.

To describe the actions that the agent can perform within this environment, we used a `Box(2)`. The first value of this object corresponds to the desired speed, while the second one represents the steering wheel position. Table 5.5 describes schematically this object.

Table 5.5. CozmoDriver-v0 Actions

Index	Action	Min	Max
0	Desired Speed (v)	0.0	+1.0
1	Steering Wheel Position (w)	-1.0	+1.0

Reward

The reward we chose for our experiment was the second one provided by section 4.1.1 on page 61. The decision has fallen on the *Lane Distance Reward* because it describes with simplicity the final goal of the task, but above all because it allows the user to have a direct counterproof of the effectiveness of the algorithm, by matching the reward to the distance travelled. Equation (5.1) reports the calculation that is executed to every time step to calculate the reward to the carried out action. c is the time expressed in seconds between one action and the next one, imposed as a system constant, while v_t is the desired speed taken by the current action expressed in millimetres per second.

Besides, we opted for setting the reward of the final episode step to zero because it occurs when the robot is approaching a harmful situation.

$$r_t = v_t \cdot c \tag{5.1}$$

Starting state

The starting state position of the system is not constant, but changes from episode to episode. This approach was preferred over the one with a fixed starting position for two simple reasons:

- Reduces the path that has to be travelled by the robot in order to be able to reposition, speeding up the experiments as it preserves battery consumption. In this approach, the robot is repositioned on the road closest to where the previous episode ended.
- It allows the agent to accumulate experiences that do not always refer to the same road segment. With this methodology, the experiences will most always begin and end in different states, leading the agent to put more effort into generalisation.

The episode starts as soon as the agent receives the start signal.

Episode termination

The episode ends when the robot goes off the road or reaches a dangerous situation. Even this time, the episode ends when the agent receives the stop signal.

Solved requirements

We have not provided a well-defined parameter to understand whether the task has been solved or not, because it depends on the path and the particular needs of the programmer. Potentially the episode could last forever if the robot could learn to run an entire circuit.

No mechanism has been implemented to communicate to the robot that the episode ended positively. For this reason, we suggest applying this environment to circuits and not paths where beginning and end do not coincide.

In our case, the route used is almost 3 meters long. So we decided to use this value as a target to reach to determine the resolution of the task.

5.1.4 Measuring performance

In recent years, we have witnessed the rapid growth of interest in deep reinforcement learning by the entire scientific community. This growth has led to an increase in experiments and works on this subject, which are often readily available. However, reproducing reinforcement learning experiments is not always as intuitive and straightforward as expected. Often, the measurements reported by papers and studies of this kind are difficult to interpret due to non-determinisms inherent in most environments in which these algorithms are applied. Without appropriate and meaningful metrics accompanied by standardisation in presenting the results, it becomes difficult to determine conclusively the improvements made to the state-of-the-art.

By reviewing the available literature, it is noticeable that reinforcement learning algorithms are often evaluated by presenting tables and graphs showing cumulative average rewards or the maximum reward achieved on a pre-set number of timesteps. However, the combined features of environments and algorithms make these values typically inadequate for a fair comparison. The cause is that numerous factors come into play, such as seeds and trials that lead to different performances and that do not contribute to making more transparent the actual performance of an algorithm. However, when these are accompanied by confidence intervals, based on a reasonably large number of attempts, then there are the premises to make decisions and formulate more informed considerations.

Once again, however, we have been forced to come to terms with reality. We were able to produce analysis as honest and specific as possible regarding experiments on *Pendulum-v0*. In this case, we could easily repeat the experiments ten times for each algorithm, so that we could report graphs containing more useful information, such as confidence margins.

On the other hand, experiments with Cozmo took a much larger number of episodes before starting to show the first improvements. We managed to maintain an average of just under 500-750 episodes per day: this underlines how difficult it was to get to conclude even a single experiment. For this experiment, we reported the results obtained without any confidence margin but focusing on the best training results as opposed to the results obtained during the test.

Another crucial consideration is the one concerning loss functions results: the values reported in a loss graph should not be considered in the typical sense from supervised learning. There are two crucial differences in reinforcement learning loss

functions:

- Data distribution depends on the current parameters. In supervised learning, we are used to working with loss functions that are defined on fixed data distribution. They are independent of the parameter that the process aims to optimise. In reinforcement learning, this characteristic does not apply because the data must be sampled from the current and most recent policy.
- A loss function can not determine and measure the performance of an algorithm. Even in this case, it could be useful to make a comparison with supervised learning: in this approach, a loss function evaluates the performance metric that we want to optimise. On the other hand, in the reinforcement learning scenario, researchers are interested in the expected return. Therefore, the loss function can not be useful to approximate this value. It is useful only when evaluated with the current parameters, with data generated by the current parameters.

The connection between loss function and performance does not apply immediately after the first step of gradient descent. Minimising a specific loss function for a given batch of data has no guarantee of improving expected return. Therefore, the word *overfitting* must not be interpreted from a supervised learning perspective: it should be merely considered as a descriptive word without any relationship with the generalisation error.

From a performance perspective, the loss function means nothing in reinforcement learning [48]. This fact is one of the fundamental points that distinguish supervised learning to reinforcement learning. The researcher should only care about the average return. For this reason, we decided to measure the performance of the experiments by using the deterministic policy with DDPG and the mean policy with SAC without any noise for ten episodes and reporting the average return.

Sections 5.2 and 5.3 on the current page and on page 96 will show the most relevant results and graphs obtained from the respective experiments. The final part of each section will be accompanied by a comment on the results obtained, paying particular attention to the comparison between the two algorithms.

5.2 Pendulum-v0 experiments

5.2.1 DDPG hyperparameters

The hyper-parameters we exploited in this experiment are shown in table 5.6 on the next page. The epsilon decay function is presented in eq. (5.2) on the following page where e is the current episode number. It is used to decrease the noise impact on actions in function of the number of episodes. When it reaches the ϵ_{end} , it will become a constant.

Table 5.6. DDPG Hyper-parameter setup for Pendulum-v0 environment

Hyper-parameters	Value
Policy Network	Learning Rate: 1×10^{-4} Architecture 3 CONV Layer $3 \times 3 \times 16$, stride 2, padding 0 2 FC Layer with hidden size = 256 1 Output value
Q Network	Learning Rate: 1×10^{-4} Architecture 3 CONV Layer $3 \times 3 \times 16$, stride 2, padding 0 2 FC Layer with hidden size = 256 1 Output value
Ornstein Uhlenbeck Noise	$\mu = 0.0 \ \sigma = 0.3 \ \theta = 0.15$
Epsilon Decay Noise	Start: 0.9, End: 0.2, Decay: 200
Gamma (γ)	0.99
Tau (τ)	1×10^{-3}
Observation	Buffer Size: 2 Image Size: 64×64
Batch Size	64
Max Number of episode steps	205
Replay Memory Size	10000
#Epoch per Episode	250
Soft Target Update per Epoch	1
Test Phase	Test frequency: every 5000 epochs Test episodes: 10

$$\epsilon = \epsilon_{\text{start}} - (\epsilon_{\text{start}} - \epsilon_{\text{end}}) \min\left(1.0, \frac{e}{\epsilon_{\text{decay}}}\right) \quad (5.2)$$

5.2.2 SAC hyperparameters

The hyper-parameters we exploited in this experiment are shown in table 5.7 on the next page.

Table 5.7. SAC Hyper-parameter setup for Pendulum-v0 environment

Hyper-parameters	Value
Policy Network	Learning Rate: 3×10^{-4} Type: Gaussian Policy Architecture 3 CONV Layer $3 \times 3 \times 16$, stride 2, padding 0 2 FC Layer with hidden size = 256 1 Output value
Q Network	Learning Rate: 3×10^{-4} Architecture 3 CONV Layer $3 \times 3 \times 16$, stride 2, padding 0 2 FC Layer with hidden size = 256 1 Output value
Gamma (γ)	0.99
Tau (τ)	5×10^{-3}
Entropy Autotune	Enabled
Observation	Buffer Size: 2 Image Size: 64×64
Batch Size	64
Max Number of episode steps	205
Replay Memory Size	10000
#Epoch per Episode	250
Soft Target Update per Epoch	1
Test Phase	Test frequency: every 5000 epochs Test episodes: 10

5.2.3 Comparative analysis

This section aims to present the most critical plots we obtained from *Pendulum-v0* experiments. The results obtained exploiting SAC algorithm are presented in figs. 5.4 and 5.6 on page 92 and on page 93, while the ones gathered with DDPG algorithm are presented in figs. 5.3 and 5.5 on page 92 and on page 93.

Figures 5.3 and 5.4 on page 92 shows the result of the training phase. These plots have the number of episodes in the abscissa and the reward obtained in the ordinate. The results of these graphs are unstable both in the average value and in margins sizes. This phenomenon is mainly caused by the noise introduced during

training: it allows the agent to explore the space in the environment without focusing on the current best action but trying to explore entirely and randomly the totality of environment space. In the first case, the DDPG noise is given by the Ornstein Uhnlebeck process noise, while SAC exploits a Gaussian Policy by sampling a random action from the current distribution given by the network. Therefore, SAC algorithms exploit the *entropy autotune* presented by its authors: its main aim is to reduce the impact of hyper-parameters by automatically tuning the α temperature parameter. This lead to a more straightforward setup of the experiment without requiring manual optimal temperature setup, which is non-trivial and needs to be tuned for each task.

It is possible to investigate about these two trends in figs. 5.9 and 5.10 on page 95. We exploited eq. (5.2) on page 89 to manipulate the importance of the noise through the whole set of episodes for each run. The contribution of the noise decreases directly proportional to the number of episodes completed to enhance exploration in the first part of the experiment. On the other side, the autotuning approach of SAC influences the way the reward is calculated and used to train the network. The objective is to give more reward to actions that have higher entropy, that is more unpredictable. This approach is motivated by the fact that an unpredictable situation can bring more information to the learning process than a more predictable one. In DDPG, the noise is regulated by the combination of Ornstein Uhlenbeck noise process and an epsilon decay function that regulates how the noise influences actions with the growth in the number of episodes completed.

It is noticeable that SAC results seem more valuable than DDPG ones: the SAC agent manages to touch the zero value after about 30 episodes and reaches a sort of asymptote between 100 and 200 after about 60 episodes. On the other hand, the DDPG agent obtained a worse performance by touching the zero value after about 100 episodes and the corresponding values of SAC asymptote only in the last part of the experiment. This fact is even more remarkable if we analyse the average of the previous 100 episodes carried out in training, as shown in figs. 5.7 and 5.8 on page 94.

A criticism that can be made to this analysis is represented by the different amounts of noise present in different episodes. If that were the case, the testing phase of the DDPG algorithm, where any noise is removed, should produce better performance or, at least, comparable to those of SAC. However, analysing the result of the test phase shown in figs. 5.5 and 5.6 on page 93, it is clear that the different trends described above remain unchanged. As mentioned before in this work, we decided to start a test phase every specified amount of epochs correctly executed. For this reason, these plots have the number of epochs in the abscissa and the average reward obtained from 10 testing episode in the ordinate. Even in the testing phase, the most important, the outstanding performance of SAC is not achieved by the DDPG one.

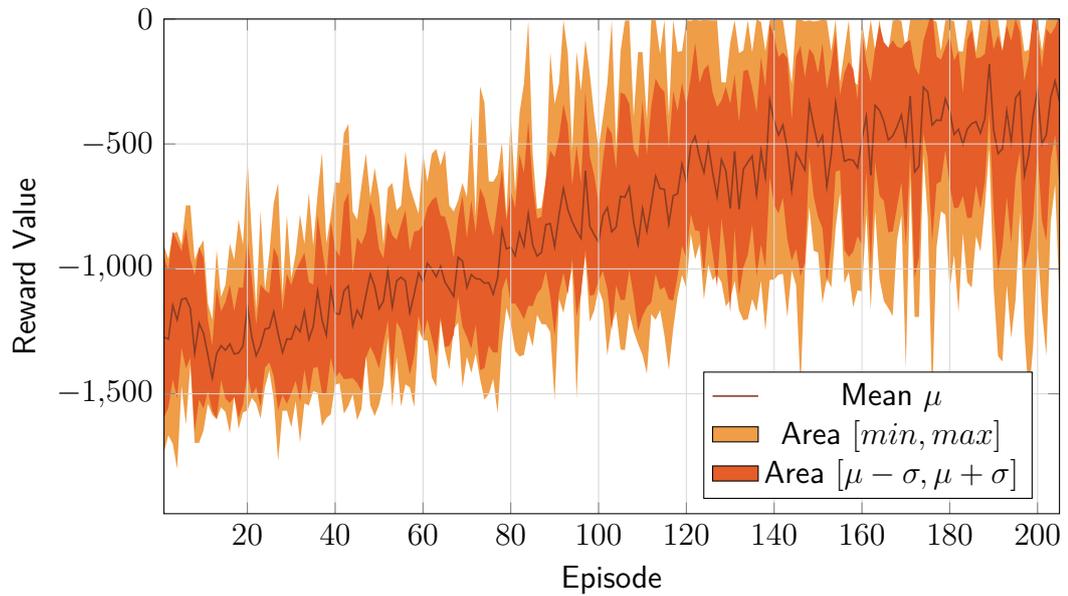


Figure 5.3. DDPG Pendulum-v0 Reward Plot. The graph reports mean, standard deviation range and min-max range of the reward of each episode over 10 runs with different seeds.

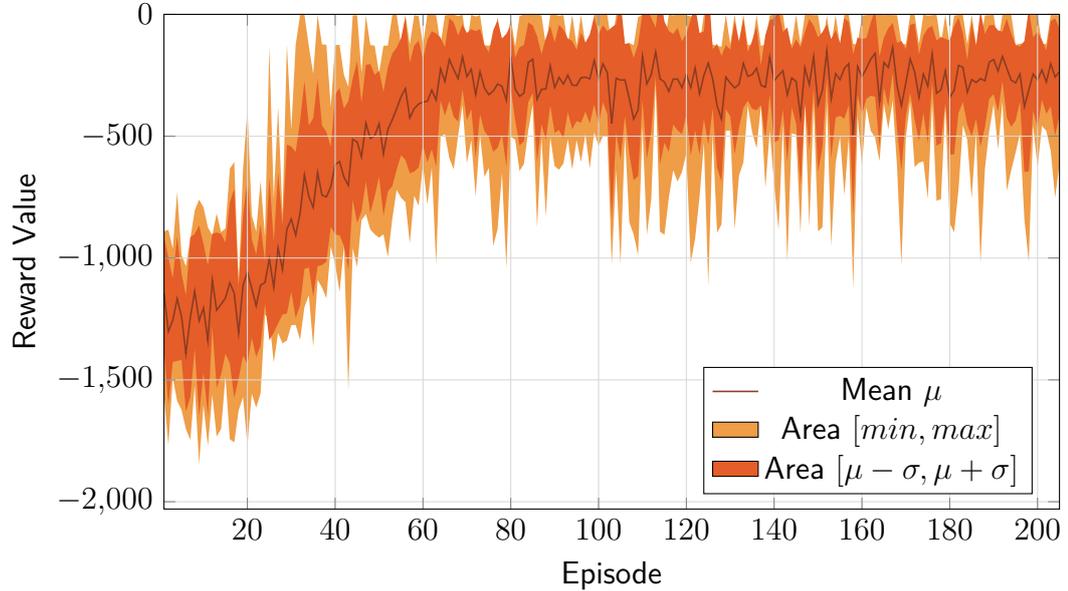


Figure 5.4. SAC Pendulum-v0 Reward Plot. The graph reports mean, standard deviation range and min-max range of the reward of each episode over 10 runs with different seeds.

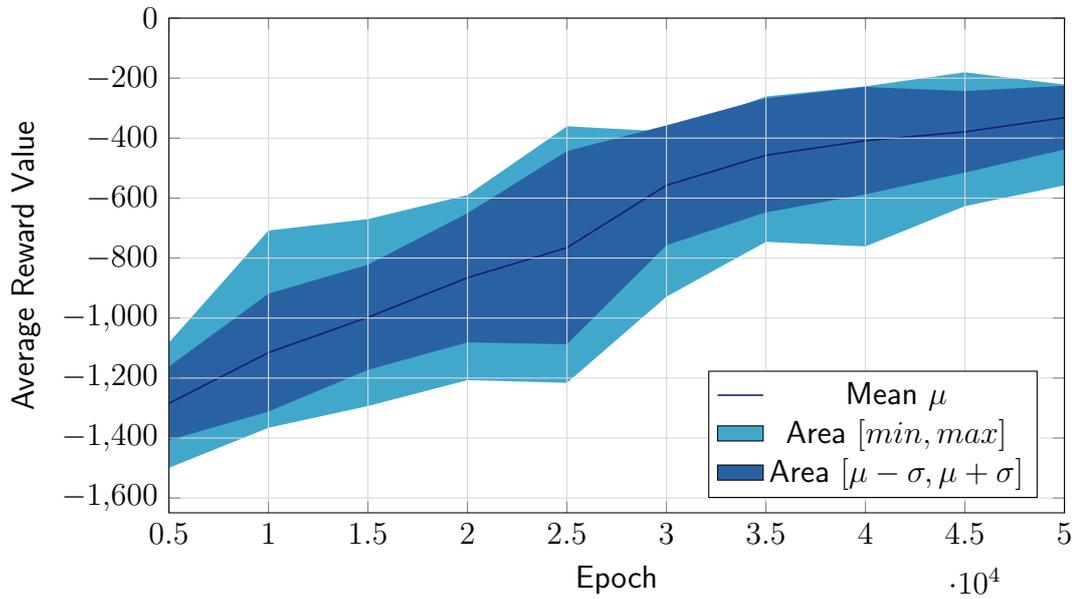


Figure 5.5. DDPG Pendulum-v0 Test Average Reward Plot. The graph reports mean, standard deviation range and min-max range of the average reward obtained from 10 test episodes every 5000 epochs. They are calculated on 10 runs with different seeds.

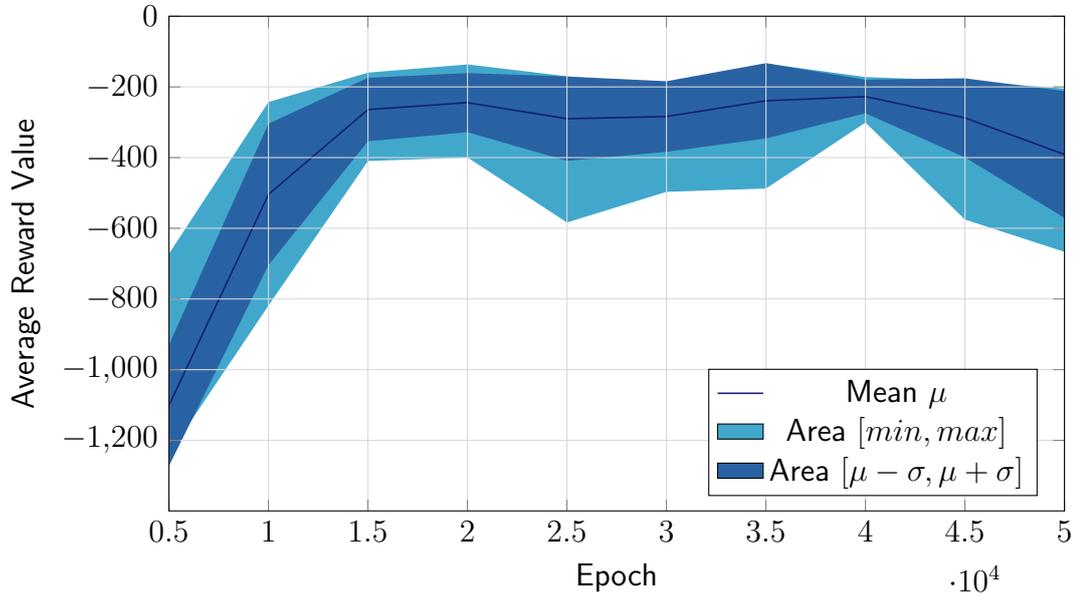


Figure 5.6. SAC Pendulum-v0 Test Average Reward Plot. The graph reports mean, standard deviation range and min-max range of the average reward obtained from 10 test episodes every 5000 epochs. They are calculated on 10 runs with different seeds.

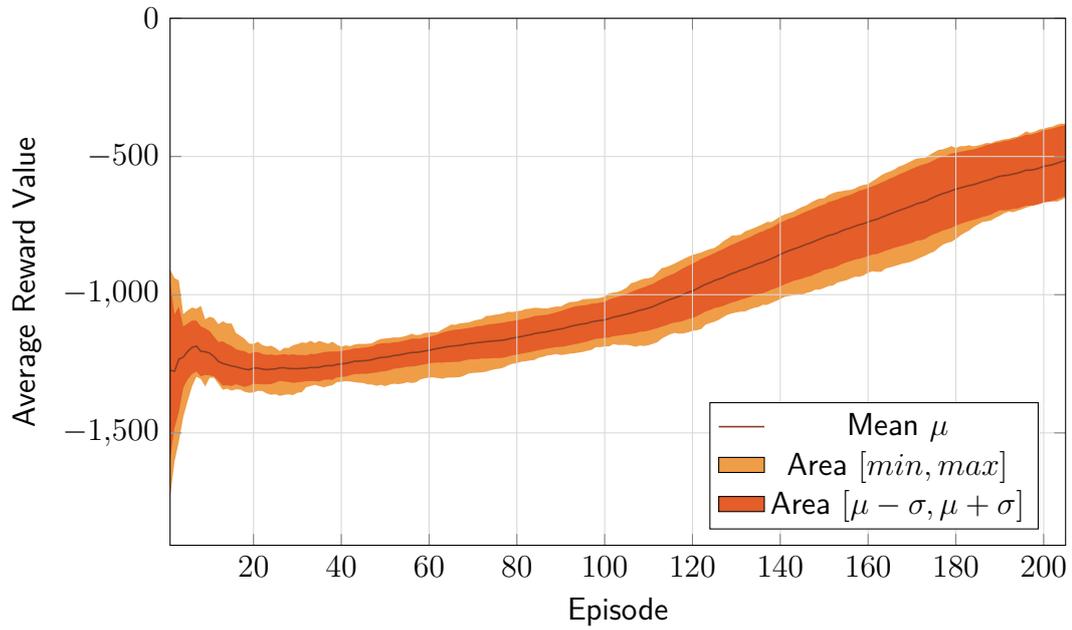


Figure 5.7. DDPG Pendulum-v0 Last 100 Episode Average Reward Plot. The graph reports mean, standard deviation range and min-max range of the last 100 episode average reward for each episode over 10 runs with different seeds.

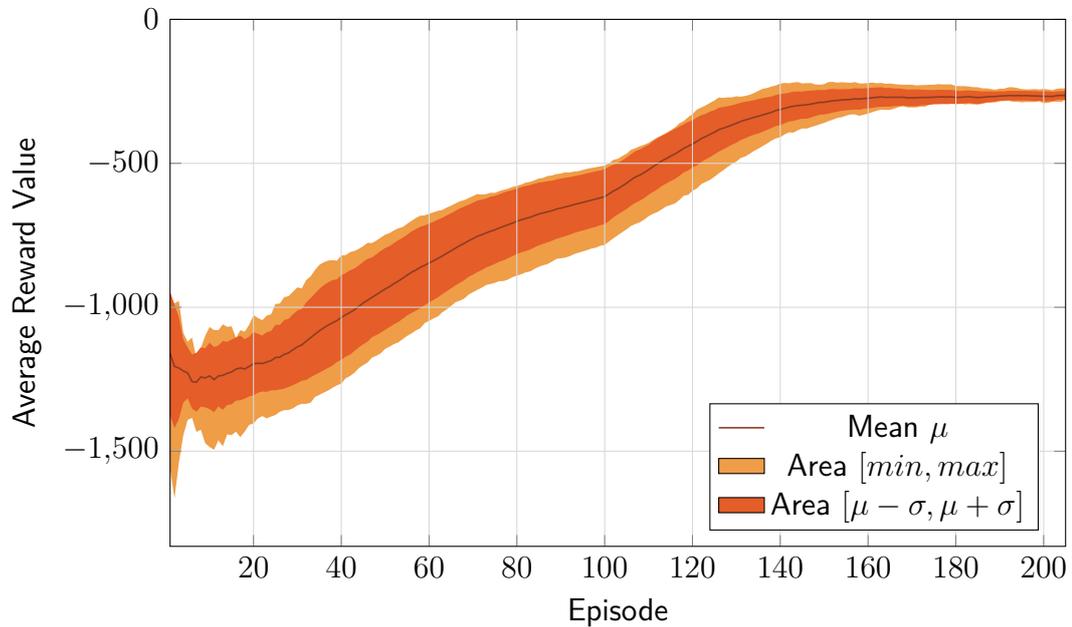


Figure 5.8. SAC Pendulum-v0 Last 100 Episode Average Reward Plot. The graph reports mean, standard deviation range and min-max range of the last 100 episode average reward for each episode over 10 runs with different seeds.

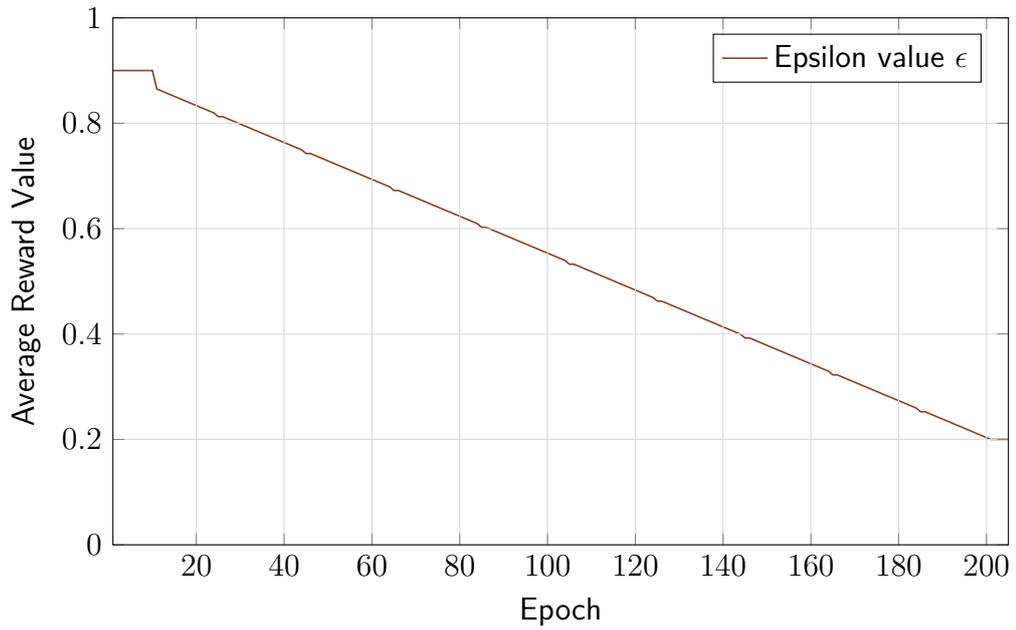


Figure 5.9. DDPG Pendulum-v0 Noise Epsilon Decay. The graph shows the trend of the noise epsilon decay applied to the Ornstein Uhlenbeck noise in DDPG.

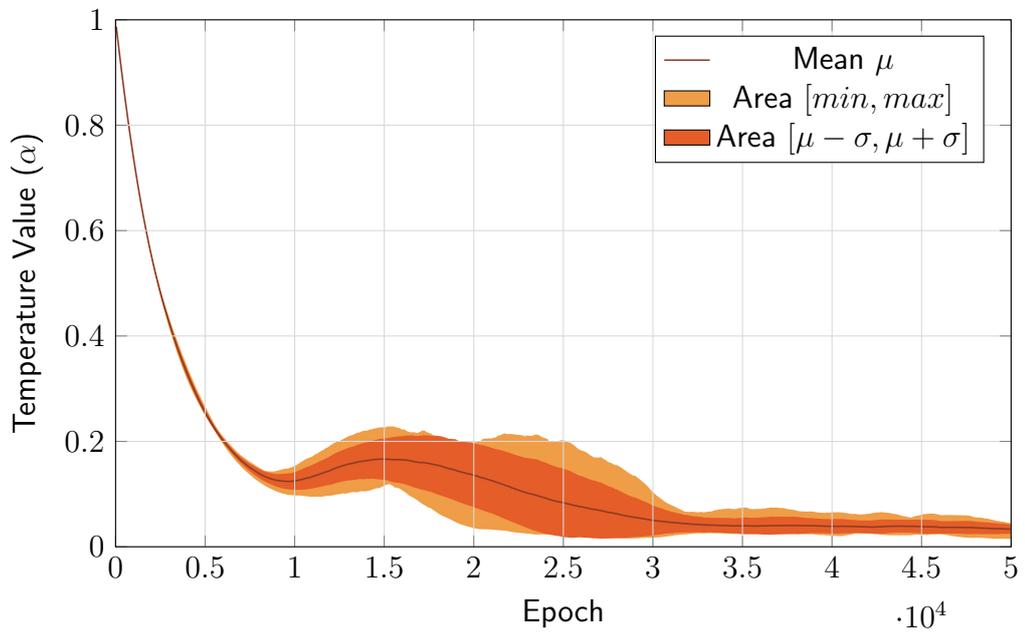


Figure 5.10. SAC Pendulum-v0 auto-tuning temperature. The graph shows the trend of the temperature parameter learned through the auto-tune process proposed by SAC authors.

5.3 CozmoDriver-v0 experiments

After the completion of the experiments carried out with *Pendulum-v0* environment, we started to implement both algorithm in parallel to work with the specific features of *CozmoDriver-v0*.

5.3.1 The DDPG approach

By following the DDPG approach, we exported the code already used in the preliminary experiments with *Pendulum-v0* environment, by adapting it with proper modifications. For instance, we gathered the learning phase at the end of each episode instead of leaving it distributed on every action of each episode.

However, the results were unexpectedly bizarre: the robot, right after the warm-up episodes phase, started to act by always selecting the same action. It kept steering to the right with the maximum velocity, even after hundreds of episodes. For this reason, we selected a range of possible algorithm components to modify in order to analyse any changes in agent behaviour: among these points, we find the neural network (e.g. weight initialisation, convolutional layers), the frequency and extent of the learning phase or the amount of noise used. Therefore, we started a set of experiments to validate these changes in order to find a solution to proceed to carry out experiments on a broad set of episodes. This process has been complicated to carry forward since it is almost impossible to do an accurate analysis (e.g. grid-search) in the real world with such a large amount of parameters.

Unfortunately, despite this research, the agent behaviour did not change from the initial one. This fact has not allowed the actual execution of the experiments envisaged by our intentions. Indeed, the presence of concise episodes within the long-term experiments (e.g. hundreds of episodes), due to a bizarre initial policy of the robot, caused the constant insertion of experience coming from faulty episodes in the replay memory: this fact inexorably poisoned the replay memory of the agent, affecting the whole learning process.

The DDPG algorithm was created by its authors with a proper deterministic nature, different from the assumptions made by the authors of the SAC algorithm, who aimed to overcome the limits of the first approach to model-free deep reinforcement learning. As an example, we can report the presence of a deterministic policy in DDPG instead of the Gaussian policy exploited by SAC. Taking all arguments into account, we confirmed the intrinsic difficulties of the DDPG algorithm regarding its application in the real world without proper preliminary experiments in simulations (e.g. hyper-parameters tuning), convincing us definitively in carrying out the experiments with SAC.

5.3.2 The SAC approach

We decided to implement the SAC algorithm for this type of task after the great results reached in previous experiments with *Pendulum-v0* and its adaptability to various kind of problems, especially real-world ones, reported by its authors.

In the first implementation, we decided to maintain the number of epochs for each episode equal to 250. However, this decision revealed its fragility soon. In *Pendulum-v0* environment, the number of steps per episode was a constant number chosen in the initial setup of hyper-parameters. On the other hand, in *CozmoDriver-v0* environment every episode can have a different number of steps because this value is not a constant, but it depends on the decision of the user that is teaching Cozmo how to drive by stopping episodes. The behaviour of these two experiments also influences the filling of the replay memory. Because each step results in a tuple to insert in this memory, it is noticeable that the agent performance in the *CozmoDriver-v0* experiment has consequences in how fast the memory is filled. Therefore, starting 250 learning epochs after the completion of a short episode that inserted little information in the replay memory can lead the algorithm to learn by fetching batches of experiences from an almost identical group to the previous one. The performance of this learning setup resulted in a bizarre policy where the robot manages to correctly perform straight sections of the track and steer in the wrong direction at each turn after almost 700 episodes. Furthermore, the temperature (α) increased until an asymptote of 4: a bizarre tendency considering the experiment carried out with the *Pendulum-v0* environment.

After the analysis of the previous experiment, we decided to set a dynamic approach in the number of epoch to take for each timestep. We decided to work with multiples of 10 and follow eq. (5.3) to determine how many steps of learning to take after each episode. In eq. (5.3), x variable determines how many epochs the algorithm must perform for each set of ten steps in the episode in question, while y specify the minimum number of epochs of the learning phase for each episode, without depending on the number of steps. In the experiment in question, we chose to set both values to 10. The results improved from the initial implementation leading to a reduction in the gap time between two consecutive episodes and a performance increase. Thanks to this method, the learning process depends on episodes lengths and led to a more manageable experiments flow.

$$\text{learning_epochs} = \left\lfloor \frac{\text{episode_steps}}{10} \right\rfloor \cdot x + y \quad (5.3)$$

Since the number of learning epochs is not predictable a priori as happened with *Pendulum-v0* experiments, we decided to manage the frequency of the test phases by starting them every 50 episodes. To appropriately represent these values in the graph, we reported the number of learning epochs carried out up to that moment.

5.3.3 SAC hyperparameters

The hyper-parameters we exploited in this experiment are shown in table 5.8.

Table 5.8. SAC Hyper-parameter setup for CozmoDriver-v0 environment

Hyper-parameters	Value
Policy Network	Learning Rate: 3×10^{-4} Type: Gaussian Policy Architecture 3 CONV Layer $3 \times 3 \times 16$, stride 2, padding 0 2 FC Layer with hidden size = 256 2 Output value
Q Network	Learning Rate: 3×10^{-4} Architecture 3 CONV Layer $3 \times 3 \times 16$, stride 2, padding 0 2 FC Layer with hidden size = 256 1 Output value
Gamma (γ)	0.99
Tau (τ)	5×10^{-3}
Entropy Autotune	Enabled
Observation	Buffer Size: 2 Image Size: 64×64
Batch Size	64
Replay Memory Size	10000
#Epoch per Episode	Equation (5.3) on the preceding page with $x = y = 10$
Soft Target Update per Epoch	1
Test Phase	Test frequency: every 50 episodes Test episodes: 10

5.3.4 Results analysis

After carrying out numerous experiments to fix bugs in the code and verify the correct execution of the algorithm flow, we managed to complete a whole set of 3000 episodes exploiting the SAC algorithm to solve the autonomous driving task with Cozmo. Taking into account waiting times between episodes and charging times, we managed to complete the experiments in almost one week, after almost 1.3×10^5 epochs of learning.

Unfortunately, the results we reached have not led to a stable resolution of the self-driving task. However, the graphs in figs. 5.12 and 5.14 on page 102 and on

page 103 reports a continuous improvement in the behaviour of the robot during the episodes.

The first 20 episodes were dedicated to the warm-up: the agent gathered replay memory experiences by exploiting a random policy. This process was essential to obtain a set large enough to allow a proper batch learning phase of the agent. After that, the agent started to exploit the randomly initialised policy network to make decisions in the real-world environment. As we can see from both training and test graphs in figs. 5.12 and 5.14 on page 102 and on page 103, the first 150 episodes were characterised by a minimal reward. This fact was particularly evident in the first testing phases, where both average reward and standard deviation were meagre. Indeed, the robot was stuck in fixed actions steering to the left or the right without considering the current surrounding environment: this behaviour was caused by the fact that the neural network was not enough trained to provide a thoughtful decision. Furthermore, the dynamic increase of learning epochs which depends on the length of each episode accentuated this phenomenon: at least in the first part of the experiment, short episodes lead to fewer learning steps and then to slower improvement in the performance of the neural network.

As the number of episodes increases, it is noticeable the rising of episode rewards as we can see from the training and the last 100 episodes average plots in figs. 5.12 and 5.13 on page 102 respectively.

The training episodes plot shows an increase in the maximum reward obtained: it culminates in reaching almost 2.7 metres in episode 2764. Despite this fact, this particular increase is difficult to detect: this factor can be explained with the addition of the noise for exploration sake, introduced during the experiment by the random sampling from the output of the gaussian policy exploited, and the presence of the temperature parameter α that manipulates the importance of the entropy during the learning phase. The presence of this kind of noise did not lead to a parallel increase of both reward and completed episodes.

Therefore, analysing average rewards calculated on the set of the last 100 episodes in fig. 5.13 on page 102, we noticed an increase until episode 900 and then an almost constant fluctuation between 350mm and 450mm. Even in this case, the results showed by this graph were not high, but this fact can be motivated again by the presence of the noise in the training process.

However, the agent reached the most significant results in the testing phase presented in fig. 5.14 on page 103. To report the testing phase more appropriately, we decided to calculate the minimum and maximum values obtained in every set of ten episodes together with the mean and the standard deviation. The graph reports these values by using confidence intervals. Following this approach, we noticed a performance increase with a maximum mean of almost 1 metre, as highlighted by fig. 5.15 on page 103. Furthermore, the maximum value reached among all tests episodes was equal to almost 3.5 metres which equals more than one complete tour of the track. It is noticeable that the results are not stable as we expected after the

experiments we carried with *Pendulum-v0* environment: the reward values do not improve uniformly with increasing epochs. However, carrying out the experiments episode by episode, we noticed a marked improvement in the performance obtained in the tests. The robot learned to approach turns and to stay on the lane of a straight road.

Despite these improvements, the agent was not able to learn how to drive securely and stably. It manages to perform great for the most of the track, but it often concluded its run with a sudden turn out of the road. These facts made us reflect on the critic points of our experiment setup that may have had a role in the instability of the results obtained.

- The length of the experience memory replay we designed was equal to 10^4 , even if the length suggested by the literature is equal to 10^6 , two lower orders of magnitude. We made this decision because of the RAM available in the development machine. The learning process of the agent needs to store whole tuples of experience in the replay memory. They contain a total of four 64×64 images, two to represent the current state and two for the next state. As we discussed in chapter 4 on page 59, another need that we had to satisfy to recover the system from fault correctly, was the implementation of a periodic backup phase. This feature was essential to complete long experiments, like the one in question, to restart from the previous checkpoint in case of unexpected errors. However, this process needed a lot of RAM to store a serialised version of the whole set of variables used in the learning process, such as neural network weights and biases or experience memory replay. To avoid problems with memory and slowdowns due to the usage of swap space, we had to reduce the dimension of the replay memory further. We think that this decision has influenced the flow of the learning process: the first motivation is the small dimension of the set used to do batch learning. This factor influences the experiment directly because only the latest experiences are available for agent usage, and this leads inexorably to a lack of generalisation.
- Another problem that emerged from this experiment was the one concerning the behaviour of the robot on straight roads. Even after numerous learning epochs, the agent often showed a curvilinear approach. After noticing this fact, we started to analyse episode images to find out some correlation to understand this behaviour better. We noticed that the image obtained from the view of one side of the straight road was very similar to the turning point situation. It was probably this similarity that caused the oddity in Cozmo behaviour. Indeed, the viewing angle of the Cozmo camera was not large enough to detect both lane lines at the same time. It would be also difficult for a human to understand the best decision to make, using the images provided by Cozmo SDK. We tried to reduce the width of the road, but, instead of

finding a considerable improvement, it became more challenging to keep the robot between the lines. In the end, we opted for maintaining the initial width of the lane to preserve the proportion with the autonomous driving problem with a real car.

- Another particular behaviour adopted by the reinforcement learning agent we trained was caused by the combination of two factors: the particular design of the track we build and the narrow viewing angle of the Cozmo camera. When Cozmo was too close to one of the two road border, the agent often seemed to recognise that line as the opposite one and decided to take a sudden turn in the wrong direction.

In the end, we can report different results between the experiments carried out with *Pendulum-v0* environment and the *CozmoDriver-v0* one. The evident motivation is the different nature of these problems. The second one is in the real world setup, where observations and actions may be brittle and different because of many factors that start from uncontrollable changes in the surrounding environment.

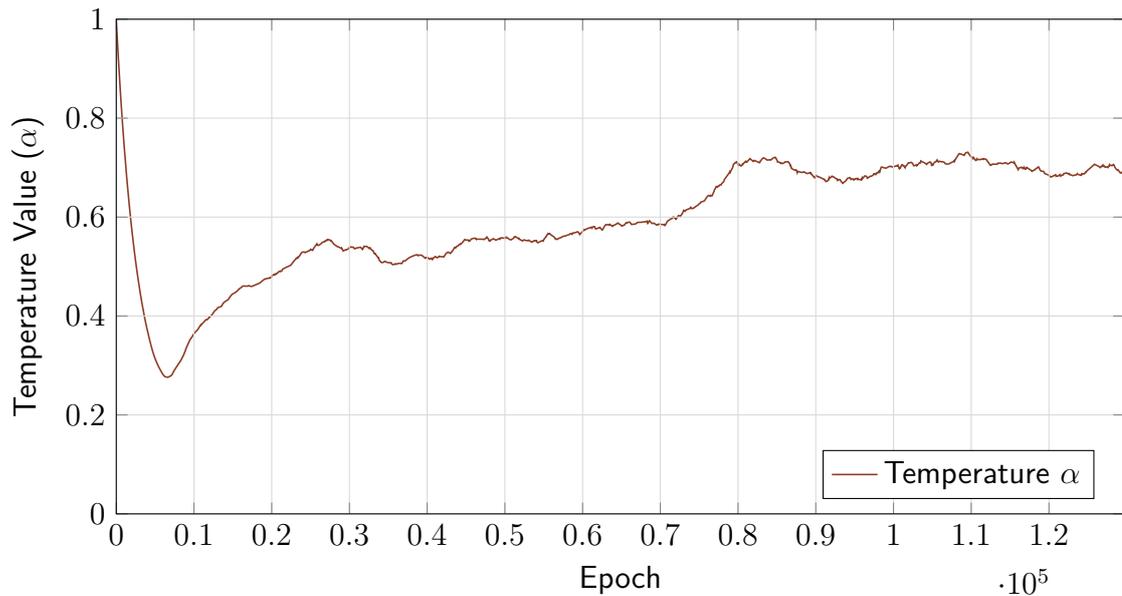


Figure 5.11. SAC Pendulum-v0 auto-tuned temperature. The graph shows the trend of the temperature parameter learned through the auto-tune process proposed by SAC authors.

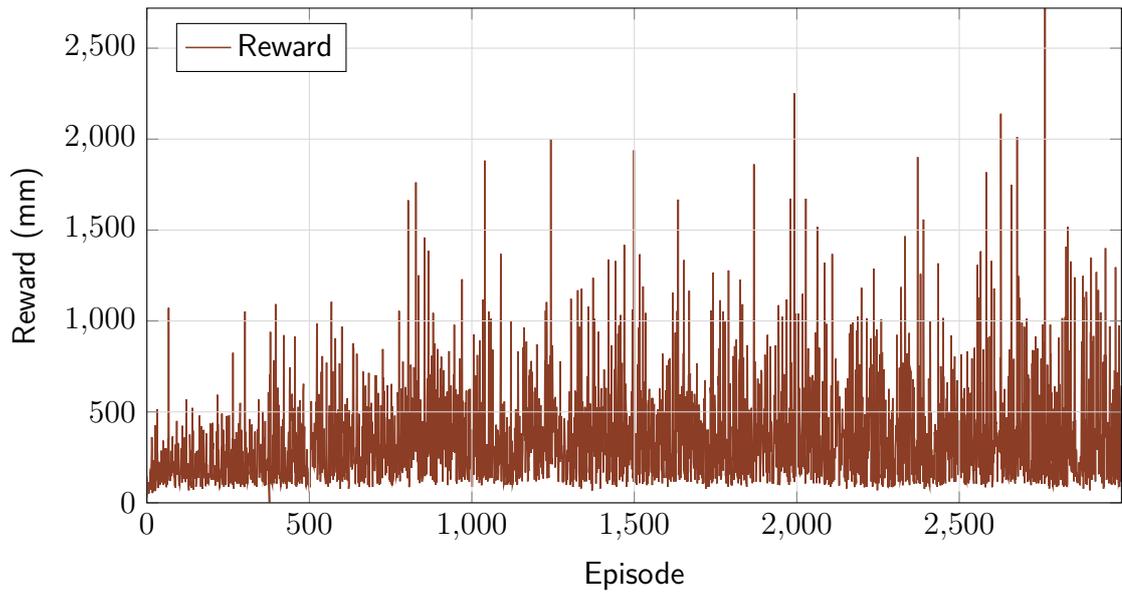


Figure 5.12. SAC CozmoDriver-v0 Reward Plot. The graph report the reward obtained from each episode.

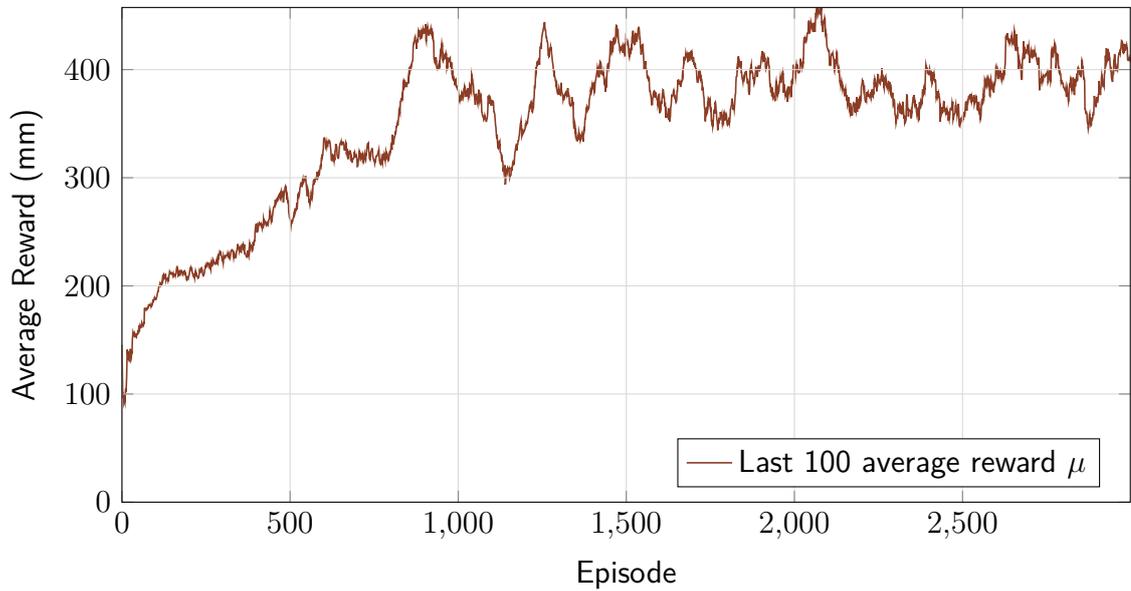


Figure 5.13. SAC CozmoDriver-v0 Last 100 Episode Average Reward Plot. The graph reports the last 100 episode average reward for each episode.

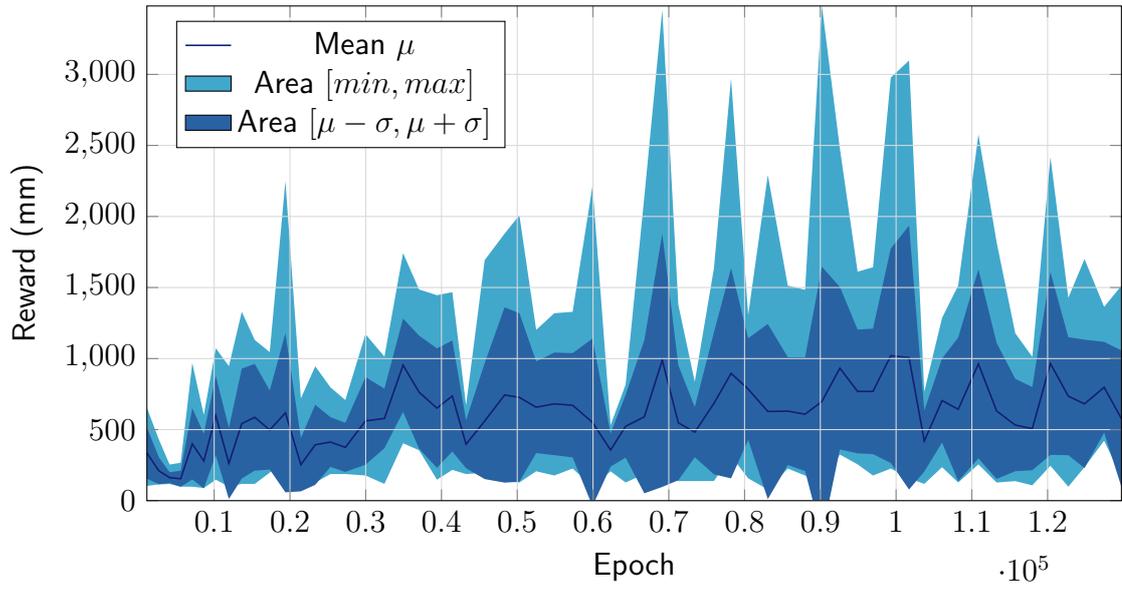


Figure 5.14. SAC CozmoDriver-v0 Test Reward Plot. The graph reports mean, standard deviation range and min-max range of the average reward obtained from 10 test episodes every 50 episodes.

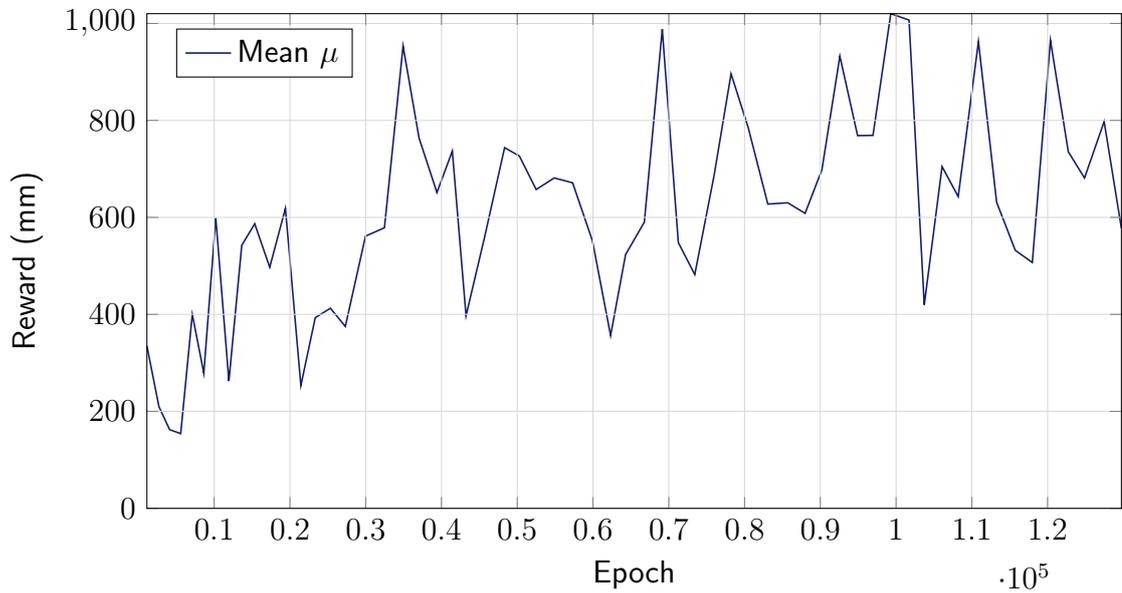


Figure 5.15. SAC CozmoDriver-v0 Test Average Reward Plot. The graph reports with a focus on the average reward obtained from 10 test episodes every 50 episodes.

Chapter 6

Conclusions

The growing interest in deep reinforcement learning approaches to real-world problems together with the fervour behind the development of autonomous driving has motivated and stimulated our research. Reinforcement learning proposes a brand new method to address decision-making problems, that is capable, in the premises, of replacing hand-made algorithms in the most varied tasks. For this reason, it is considered one of the enabling technologies to take a further concrete step towards Artificial General Intelligence (AGI). Although it achieved its best results in simulated environments such as video games, the interest of research in recent times has shifted to applications in the real world, looking for algorithms more and more easily configurable and parameter agnostic.

The first contribution of this thesis consists of the design of a control system to apply reinforcement learning algorithms in the real world. To achieve this aim, we decided to use the standardised approach provided by OpenAI Gym to project environments. We implemented the same interface used by simulated environments binding OpenAI Gym methods to features and functions offered from Anki Cozmo SDK. The approach used in the development of this system has allowed obtaining an environment in which any researcher can apply his algorithms interfacing directly with the reinforcement learning framework, without worrying about direct interfacing with the robot.

The designed system allowed us to perform reinforcement learning experiments straightforwardly, meeting the specifications required, such as the possibility to backup and restore their state.

The second contribution of this thesis consists of the application of a reinforcement learning algorithm suitable for experiments in the real world. We designed our implementation of Soft Actor-Critic (SAC) by modifying its original flow to match the requirements of the environment. Firstly, we implemented a revised environment of a traditional control problem to apply deep reinforcement learning algorithms instead of traditional ones, using the same convolutional neural network used with Cozmo experiments. Therefore, we performed and reported an

experiment of 3000 episodes with the environment designed for Cozmo. We based our approach on SAC algorithm after the analysis of the performance comparison between DDPG and SAC experiments in the previously mentioned revised environment, which showed better performances with SAC. The results were not so astonishing as we expected from the results presented in [29, 30], but they appear aligned with those obtained by [21]. We notice a constant improvement in the behaviour of the robot, especially in the testing phase, reaching a maximum value of more than 3 meters and an average of about 1 meter on 10 test episodes. After the conclusion of the experiments, as reported in section 5.3.4 on page 98, we focused on what might have been the most significant factors that led to these results.

We localised two major problems which, in our opinion, have had a particular influence on the results obtained. The first factor was the amount of RAM available in the development machine. Off-policy reinforcement learning algorithms require a memory replay in which to store past experiences and, in particular in our implementation, a portion of free RAM to be able to backup variables easily. This limitation forced us to decrease the size of the replay memory and a consequent early deletion of less recent episodes. Analysing the plots, we noticed that this fact translated in the increase of the temperature: this symptom underlines the need for the algorithm to explore more the solution space. The second major problem was the limitation of the camera sensor on the robot, particularly its viewing angle. The features offered by the Anki Cozmo camera proved to be inadequate to observe the track we designed. We noticed this fact after many episodes when the robot started to improve its performance: it began to adopt a wave behaviour on the straights, interpreting the vision of a single road line as a curve. Moreover, we noticed the difficulty of the algorithm in detecting differences between left and right lines: an excessive approach to one of them led the agent to recognise that line as the opposite one and then to steer abruptly, making a mistake. The last-mentioned problem may be related to the fact that the colour of the road is identical to the part beyond road lines. However, Anki developers primarily designed the Cozmo camera for facial recognition, so it does not have a viewing angle large enough to allow a comprehensive view of the road.

6.1 Future work

Our proposals about future improvements to the project grow from the weakness in our approach that we just described. Our attempt to make the system data-efficient by decreasing the experience memory replay did not work. It could be interesting to execute these algorithms on a device with a bigger RAM, but also to design this approach with a Variational Auto-Encoder (VAE) [32] to reduce the dimensionality of the information retrieved during experiments and compare the results with the ones obtained in this thesis. Indeed, this method revealed improvements in many

applications and in particular in the one reported in [29, 30].

It may be useful to enhance sensors installed in the self-driving robot to improve SAC algorithm performances. We suggest, in particular, to substitute the camera with one that has a viewing angle large enough to visualise the whole width of the track. In addition to the possibility to build up a personal *Donkey Car* with custom specifications and sensors, we believe that one valuable alternative to Anki Cozmo could be Anki Vector, the successor of Cozmo which mounts a 720p camera with 120° Ultra Wide FoV. It could be interesting to use Anki Vector to perform reinforcement learning algorithms with the usage of the renewed front camera together with the infrared laser scanner on-board. This approach can lead to the attractive possibility to investigate approaches to data fusion with data provided by a set of sensors and see the reflections of these choices in the performance of the learning process.

In this thesis, we focused on model-free reinforcement learning algorithms to solve the self-driving task we proposed, developing our ideas starting from the intuitions provided by [29, 30]. However, taking into account the recent results obtained in this research field as reported in [23, 75], we think that another intriguing research to carry out is an investigation about the application of model-based reinforcement learning algorithms to autonomous driving. A more in-depth review of the literature to better understand the feasibility of this approach compared to model-free ones, focusing on its strengths and weaknesses, can be the right starting point to make the next step towards the application of reinforcement learning algorithms to autonomous systems.

Appendix A

Reinforcement Learning

A.1 Bellman equation

The value function is decomposable in the immediate reward r_t and the discounted state value of the next state. It is possible to obtain the result in eq. (A.1) by writing expectations explicitly.

$$\begin{aligned}
 V^\pi(s) &= \mathbb{E}[g_t | s_t = s] \\
 &= \mathbb{E}[r_{t+1} + \gamma r_{t+2} + \gamma^2 r_{t+3} + \dots | s_t = s] \\
 &= \mathbb{E}[r_{t+1} + \gamma g_{t+1} | s_t = s] \\
 &= \sum_{a \in \mathcal{A}} \pi(a|s) \sum_{s' \in \mathcal{S}, r \in \mathcal{R}} P(s', r | s, a) [r + \gamma \mathbb{E}[g_{t+1} | s_{t+1} = s']] \\
 &= \sum_{a \in \mathcal{A}} \pi(a|s) \sum_{s' \in \mathcal{S}, r \in \mathcal{R}} P(s', r | s, a) [r + \gamma V^\pi(s')]
 \end{aligned} \tag{A.1}$$

This equation expresses the relationship between the value of a state and the values of its successor states. It is further possible to derive the Bellman Equation for Action-Value function using the same procedure described above.

The resulting formulas are shown in eq. (2.7) on page 10.

Furthermore, it is possible to obtain the Bellman Equation solution in eq. (A.2) working with matrix notation.

$$\begin{aligned}
 V^\pi &= \mathcal{R}^\pi + \gamma \mathcal{P}^\pi V^\pi \\
 (I - \gamma \mathcal{P}^\pi) V^\pi &= \mathcal{R}^\pi \\
 V^\pi &= (I - \gamma \mathcal{P}^\pi)^{-1} \mathcal{R}^\pi
 \end{aligned} \tag{A.2}$$

A.2 Dynamic programming

Policy iteration algorithm

Algorithm A.1: Policy Iteration for estimating $\pi \sim \pi^*$

Input: π the policy to be evaluated; a small threshold θ which defines the accuracy of the estimation

- 1 Initialise $V(s) \forall s \in \mathcal{S}$ arbitrarily, except that $V(\text{terminal}) = 0$
- 2 $is_policy_stable \leftarrow true$
- 3 **repeat**
 - 4 **repeat** */
 - 5 $\Delta \leftarrow 0$
 - 6 **for each** $s \in \mathcal{S}$ **do**
 - 7 $v \leftarrow V(s)$
 - 8 $V(s) \leftarrow \sum_{a \in \mathcal{A}} \pi(a|s) \sum_{s' \in \mathcal{S}, r \in \mathcal{R}} P(s', r|s, a) [r + \gamma V(s')]$
 - 9 $\Delta \leftarrow \max(\Delta, |v - V(s)|)$
 - 10 **end**
 - 11 **until** $\Delta < \theta$
 - 12 $V_\pi \leftarrow V(s)$
 - 13 **while** $true$ **do** */
 - 14 **for each** $s \in \mathcal{S}$ **do**
 - 15 $old_action \leftarrow \pi(s)$
 - 16 $\pi(s) \leftarrow \arg \max_a \sum_{s' \in \mathcal{S}, r \in \mathcal{R}} P(s', r|s, a) [r + \gamma V_\pi(s')]$
 - 17 **if** $old_action \neq \pi(s)$ **then**
 - 18 $is_policy_stable \leftarrow false$
 - 19 **end**
 - 20 **end**
 - 21 **end**
 - 22 **until** $\neg is_policy_stable$

Output: V^* and π^*

Policy improvement theorem

Let π and π' be any pair of deterministic policy such that

$$Q_\pi(s, \pi'(s)) \geq V_\pi(s) \forall s \in \mathcal{S} \quad (\text{A.3})$$

Then the policy π' leads to

$$V'_\pi(s) \geq V_\pi(s) \quad (\text{A.4})$$

Therefore, the presence of strict inequality in eq. (A.3) on the preceding page for a state leads to a strict inequality of eq. (A.4).

The proof of this theorem is shown in eq. (A.5).

$$\begin{aligned}
 V_\pi(s) &\leq Q_\pi(s, \pi'(s)) \\
 &= \mathbb{E}[r_{t+1} + \gamma V_\pi(s_{t+1}) | s_t = s, a_t = \pi'(s)] \\
 &= \mathbb{E}_{\pi'}[r_{t+1} + \gamma V_\pi(s_{t+1}) | s_t = s] \\
 &\leq \mathbb{E}_{\pi'}[r_{t+1} + \gamma Q_\pi(s_{t+1}, \pi'(s_{t+1})) | s_t = s] \quad (\text{by A.3}) \\
 &= \mathbb{E}_{\pi'}[r_{t+1} + \gamma \mathbb{E}_{\pi'}[r_{t+2} + \gamma V_\pi(s_{t+2}) | s_{t+1}, a_{t+1} = \pi'(s_{t+1})] | s_t = s] \\
 &= \mathbb{E}_{\pi'}[r_{t+1} + \gamma r_{t+2} + \gamma^2 V_\pi(s_{t+2}) | s_t = s] \\
 &\leq \mathbb{E}_{\pi'}[r_{t+1} + \gamma r_{t+2} + \gamma^2 r_{t+3} + \gamma^3 V_\pi(s_{t+3}) | s_t = s] \\
 &\vdots \\
 &\leq \mathbb{E}_{\pi'}[r_{t+1} + \gamma r_{t+2} + \gamma^2 r_{t+3} + \gamma^3 r_{t+4} + \dots | s_t = s] \\
 &= v_{\pi'}(s)
 \end{aligned} \quad (\text{A.5})$$

Value iteration algorithm

Algorithm A.2: Value Iteration, for estimating $\pi \sim \pi^*$

Input: A small threshold θ which defines the accuracy of the estimation

- 1 Initialise $V(s) \forall s \in \mathcal{S}$ arbitrarily, except that $V(\text{terminal}) = 0$
- 2 **repeat**
- 3 $\Delta \leftarrow 0$
- 4 **for each** $s \in \mathcal{S}$ **do**
- 5 $v \leftarrow V(s)$
- 6 $V(s) \leftarrow \max_a \sum_{s' \in \mathcal{S}, r \in \mathcal{R}} P(s', r | s, a) [r + \gamma V(s')]$
- 7 $\Delta \leftarrow \max(\Delta, |v - V(s)|)$
- 8 **end**
- 9 **until** $\Delta < \theta$
- 10 Output a deterministic policy, $\pi \sim \pi^*$, such that

$$\pi(s) = \arg \max_a \sum_{s' \in \mathcal{S}, r \in \mathcal{R}} P(s', r | s, a) [r + \gamma V(s')]$$

Output: V^* and π^*

Bibliography

- [1] ABADI, M., AGARWAL, A., BARHAM, P., BREVDO, E., CHEN, Z., CITRO, C., CORRADO, G. S., DAVIS, A., DEAN, J., DEVIN, M., ET AL. Tensorflow: Large-scale machine learning on heterogeneous distributed systems. *arXiv preprint arXiv:1603.04467* (2016).
- [2] BADRINARAYANAN, V., KENDALL, A., AND CIPOLLA, R. Segnet: A deep convolutional encoder-decoder architecture for image segmentation. *IEEE transactions on pattern analysis and machine intelligence* 39, 12 (2017), 2481–2495.
- [3] BELLEMARE, M. G., NADDAF, Y., VENESS, J., AND BOWLING, M. The arcade learning environment: An evaluation platform for general agents. *Journal of Artificial Intelligence Research* 47 (2013), 253–279.
- [4] BELLMAN, R. E., AND DREYFUS, S. E. *Applied dynamic programming*, vol. 2050. Princeton university press, 2015.
- [5] BISHOP, C. M. *Pattern recognition and machine learning*. Springer, 2006.
- [6] BROCKMAN, G., CHEUNG, V., PETTERSSON, L., SCHNEIDER, J., SCHULMAN, J., TANG, J., AND ZAREMBA, W. Openai gym, 2016. *arXiv preprint arXiv:1606.01540* (2016).
- [7] CARNEGIE MELLON UNIVERSITY. 15-494/694: Cognitive robotics, 2019. <http://www.cs.cmu.edu/afs/cs/academic/class/15494-s17/>.
- [8] CHARAFEDDINE, M. Reinforcement Learning in the Wild and Lessons Learned, 2018. <https://link.medium.com/SRUZ24Itx4>.
- [9] DEISENROTH, M., AND RASMUSSEN, C. E. Pilco: A model-based and data-efficient approach to policy search. In *Proceedings of the 28th International Conference on machine learning (ICML-11)* (2011), pp. 465–472.
- [10] DENG, J., DONG, W., SOCHER, R., LI, L.-J., LI, K., AND FEI-FEI, L. Imagenet: A large-scale hierarchical image database. In *2009 IEEE conference on computer vision and pattern recognition* (2009), Ieee, pp. 248–255.

- [11] DUAN, Y., CHEN, X., HOUTHOOFT, R., SCHULMAN, J., AND ABBEEL, P. Benchmarking deep reinforcement learning for continuous control. In *International Conference on Machine Learning* (2016), pp. 1329–1338.
- [12] DUCHI, J., HAZAN, E., AND SINGER, Y. Adaptive subgradient methods for online learning and stochastic optimization. *Journal of Machine Learning Research* 12, Jul (2011), 2121–2159.
- [13] ERHAN, D., BENGIO, Y., COURVILLE, A., AND VINCENT, P. Visualizing higher-layer features of a deep network. *University of Montreal 1341*, 3 (2009), 1.
- [14] FOX, R., PAKMAN, A., AND TISHBY, N. Taming the noise in reinforcement learning via soft updates. *arXiv preprint arXiv:1512.08562* (2015).
- [15] FRANÇOIS-LAVET, V., HENDERSON, P., ISLAM, R., BELLEMARE, M. G., PINEAU, J., ET AL. An introduction to deep reinforcement learning. *Foundations and Trends® in Machine Learning* 11, 3-4 (2018), 219–354.
- [16] FUJIMOTO, S., VAN HOOF, H., AND MEGER, D. Addressing function approximation error in actor-critic methods. *arXiv preprint arXiv:1802.09477* (2018).
- [17] GLOROT, X., AND BENGIO, Y. Understanding the difficulty of training deep feedforward neural networks. In *Proceedings of the thirteenth international conference on artificial intelligence and statistics* (2010), pp. 249–256.
- [18] GU, S., HOLLY, E., LILICRAP, T., AND LEVINE, S. Deep reinforcement learning for robotic manipulation with asynchronous off-policy updates. In *2017 IEEE international conference on robotics and automation (ICRA)* (2017), IEEE, pp. 3389–3396.
- [19] HAARNOJA, T., TANG, H., ABBEEL, P., AND LEVINE, S. Reinforcement learning with deep energy-based policies. In *Proceedings of the 34th International Conference on Machine Learning-Volume 70* (2017), JMLR. org, pp. 1352–1361.
- [20] HAARNOJA, T., ZHOU, A., ABBEEL, P., AND LEVINE, S. Soft actor-critic: Off-policy maximum entropy deep reinforcement learning with a stochastic actor. *arXiv preprint arXiv:1801.01290* (2018).
- [21] HAARNOJA, T., ZHOU, A., HARTIKAINEN, K., TUCKER, G., HA, S., TAN, J., KUMAR, V., ZHU, H., GUPTA, A., ABBEEL, P., ET AL. Soft actor-critic algorithms and applications. *arXiv preprint arXiv:1812.05905* (2018).

- [22] HASSELT, H. V. Double q-learning. In *Advances in Neural Information Processing Systems 23*, J. D. Lafferty, C. K. I. Williams, J. Shawe-Taylor, R. S. Zemel, and A. Culotta, Eds. Curran Associates, Inc., 2010, pp. 2613–2621.
- [23] HAWKE, J., SHEN, R., GURAU, C., SHARMA, S., REDA, D., NIKOLOV, N., MAZUR, P., MICKLETHWAITE, S., GRIFFITHS, N., SHAH, A., ET AL. Urban driving with conditional imitation learning. *arXiv preprint arXiv:1912.00177* (2019).
- [24] HENDERSON, P., ISLAM, R., BACHMAN, P., PINEAU, J., PRECUP, D., AND MEGER, D. Deep reinforcement learning that matters. In *Thirty-Second AAAI Conference on Artificial Intelligence* (2018).
- [25] HESSEL, M., MODAYIL, J., VAN HASSELT, H., SCHAUL, T., OSTROVSKI, G., DABNEY, W., HORGAN, D., PIOT, B., AZAR, M., AND SILVER, D. Rainbow: Combining improvements in deep reinforcement learning. In *Thirty-Second AAAI Conference on Artificial Intelligence* (2018).
- [26] HUVAL, B., WANG, T., TANDON, S., KISKE, J., SONG, W., PAZHAYAMPALLIL, J., ANDRILUKA, M., RAJPURKAR, P., MIGIMATSU, T., CHENG-YUE, R., ET AL. An empirical evaluation of deep learning on highway driving. *arXiv preprint arXiv:1504.01716* (2015).
- [27] IOFFE, S., AND SZEGEDY, C. Batch normalization: Accelerating deep network training by reducing internal covariate shift. *arXiv preprint arXiv:1502.03167* (2015).
- [28] KENDALL, A. Now is the Time for Reinforcement Learning on Real Robots, 2019. https://alexgkendall.com/reinforcement_learning/now_is_the_time_for_reinforcement_learning_on_real_robots/.
- [29] KENDALL, A., HAWKE, J., JANZ, D., MAZUR, P., REDA, D., ALLEN, J.-M., LAM, V.-D., BEWLEY, A., AND SHAH, A. Learning to drive in a day. *arXiv preprint arXiv:1807.00412* (2018).
- [30] KENDALL, A., HAWKE, J., JANZ, D., MAZUR, P., REDA, D., ALLEN, J.-M., LAM, V.-D., BEWLEY, A., AND SHAH, A. Learning to drive in a day. In *2019 International Conference on Robotics and Automation (ICRA)* (2019), IEEE, pp. 8248–8254.
- [31] KINGMA, D. P., AND BA, J. Adam: A method for stochastic optimization. *arXiv preprint arXiv:1412.6980* (2014).
- [32] KINGMA, D. P., AND WELLING, M. Auto-encoding variational bayes. *arXiv preprint arXiv:1312.6114* (2013).

- [33] KONDA, V. R., AND TSITSIKLIS, J. N. Actor-critic algorithms. In *Advances in neural information processing systems* (2000), pp. 1008–1014.
- [34] KULLBACK, S. Information theory and statistics. Tech. rep., 1959.
- [35] KULLBACK, S., AND LEIBLER, R. A. On information and sufficiency. *The annals of mathematical statistics* 22, 1 (1951), 79–86.
- [36] KURAMA, V. PyTorch vs. TensorFlow: Which Framework Is Best for Your Deep Learning Project?, February 2019. <https://builtin.com/data-science/pytorch-vs-tensorflow>.
- [37] LAPAN, M. *Deep Reinforcement Learning Hands-On: Apply modern RL methods, with deep Q-networks, value iteration, policy gradients, TRPO, AlphaGo Zero and more*. Packt Publishing Ltd, 2018.
- [38] LECUN, Y., BENGIO, Y., ET AL. Convolutional networks for images, speech, and time series. *The handbook of brain theory and neural networks* 3361, 10 (1995), 1995.
- [39] LECUN, Y., BENGIO, Y., AND HINTON, G. Deep learning. *nature* 521, 7553 (2015), 436.
- [40] LECUN, Y., BOTTOU, L., BENGIO, Y., HAFFNER, P., ET AL. Gradient-based learning applied to document recognition. *Proceedings of the IEEE* 86, 11 (1998), 2278–2324.
- [41] LILICRAP, T. P., HUNT, J. J., PRITZEL, A., HEESS, N., EREZ, T., TASSA, Y., SILVER, D., AND WIERSTRA, D. Continuous control with deep reinforcement learning. *arXiv preprint arXiv:1509.02971* (2015).
- [42] LIN, L.-J. Self-improving reactive agents based on reinforcement learning, planning and teaching. *Machine learning* 8, 3-4 (1992), 293–321.
- [43] MNIH, V., BADIA, A. P., MIRZA, M., GRAVES, A., LILICRAP, T., HARLEY, T., SILVER, D., AND KAVUKCUOGLU, K. Asynchronous methods for deep reinforcement learning. In *International conference on machine learning* (2016), pp. 1928–1937.
- [44] MNIH, V., KAVUKCUOGLU, K., SILVER, D., GRAVES, A., ANTONOGLU, I., WIERSTRA, D., AND RIEDMILLER, M. Playing atari with deep reinforcement learning. *arXiv preprint arXiv:1312.5602* (2013).
- [45] MNIH, V., KAVUKCUOGLU, K., SILVER, D., RUSU, A. A., VENESS, J., BELLEMARE, M. G., GRAVES, A., RIEDMILLER, M., FIDJELAND, A. K., OSTROVSKI, G., ET AL. Human-level control through deep reinforcement learning. *Nature* 518, 7540 (2015), 529.

- [46] OPENAI. OpenAI Five, 2018. <https://openai.com/blog/openai-five/>.
- [47] OPENAI. How to train your OpenAI Five, 2019. <https://openai.com/blog/how-to-train-your-openai-five/>.
- [48] OPENAI. OpenAI Spinning Up, 2019. <https://spinningup.openai.com/en/latest/>.
- [49] ORT, T., PAULL, L., AND RUS, D. Autonomous vehicle navigation in rural environments without detailed prior maps. In *2018 IEEE International Conference on Robotics and Automation (ICRA)* (2018), IEEE, pp. 2040–2047.
- [50] PASZKE, A., GROSS, S., CHINTALA, S., CHANAN, G., YANG, E., DEVITO, Z., LIN, Z., DESMAISON, A., ANTIGA, L., AND LERER, A. Automatic differentiation in pytorch.
- [51] PLAPPERT, M., ANDRYCHOWICZ, M., RAY, A., MCGREW, B., BAKER, B., POWELL, G., SCHNEIDER, J., TOBIN, J., CHOCIEJ, M., WELINDER, P., KUMAR, V., AND ZAREMBA, W. Ingredients for robotics research, February 2018. <https://openai.com/blog/ingredients-for-robotics-research/>.
- [52] RAFFIN, A. Learning to Drive Smoothly in Minutes, January 2019. <https://towardsdatascience.com/learning-to-drive-smoothly-in-minutes-450a7cdb35f4>.
- [53] RAWLIK, K., TOUSSAINT, M., AND VIJAYAKUMAR, S. On stochastic optimal control and reinforcement learning by approximate inference. In *Twenty-Third International Joint Conference on Artificial Intelligence* (2013).
- [54] RESEARCH, B. A. I. Soft actor critic—deep reinforcement learning with real-world robots, 2018. <https://bair.berkeley.edu/blog/2018/12/14/sac/>.
- [55] REZENDE, D. J., MOHAMED, S., AND WIERSTRA, D. Stochastic backpropagation and approximate inference in deep generative models. *arXiv preprint arXiv:1401.4082* (2014).
- [56] RUMELHART, D. E., HINTON, G. E., WILLIAMS, R. J., ET AL. Learning representations by back-propagating errors. *Cognitive modeling* 5, 3 (1988), 1.
- [57] SCHAUL, T., QUAN, J., ANTONOGLU, I., AND SILVER, D. Prioritized experience replay. *arXiv preprint arXiv:1511.05952* (2015).
- [58] SCHULMAN, J., WOLSKI, F., DHARIWAL, P., RADFORD, A., AND KLIMOV, O. Proximal policy optimization algorithms. *arXiv preprint arXiv:1707.06347* (2017).

- [59] SHALEV-SHWARTZ, S., AND BEN-DAVID, S. *Understanding machine learning: From theory to algorithms*. Cambridge university press, 2014.
- [60] SILVER, D. University College London Course on Reinforcement Learning. <http://www0.cs.ucl.ac.uk/staff/d.silver/web/Teaching.html>, 2015.
- [61] SILVER, D., HUANG, A., MADDISON, C. J., GUEZ, A., SIFRE, L., VAN DEN DRIESSCHE, G., SCHRITTWIESER, J., ANTONOGLU, I., PANNEER-SHELVAM, V., LANCTOT, M., ET AL. Mastering the game of go with deep neural networks and tree search. *nature* 529, 7587 (2016), 484.
- [62] SILVER, D., HUBERT, T., SCHRITTWIESER, J., ANTONOGLU, I., LAI, M., GUEZ, A., LANCTOT, M., SIFRE, L., KUMARAN, D., GRAEPEL, T., ET AL. Mastering chess and shogi by self-play with a general reinforcement learning algorithm. *arXiv preprint arXiv:1712.01815* (2017).
- [63] SILVER, D., LEVER, G., HEESS, N., DEGRIS, T., WIERSTRA, D., AND RIEDMILLER, M. Deterministic policy gradient algorithms.
- [64] SPRINGENBERG, J. T., DOSOVITSKIY, A., BROX, T., AND RIEDMILLER, M. Striving for simplicity: The all convolutional net. *arXiv preprint arXiv:1412.6806* (2014).
- [65] STANFORD UNIVERSITY. CS231n: Convolutional neural networks for visual recognition, 2019. <http://cs231n.github.io/>.
- [66] SUTTON, R. S., AND BARTO, A. G. *Reinforcement learning: An introduction*. MIT press, 2018.
- [67] TIELEMAN, T., AND HINTON, G. Lecture 6.5-rmsprop: Divide the gradient by a running average of its recent magnitude. *COURSERA: Neural networks for machine learning* 4, 2 (2012), 26–31.
- [68] TODOROV, E., EREZ, T., AND TASSA, Y. Mujoco: A physics engine for model-based control. In *2012 IEEE/RSJ International Conference on Intelligent Robots and Systems* (2012), IEEE, pp. 5026–5033.
- [69] TOURETZKY, D. Cozmopedia Wiki, 2018. <https://github.com/touretzkyds/cozmopedia/wiki>.
- [70] TOUSSAINT, M. Robot trajectory optimization using approximate inference. In *Proceedings of the 26th annual international conference on machine learning* (2009), ACM, pp. 1049–1056.
- [71] UHLENBECK, G. E., AND ORNSTEIN, L. S. On the theory of the brownian motion. *Physical review* 36, 5 (1930), 823.

- [72] VAN HASSELT, H., GUEZ, A., AND SILVER, D. Deep reinforcement learning with double q-learning. In *Thirtieth AAAI conference on artificial intelligence* (2016).
- [73] WANG, Z., SCHAU, T., HESSEL, M., VAN HASSELT, H., LANCTOT, M., AND DE FREITAS, N. Dueling network architectures for deep reinforcement learning. *arXiv preprint arXiv:1511.06581* (2015).
- [74] WATKINS, C. J. C. H. Learning from delayed rewards.
- [75] WAYVE. Learned urban driving, December 2019. <https://wayve.ai/blog/learned-urban-driving>.
- [76] WAYVE. Learning to drive like a human, April 2019. <https://wayve.ai/blog/driving-like-human>.
- [77] ZIEBART, B. D., MAAS, A., BAGNELL, J. A., AND DEY, A. K. Maximum entropy inverse reinforcement learning.