Doctoral Symposium

EPIA 2022
21st EPIA Conference on Artificial Intelligence

August 31, 2022
Instituto Superior Técnico, Lisbon, Portugal
Organizers

Fernando P. Santos  
*Informatics Institute, University of Amsterdam, Netherlands*

Henrique Lopes Cardoso  
*Faculty of Engineering of the University of Porto*

João Sacramento  
*Institute of Neuroinformatics, ETH Zürich, Switzerland*
Program Committee

Alberto Fernandez  
*University Rey Juan Carlos, Spain*

Hugo Gonçalo Oliveira  
*CISUC, University of Coimbra, Portugal*

Alberto Simões  
*Polytechnic Institute of Cávado and Ave, Portugal*

Ilaria Torre  
*KTH Royal Institute of Technology, Sweden*

Ana L. C. Bazzan  
*Federal University of Rio Grande do Sul, Brazil*

Irene Rodrigues  
*University of Évora, Portugal*

Andreia Sofia Teixeira  
*University of Lisbon, Portugal*

João Fabro  
*UTFPR, Federal University of Technology-Parana, Brazil*

António Branco  
*University of Lisbon, Portugal*

Juan Pavón  
*Complutense University of Madrid, Spain*

Filipa Correia  
*ITI-LARSyS, University of Lisbon, Portugal*

Renata Vieira  
*University of Évora, Portugal*

Flavio Pinheiro  
*NOVA IMS, Universidade NOVA de Lisboa, Portugal*

Susana Vinga  
*University of Lisbon, Portugal*
Mentors

Alberto Fernández  
*University Rey Juan Carlos, Spain*

Carlos Martinho  
*University of Lisbon, Portugal*

Alberto Sardinha  
*University of Lisbon, Portugal*

Catarina Silva  
*University of Coimbra, Portugal*

André de Carvalho  
*University of São Paulo, Brazil*

Isabel Trancoso  
*University of Lisbon, Portugal*

André F. T. Martins  
*University of Lisbon, Portugal*

João Gama  
*University of Porto, Portugal*

Andreia Sofia Teixeira  
*University of Lisbon, Portugal*

Luís Correia  
*University of Lisbon, Portugal*

Brigida M. Faria  
*Polytechnic Institute of Porto, Portugal*

Luis Paulo Reis  
*University of Porto, Portugal*

Bruno Martins  
*University of Lisbon, Portugal*

Paulo Novais  
*University of Minho, Portugal*

Carlos Lisboa Bento  
*University of Coimbra, Portugal*

Pedro Faria  
*Polytechnic of Porto - School of Engineering, Portugal*
Accepted Submissions

Artificial Intelligence for Health

Tailoring Precision Medicine Treatments with Machine Learning for Skin Diseases  
*Ana Duarte*

Detecting life-threatening patterns in Point-of-care ECG using efficient memory and processor power  
*Francisco Bischoff*

Explainable Temporal Models for Prognosis of Chronic Diseases: a Clinical Decision Support System  
*João Miguel Alves*

Improving the Robustness of Multimodal AI with Asynchronous and Missing Inputs  
*Ricardo Santos*

Humans and Artificial Intelligence

Adapting Behaviour Based On Trust In Human-Agent Ad Hoc Teamwork  
*Ana Carrasco*

Allocation of Compliance Responsibilities in Artificial Intelligence Lifecycle  
*Ana Paula Gonzalez Torres*

Methods for Urban Data Analysis: Towards Safety and Inclusiveness  
*Cláudia Rodrigues*

Theoretical Learning Creators and Creative Scientists  
*Luís Espírito Santo*

Multi-Agent Systems and Reinforcement Learning

Data Trading and Negotiation in Multi-Agent Systems  
*Hajar Bagcheband*
Reputation-based cooperation with private information
Henrique Correia da Fonseca

Artificial intelligence for zero-defect manufacturing in laser-based processes
João Sousa

Offline RL: Towards a wider application of RL methods in real-world domains
Pedro Santos

Natural Language Processing

Paraphrase Generation with Meaning Representations
Afonso Sousa

Biomedical Information Extraction in Domain-Specific Texts
André Gonçalves

Machine Translation for Emakhuwa of Mozambique
Felermino Ali

Automatic Dialogue Flow Extraction and Guidance
Patrícia Ferreira
Artificial Intelligence for Health
Tailoring Precision Medicine Treatments with Machine Learning for Skin Diseases

Ana Duarte

Abstract. The progressive decrease in the cost of sequencing the human genome has contributed to the development of precision medicine. In this field, the application of machine learning techniques to genomic data enables the identification of genetic profiles. These genetic profiles can then be used to personalise the diagnosis and/or treatment of groups of patients. Despite its increasing application, precision medicine is still at an early stage and further studies are needed in this area. The main objective of the research is to determine the specific time that maximizes the effectiveness of dermatological therapies depending on the profile of each patient. To this end, machine learning techniques will be used to support the development of a system capable of reflecting the need for specific treatments for a given patient at a given time.

Keywords: Precision Medicine, Biomarker, Machine Learning, Genome.

1 Introduction

Patients do not respond in the same way to the same treatments. Therefore, the paradigm of medicine based on a traditional “one size fits all” approach is gradually being replaced by a “tailored” approach [1]. This means that, instead of prescribing a universal treatment for the same diagnosis, we are now moving towards “tailored” treatments, that take into account the specificities of each patient. In fact, the basis of precision medicine is to adapt therapies to the patient’s profile, considering the genetic, environmental and lifestyle information. Greater personalisation of treatment allows patients to receive the right prescription at the right time, that maximizing efficacy and minimizing risks and costs [2].

Inflammatory skin diseases are among the medical areas that can benefit most from the use of a personalised approach. Typically, glucocorticoids are prescribed to treat most of these diseases. However, these drugs are not suitable for large areas of skin covered by lesions and have some significant adverse effects such as bone and cardiovascular toxicity [3, 4]. Recently, biological alternatives have emerged, using biologic drugs that allow for more targeted therapy. Biological drugs can be used to block and neutralise specific parts of the immune system to combat the inflammatory processes associated with autoimmune diseases [5, 6].

1 Advisor: Professor Orlando Belo (obelo@di.uminho.pt), ALGORITMI R&D Centre, University of Minho, Campus of Gualtar, 4710-057 Braga

This work has been supported by FCT – Fundação para a Ciência e Tecnologia within the R&D Units Project Scope: UIDB/00319/2020.
In the event that biological treatments do not produce the expected results, one of the most common approaches in medical practise is a “trial and error” process. This means that after a biological medicine is prescribed, its effectiveness is tested and if the therapy does not produce the expected effect, a new medicine is prescribed. These steps are constantly repeated until a successful result is achieved [7, 8].

Biomarkers play a fundamental role to overcome the limitations of such approach. They refer to objectively measurable characteristics of patients that can be used to assess the normality of their biological and pathogenic processes as well as their pharmacological responses to a particular therapy [9]. Thus, biomarkers allow for patients to be grouped according to their individual characteristics and, consequently, medical care can be adapted to the patients’ profile.

Due to the development of human genome sequencing in the field of precision medicine, biomarkers linked to omics data have gained more importance. This type of data has the potential to contribute significantly to the development of precision medicine, especially when dealing with diseases with a strong hereditary component such as cancer or other even more heterogeneous and complex diseases. Machine learning techniques are one of the fastest and most effective ways to turn this data into knowledge. Unlike conventional techniques, machine learning algorithms allow complex interactions to be taken into account and are particularly useful for biomarker selection and disease diagnosis and prognosis. Some of the most commonly used techniques for analysing omics data are k-Nearest Neighbours, Random Forest, Support Vector Machine, Naïve Bayes and Linear Regression, just to name a few.

2 State of the Art

The studies conducted in the field of precision medicine were largely motivated by the launch of the Precision Medicine Initiative programme in 2015. The main goal of this initiative was to promote more individualised medical practise by collecting data regarding clinical records, genetic profiles, environmental conditions, and lifestyle, from a cohort of American volunteers. In addition to the US, other countries have also invested in precision medicine. For example, in 2018, the UK started to include whole genome sequencing in routine care in order to collect over 5 million human genomes.

In dermatology specifically, there are already some studies in the field of precision medicine. For example, in [10], for example, the Random Forest technique was used to quantify the influence of genes on the onset of Systemic Lupus Erythematosus (SLE). As a result, the authors discovered 15 new risk genes and created a model that can identify about 70% of patients with SLE who will develop renal lupus. If applied before the onset of symptoms, this prediction allows early treatment of patients at increased risk.

In other autoimmune diseases, IFNβ is one of the most popular biologic drugs used to treat multiple sclerosis. However, 35% of patients treated with IFNβ develop neutralising antibodies, which reduce the efficacy of the medicine. In [11], it was found that some serum metabolites can act as biomarkers for predicting patients who will develop neutralising antibodies to IFNβ treatment. In this example, the authors used some machine learning techniques to identify biomarkers. They demonstrated that in
this case a traditional trial-and-error approach could be replaced by personalised treatments [7, 12, 13].

To determine the risk of developing comorbidities, L. Coelewijn et al. [14] conducted a study aimed at identifying patients with a high likelihood of developing cardiovascular disease. Using machine learning techniques, the researchers were able to establish a link between the presence of certain metabolites and the formation of atherosclerosis plaques.

In the field of medical image diagnosis, Y. Liu et al. [15] developed a Deep Learning system that can recognise 26 different dermatological diseases. In this study, dermatological images were used to build a convolutional neural network. The accuracy of the developed model was comparable to the accuracy of dermatologists.

The literature review in the field of precision medicine revealed that although some studies already exist in dermatology, they are few, especially at the level of disease identification and predictive biomarkers using machine learning techniques. Moreover, these studies do not usually examine Hispanics, so it is necessary to analyse populations that are genetically closer to the Portuguese population. Another important aspect in this context is the recent publication of the sequencing of the last 8% of the human genome [16]. This sequencing will require further studies, as it relates to areas of DNA for which data are not yet available, and represents an opportunity to contribute to the development of precision medicine.

3 Research Questions and Methodology

In order to contribute with relevant advances in precision medicine in the field of dermatology, the most important questions to be answered are:

- Question 1: Is it possible to identify different skin diseases and their severity from photographs showing skin lesions?
- Question 2: Are there biomarkers that clearly identify the predisposition to develop certain types of skin diseases?
- Question 3 – Is it possible to determine the most favourable time to take medication, given the patient profile, and the type and severity of the disease?

The proposed work is thus divided into several tasks, each with its own methodology. The first phase consists of using classified images to build a Deep Learning model capable of recognising different dermatological diseases and their severity. To achieve this goal, a methodology similar to the one described in [17] will be applied. In this work, the authors used images of patients with psoriasis, and extracted and selected the most relevant features of those images.

Next, it is planned to develop a new model to identify patient profiles by integrating different data including genomic and proteomic features. The methodology for conducting this second phase is the Cross Industry Standard Process for Data Mining.

Subsequently, based on the models created in the previous phases, risk indexes will be created to track the evolution of a particular disease over time and to indicate the most appropriate time for a patient to take medication. The methodology to be followed in this last phase is identical to the approach described in the previous phase.
References


Detecting life-threatening patterns in Point-of-care ECG using efficient memory and processor power

Francisco Bischoff

1 Department of Community Medicine, Information and Health Decision Sciences (MEDCIDS), Faculty of Medicine, University of Porto, Porto, Portugal

Abstract. Currently, Point-of-Care (POC) ECG monitoring works either as plot devices or alarms for abnormal cardiac rhythms using predefined normal trigger ranges. Great effort has been made to improve the accuracy of such monitoring, but in the ICU setting. Thinking outside the ICU setting, where high-end devices are available, we aim to identify, on streaming data, life-threatening heart electric patterns using low CPU and memory, enabling ward monitors, home devices, and even wearable devices to be able to identify such events.

Keywords: anomaly detection · ECG · matrix profile · time series · point-of-care

1 Introduction

Currently, Point-of-Care (POC) ECG monitoring works either as plot devices or alarms for abnormal cardiac rhythms using predefined normal trigger ranges. Modern devices also incorporate algorithms to analyze arrhythmias improving their specificity. On the other hand, full 12-derivation ECG machines are complex, are not suited to use as simple monitors and are used with strict techniques for formal diagnostics of hearth electric conduction pathologies. The automatic diagnostics are derived from a complete analysis of the 12-dimension data after it is fully and well collected.

In February 2015, the CinC/Physionet Challenge 2015 was about “Reducing False Arrhythmia Alarms in the ICU” [4]. The introduction article stated that it had been reported that up to 86% of the alarms are false, which can lead to decreased staff attention and an increase in patients’ delirium [3, 12, 15].

This subject highlights the importance of correctly identifying abnormal hearth electric patterns. Meanwhile, this opens the opportunity of thinking outside the ICU setting, where we still monitor patients (and ourselves) using devices with low processing power, such as ward monitors, home devices, and wearable devices.

* Supervisor: Professor Pedro Pereira Rodrigues (MEDCIDS, Porto), co-supervisor: Professor Eamonn Keogh (UCR, Riverside)
2 Objectives and research question

While this research was inspired by the Physionet’s challenge, its purpose is not to beat the state-of-the-art on that challenge but to identify, on streaming data, abnormal heart electric patterns, specifically those which are life-threatening, using low CPU and low memory requirements.

The main question is: can we accomplish this objective using a minimalist approach (low CPU, low memory) while maintaining robustness?

3 Related Works

The Physionet’s challenge yielded several papers on the subject [5, 7, 10, 11, 16]. However, independently of their approach to this problem, none of the authors reported benchmarks, memory usage, robustness test, or context invariance that could assure its implementation in smaller devices.

4 Planned approach

4.1 Dataset

The dataset used is the CinC/Physionet Challenge 2015 public dataset [4], composed of 750 patients with at least five minutes records. The events we seek to identify are the life-threatening arrhythmias as defined by Physionet’s challenge [4].

4.2 Matrix Profile

This work will use the state-of-the-art [6, 8] time series analysis technique called Matrix Profile (MP) that, once computed, allows us to derive frameworks for all sorts of tasks, such as motif discovery, anomaly detection, regime change detection, and others [18]. The MP is known to be an incredible fast algorithm [9, 13], thus viewing on the other side (not to process billions of data points using a desktop), it has a great potential to be used on small devices.

The streaming data coming from a patient is processed to create its MP in real-time. Then, the FLOSS algorithm [9] is computed to detect a regime change. When a new regime is detected, a sample of this new regime is analyzed by a model, and a decision is made. If the new regime is life-threatening, the alarm will be fired.

4.3 Detecting regime changes

The regime change detection will use the FLOSS algorithm [9], an online algorithm built on top of the computed MP. The algorithm is based on the assumption that between two regimes, the most similar shape (its nearest neighbor, 1-NN) is located on “the same side”. The details of the algorithm are described
in the original paper [9]. In short, the algorithm keeps track of the number of 1-NN references (called Arc Counts) that crosses a point in time. As shown in the original article, figures 2 and 3 [9], a drop in the Arc Counts indicates a regime change.

4.4 Classification of the new regime

The next step is verifying if the new regime detected is a life-threatening pattern. The aim is not to identify the exact type of the new regime but if it is life-threatening or not. The method of choice is a classification model using shapelets as signatures of such patterns. In this case, we will need to use a set of shapelet candidates, which maximize the classification performance.

Leveraging on the MP concept, we can use the Contrast Profile (CP) [14] to derive a set of shapelets candidates. The CP looks for patterns simultaneously very similar to its neighbors in class A while being very different from the nearest neighbor in class B.

For a complete understanding of the process, in the original article, figure 6 shows a practical example [14].

4.5 Validation

Both processes of detecting regime change and classification of the new regime has its own type of scoring. The extended details is available online [1]. The best parameters will be selected using nested resampling [2]. While the regime change will try to minimize the false negatives (keeping the false positives as low as possible), the classification model will try to eliminate the false positives.

4.6 Implementation

Later, this workflow will be experimented on a low-power device, such as an ESP32 microcontroller [17], to validate the concept and measure the performance and benchmarks.

5 Expected results and outcomes

Ultimately, this thesis will provide a framework for identifying life-threatening conditions using biological streaming data on devices with low CPU and memory specifications. We expect to achieve a high-quality model for identifying these pathological conditions while maintaining their robustness in the presence of noise and artifacts seen in real-world applications.
References


Explainable Temporal Models for Prognosis of Chronic Diseases: a Clinical Decision Support System

João Miguel Alves1,2
1 Department of Community Medicine, Information and Health Decision Sciences (MEDCIDS), Faculty of Medicine, University of Porto, Porto, Portugal
up199801351@edu.med.up.pt
2 CINTESS – Center for Health Technology and Services Research, Porto, Portugal

Abstract. Bayesian Network models have been used in clinical practice with increasing acceptance for disease prognosis. However, modelling long-term outcomes of chronic diseases requires taking in consideration its time varying element. This can be achieved by the use of Temporal or Dynamic Bayesian Networks, which have been applied in recent years with promising results for the prediction of long-term outcomes for several diseases. Nonetheless, Temporal or Dynamic Bayesian Networks, being an emergent methodology, are not yet extensively used in clinical practice. Scientific and academic developments are very sparsely available for use in clinical settings.

We hypothesize that for patients with a chronic disease, clinical decision making based on explainable temporal modelling would improve prognosis of long-term outcomes, when compared to standard clinical decision methods. The aim of this research is thus to contribute to the decision-making process of healthcare professionals handling chronic diseases, with support of explainable temporal models that can be used in a clinical setting.

To achieve the expected results, we will carry out a systematic review on temporal models used in clinical context. The research will then focus on developing and validating a data-driven temporal model, followed by the development of an application to be used in clinical settings to support clinical decision making on a chronic disease.

Keywords: Artificial Intelligence in Medicine · Clinical Decision Support Systems · Temporal Modelling · Dynamic Bayesian Networks

1 Introduction

Chronic diseases are a major cause of mortality and morbidity in developed countries, affecting approximately 1 in 3 adults globally [5]. Diseases such as cancer, chronic respiratory problems, diabetes, heart attack and stroke, are not
only leading causes of death, but also yield a high burden of disability amongst the living [14]. For an adequate management of long term conditions, focus should be on monitoring long-term outcomes to reduce recidivism and improve quality of life.

In recent years, several Artificial Intelligence (AI) technologies have been tested for the best diagnosis or prognosis results [7], and several models have been used to predict the risk of chronic diseases [15]. However, to be useful in medical practice, AI models must be able to produce human interpretable results [2,10]. Bayesian Networks (BN) are amongst the most widely used and accepted models applied in medical practice for disease prognosis [22], due to their robustness and easiness of interpretation by physicians [6]. Unfortunately, static models such as standard BNs fail to capture the dynamic nature of chronic diseases, which evolve throughout a long timespan. A potential workaround may be achieved with Temporal Bayesian Networks (TBN) [17], which have been applied to predict outcomes of several diseases [11] with promising results. It is thus a field in evolution worth receiving increased attention.

2 Background

BNs have been regarded as models of choice to be used in clinical settings for personalised decision-support systems [21], and evidence has been presented on its benefits for diagnosis and prognosis in several clinical conditions [3,8,4,19]. However, these models were not designed to handle the temporal reasoning required in the context of chronic disease management [1].

Recent efforts to incorporate temporal abstraction in Bayesian Networks seem to be setting the grounds to overcome this limitation [17]: Temporal Bayesian Networks (TBN) were first introduced by Tawfik in 1994 [20], to which Dynamic Bayesian Networks (DBN) followed as a way to model dynamic systems [12]. In 2002, Noldeman et al. [13] presented a new modelling language for Continuous-time Bayesian Networks, and in 2012 Ramati developed a further adaptation to the irregular time nature of available data [18] thus introducing the concept of Irregular-time Bayesian networks. Both continuous and discrete time modelling have been combined in 2017 by Liu et al. in a novel class of models called Hybrid-time Bayesian Networks [9], which can incorporate multiple frequencies of time abstractions in Bayesian Networks.

We propose to continue previous efforts [16] to the decision-making process of healthcare professionals, now adding temporal abstraction to disease modelling.

3 Methods

This project aims to answer the following research question: In patients with a chronic disease, how does clinical decision-making based on data-driven explainable temporal modelling, compared to standard clinical decision methods, improve prognosis of long-term outcomes. To answer this question, we will pursue the studies described below.
3.1 Study 1 – Systematic Review

The first step will be a Systematic Review, to assess what temporal or dynamic models based on Bayesian Networks (BN) have been used in a healthcare context. More specifically, we aim to assess which of those models can be used to prognose the evolution and outcomes of a chronic disease.

Studies will be selected to meet as inclusion criteria: i) reference to Temporal or Dynamic Bayesian Networks, and ii) reference to health, medical or clinical context. No exclusion criteria have been defined, nor the search will be bound to any specific study design or date limits.

3.2 Study 2 – Model development and validation

The next step will aim to develop and validate an explainable temporal model to be used as clinical decision support system for a single chronic disease. We will conduct a cohort study for a given chronic disease throughout nine months. A set of patients will have their clinical data retrospectively analysed to train the model, while being prospectively followed to validate the proposed model. Participants inclusion criteria are i) patients with the chronic disease in study, ii) being followed in a healthcare institution, iii) for which there is retrospective clinical data for a minimum of 1 year with multiple observations along that period. Data points to be collected will carry a timestamp, and variables of interest consist of patient information (anonymised ID code, age, sex), as well as any variables pertaining to the chronic disease in study, and its related risk factors (diagnosis, symptoms, medication, medical exams results, clinical analysis values, etc.).

We will gauge the model’s prognosis accuracy along the duration of the study as we collect additional data on the evolution of each patient’s condition.

3.3 Study 3 – Proof of concept

Finally, the last step will aim to apply the previously validated model to a real case clinical setting. This step will comprise the development of an application, driven by a temporal statistical model on expected outcomes of the chronic disease in study, linked to a user interface (UI) to be operated by a physician during clinical practice. The envisioned application will provide support to clinical decision making based on the most probable evolution of the disease for each given patient, namely regarding most probable further complications, potential relapses, and expected improvements with medication or surgery.

3.4 Expected results

With this project, we expect to have a validated prognosis tool composed of a graphic user interface powered by a temporal probabilistic model. This tool is expected to be made available to be used in clinical settings as a clinical decision support system for the prediction of long-term outcomes in a chronic disease.
References


Explainable Temporal Models for Prognosis of Chronic Diseases

Improving the Robustness of Multimodal AI with Asynchronous and Missing Inputs

Ricardo Santos\textsuperscript{1,2,*}

\textsuperscript{1} Physics Department, NOVA School of Science and Technology, Lisbon, Portugal
\textsuperscript{2} Associação Fraunhofer Portugal Research, Porto, Portugal

Abstract. Delivering Decision Support Systems (DSS) to clinical environments is not an easy task. In healthcare contexts, the data generated by a single patient is immense. Laboratory tests, exams and clinical notes describe different physiological processes and are structurally distinct. Furthermore, these are collected in asynchronous moments throughout the patient journey and based on specific decisions. Current Artificial Intelligence (AI) algorithms cannot consider this gamut of possible scenarios. The developed DSSs are either particular to a specific task and data type or are hardly deployable and generalisable to real-world settings. This thesis proposes to study how to deliver robust AI-based solutions to the healthcare context, considering from a data-centric perspective the high variability of available data at each prediction moment, the distinct patient history, and the need for longitudinal evaluations. For this purpose, this work will focus on multimodality, considering that some inputs may be missing and collected asynchronously, while acknowledging the need for trustworthy estimations.

Keywords: Machine Learning · Multimodality · Temporality · Missing data · Healthcare.

1 Introduction

Revolutions in healthcare improved the quality of life with new diagnostic techniques and more successful treatments. The consequent ageing of the population brings new challenges related to increased costs and a lack of human resources to process all generated information \cite{10}. In this sense, Artificial Intelligence-based (AI) Decision Support Systems (DSS) promise to help with tools to automatically identify diseases and personalised treatments, among other tasks.

Despite the efforts, current algorithms have restrictive limitations that hinder their wide deployment and adoption. In specific tasks, such as medical image evaluation, Machine Learning (ML) and Deep Learning (DL) models attain performances comparable to human specialists \cite{7}. Although some point out interpretability and trust concerns, new approaches have been proposed to overcome the "black-box” mechanisms of some algorithms \cite{5}. However, these models hardly deal with broader tasks, common in clinical contexts.

* Advisors: Prof. Dr. Hugo Gamboa\textsuperscript{1,2} and Dr. André Carreiro\textsuperscript{2}
Throughout life, a person visits a doctor’s office multiple times. During this period, laboratory analyses, exams, and clinical notes, among other information, are collected, stored, and used in every assessment. In the same way that physiological processes are complex and need to be evaluated by clinicians through multiple sources across time, AI models should also be able to leverage all available information for an estimation. Multimodal solutions exist, but usually consider fixed inputs or resort to simple fusion processes. This may lead to poor performance and data waste in dynamic clinical contexts.

Also, some diseases develop over longer periods. Historical data helps clinicians understand the disease progression, ideally before any symptoms appear. Similarly, AI models may leverage this continuity, although depending on particular snapshots, disregarding the variability of possible scenarios.

Following the identified limitations, we propose to study how to improve the robustness of AI-based DSSs following a data-centric perspective. We will focus on assuring that models can work with the information available at each time, both in terms of data modalities and considering the patient history while providing information about inference confidence. Clinical use cases are good examples of such variability, although the proposed research can be generalised to other domains. This work thus proceeds with the following research questions:

1. How can clinical DSSs become more robust when dealing with real-world multimodal data with missing inputs?
2. Do clinical DSSs inferences improve when leveraging non-fixed historical information?
3. Can techniques to deal with missing and temporal data improve trust on AI applied to healthcare?

2 Literature Review

Multimodality refers to the processing of multiple data modalities. These are generally structurally different and complementary [1]. Works on the topic often deal with the fusion of different clinical modalities, such as Electronic Health Records (EHR), clinical notes, laboratory analysis and a manifold of exams.

Huang et al. [3] presented a review of DL-based works for the fusion of medical images and EHR. Fusion techniques are split into three types: Late fusion, at the decision level; Early fusion, at the feature level; and Joint fusion, an intermediate approach where individual feature extraction and prediction are trained simultaneously, mostly applied in DL architectures.

Regarding temporality, Recurrent Neural Networks (RNN) are commonly used, as they include memory units to propagate past information across the network for comprehensive decision. Hugle et al. [4] proposed the AdaptiveNet, a Long-Short Term Memory-based (LSTM) network to model the probability of progression using a temporal window. Shi et al. [8] developed LSTM models with an attention mechanism to predict the patients’ risk of mortality leveraging temporal information, such as EHRs, demographic data and laboratory results.
On other perspective, joint models can be used to model longitudinal data with survival or time-to-event outcomes [9].

Such techniques do not account for the high variability of real clinical contexts, as different variables are not necessarily registered on every visit. Carreiro et al. [2] addressed this issue by creating temporal snapshots of clinical information to predict the time frame until patients with Amyotrophic Lateral Sclerosis need assistive ventilation.

The processing of multimodal inputs and temporal information are well-known problems in the AI domain. Nonetheless, when considering the variability of real-world healthcare contexts, such proposals are not robust to be widely accepted and deployed. Recent work of Ma et al. [6] acknowledged the need to account for severe missing data since training, proposing a Bayesian meta-learning framework for encoder-decoder schemes.

3 Methodology

We will give models ways to deal with the variability of real-world scenarios when making predictions, while assuring that users understand taken assumptions and the consequently reduced confidence. A data-centric perspective will be followed, as the proper information processing is the key to robust solutions.

This research fits the scope of a national research project, CardioFollow.AI, in which data from a Cardiothoracic surgery department is being processed. This database includes surgery and follow-up information from more than eight thousand patients collected over ten years. Furthermore, public databases may be used to extend and validate the developed algorithms, such as the Alzheimer’s Disease Neuroimaging Initiative, including multimodal and longitudinal data.

Initial work was centred on processing the cardiac surgery data, performing statistical evaluations between the variables and establishing a baseline solution to monitor the risk of post-surgery complications. Next, we will understand the impact of missing data on the model’s predictions and developing techniques to overcome such limitations. The generalisation to broader modalities and the use of longitudinal data and continuous predictions will then be studied.

Dynamic modality fusion techniques will be explored, considering the variability of inputs since training, possibly using adaptable weights in the multimodal and temporal dimensions. While in a perfect scenario a model may give some modality critical importance, if that one is missing the contribution hierarchy of the remaining may change. Consequently, although robustness increases, concerns about model confidence rise. We will study the impact of such dynamic weighting with uncertainty measures, to guarantee trustworthy and deployable outcomes. Although traditional ML models usually provide more interpretability features, DL techniques, such as RNN-based models, will also be studied to compare different solutions.

The outcomes of this thesis will be a set of tools or methodologies that may be used to develop not only clinical DSSs, but also in other learning tasks with similar variability features.
References

Humans and Artificial Intelligence
Adapting Behaviour Based On Trust In Human-Agent Ad Hoc Teamwork*

Ana Carrasco**
INEC-ID, Instituto Superior Técnico, University of Lisbon
Lisbon, Portugal
ana.carrasco@gaips.inesc-id.pt

Abstract. This work proposes a framework that incorporates trust in an ad hoc teamwork scenario with human-agent teams, where an agent must collaborate with a human to perform a task. During the task, the agent must infer, through interactions and observations, how much the human trusts it and adapt its behaviour to maximize the team’s performance. To achieve this, we propose collecting data from human participants in experiments to define different settings (based on trust levels) and learning optimal policies for each of them. Then, we create a module to infer the current setting (depending on the amount of trust). Finally, we validate this framework in a real-world scenario and analyse how this adaptable behaviour affects trust.

Keywords: Ad Hoc Teamwork · Trust · Human-Robot Interaction

1 Introduction

Ad Hoc Teamwork (AHT) [8] is a well-known research problem where an agent must be able to cooperate with a group of teammates (humans or agents), without any prior coordination or communication protocols. The AHT is characterized by three assumptions: the agent has no prior coordination or communication mechanisms established with its teammates, the agent has no control over the teammates and all teammates are assumed to have a common objective (or task) [5]. As defined by Melo and Sardinha [4], the AHT problem can be divided into three sub-tasks: identifying the common task, identifying the teammates and what they are doing and plan actions accordingly.

A review of the recent literature on the subject reveals that, as autonomous agents capabilities advance, human-robot collaboration scenarios become more

---

* This work was partially supported by national funds through FCT, Fundação para a Ciência e a Tecnologia, under project UIDB/50021/2020 (INESC-ID multi-annual funding) and the HOTSPOT project, with reference PTDC/CCI-COM/7203/2020. In addition, this material is based upon work supported by TAILOR, a project funded by EU Horizon 2020 research and innovation programme under GA N. 952215.

** The advisors of this work are: Ana Paiva (paiva.a@gmail.com), Alberto Sardinha (jose.alberto.sardinha@tecnico.ulisboa.pt), Francisco S. Melo(fmelo@inesc-id.pt)
common. We argue that AHT scenarios with human-agent teams are especially relevant, since they solve the problem of integrating an ad hoc agent in a team with a human, without requiring any prior experience with that human. However, very few works on AHT focus on teams with humans, and even fewer regard the human-agent trust dynamics. Ribeiro et al. [6] introduce a framework for AHT in human-robot teams, tackling two main challenges in human-robot collaboration: task-related challenges and communication challenges between robots and humans. This work builds on that by identifying and addressing the challenges raised by the trust dynamics between the human and the agent.

Trust in human-robot interaction is a well researched topic. Lee and See [3] and Schaefer [7] explore the impact of trust in human-robot interactions, how to model and measure it. These works argue that successful collaboration between humans and robots require appropriate levels of mutual trust, since that trust impacts the task performance. Chen et al. [1] introduce a computational model based on a POMDP that uses trust as a latent variable. This model allows a robot to infer the trust of a human and choose actions that maximize the long term performance. This model is validated through human participant experiments on a table-clearing task.

Inspired by these works, the goal of this work is to introduce a framework, in a real world AHT scenario, where the agent is able to infer how much the human trusts it and change the way it cooperates with the human. We hypothesize that the agent’s adaptable behaviour will not only improve task performance but also calibrate the amount of trust the human has on the agent.

2 Experimental Setup

The structure for the proposed framework is depicted in Figure 1.

![Fig. 1. Structure of the proposed framework.](image)

First, information on different settings, i.e., different models of human behaviour based on the level of trust they show towards the agent, is saved into a settings library. The agent then infers the current setting by combining this
information with observations from the environment and the teammate. It then updates a distribution of possible settings (beliefs), and uses these beliefs and the information about the setting to choose the best action to take.

To validate this framework, we propose a controlled experiment where human participants must complete a task with an agent. The structure of this experiment is inspired by the work of Ribeiro et al. [6] and Chen et al. [1]. In the work of Ribeiro et al. [6], the robot assists the human in a task that follows a set of rules under the Toxic Waste Domain. In this domain, the robot and the human must clean the toxic waste from a room. The human must pick up the waste and dispose of it while the robot’s role is to be the container where the waste is disposed of. Due to the toxicity of the waste, the human is penalized for the time holding the waste.

This work takes this scenario but adjusts the rules and the environment characteristics to add some risk related to trusting the agent. This allows for an assessment of the human’s trust in the agent (i.e., if and when that trust is higher or lower), similarly to what was done by Chen et al. [1]. In their work, the risk was associated with the robot dropping items, whereas in this experiment the risk is directly connected to time consumption. The experiment is timed, and the participant is penalized for taking longer to complete the task. Note that, despite the human’s perception, the robot is capable of executing its part of the task perfectly by itself. The performance of the team depends on how much the human trusts in the robot to execute the task in a reasonable time period. If implemented correctly, the robot’s adaptable behaviour will allow for an improvement on this performance, keeping up with the natural evolution of the human-robot trust dynamics.

The first stage of the study consists of gathering data regarding the behaviour of the participants when collaborating with the agent. This will allow us to choose the best way to measure trust levels and build the settings library to be used in the framework. In this first stage, the proposed experimental setup is tested virtually in an environment called Overcooked\textsuperscript{1}. In this scenario, we introduce elements like an "icy zone", where the agent’s navigation capabilities are decreased. The goal is to simulate some level of risk and create some level of uncertainty regarding the robot’s performance, which is an inherent trait in the real-world scenario, but might lack in the virtual one.

3 Future Work

Currently, the study is still in its early stages of modeling the experiment environment and gathering data. The next steps include exploring the best way to measure trust in the proposed scenario (whether subjectively, objectively or both [2]), in order to develop a trust inferring module; Compute optimal policies adequate for different levels of trust; Test the agent with adaptable behaviour in a real world scenario; Study the impact of the robot’s adaptable behaviour in trust, during and after the task.

\textsuperscript{1} https://github.com/HumanCompatibleAI/overcooked_ai
References

Allocation of Compliance Responsibilities in Artificial Intelligence Lifecycle

Ana Paula Gonzalez Torres

Doctoral Candidate, Aalto University, Konemiehentie 2, 02150, Espoo, Finland
ana.gonzaleztorres@aalto.fi

Abstract. This research examines how regulatory compliance responsibilities can be feasibly distributed among the parties involved in the development and deployment of AI systems for public sector services. In particular, we consider how to ensure ways of supporting compliance with the "AI Act" in adoptions of AI applications in public administration institutions by means of Artificial Intelligence as a Service (AIaaS) offered by private organisations.

Keywords: Regulation, Artificial Intelligence as a Service (AIaaS), Compliance, Public administration.

1 Introduction to the topic

Artificial Intelligence (AI) based systems are increasingly being adopted to provide digital public services. Nonetheless, it is often unclear who is accountable for ensuring their usage and operation correspond to the expectations of users and providers, as well as compliance with states goals and norms (such as fairness, non-discrimination, equity, etc.) The challenge of allocating compliance responsibilities lies in the opaque organisational structures involved in developing and deploying AI systems and the current unclear legal framework. Currently, under the proposed "AI Act", the distribution of requirements and obligations relies on the type of "operator", which encompasses "the provider, the user, the authorised representative, the importer, and the distributor"[1]. Meanwhile, in practice, the lifecycle of an AI system involves different parties with different roles, which tend to vary depending on the organisation and the use case. For instance, depending on the organisation at hand, the responsibility for overseeing the development of AI systems can belong to the “Chief AI Ethics Officer” or "Data Protection Officer" or flatly fall under the many tasks of the legal department. Thus, there is much uncertainty around the pertinent roles and their corresponding responsibilities through the AI lifecycle.

In particular, in the public sector, there is much desire to adopt AI applications. Still, often, there is a lack of trained, experienced and skilled professionals with sufficient expertise in developing AI-based systems. This has led to private and public

---

1 Nitin Sawhney, Professor of Practice, Aalto University, Department of Computer Science, Konemiehentie 2, Room B345, 02150 Espoo, Finland.
administration partnerships for developing digital public services based on AI systems. For instance, in some cases, private companies offer AI as a Service (AIaaS). The services are usually sold to customers by cloud services companies that possess the AI talent, data, and computing resources necessary to train AI systems. Through AIaaS, customers provide inputs and receive back the analyses' results through on-demand access to various AI-backed capabilities (e.g., object recognition, face detection, speech transcription) [14]. AIaaS are usually available 'turn-key,' meaning on demand at a relatively low cost. Nonetheless, some providers offer AI services on a consultancy basis, working closely with the customer to tailor pre-trained AI models to their specific needs. This service is usually reserved for higher-value customers, like public administration institutions [6].

The importance of understanding the roles and responsibilities through the AI lifecycle in partnerships between public and private organisations lies in the different legal standards and in the observation that, for certain services, citizens cannot “take their business elsewhere”. In AIaaS, even if the customer determines the resulting AI application, the results obtained from the AI service will directly influence the capabilities of an application's functionality [4]. In such regards, significant consequences can derive from Annex III of the proposed “AI Act”, which establishes as “high-risk” those AI systems employed in areas like "access to and enjoyment of essential private services and public services and benefits" or "administration of justice and democratic process"[2]. On the one hand, regardless of the initial purpose of the AIaaS providers, if they partner with public administrations in developing and deploying AI applications in certain domains, they could be regarded as enabling “high-risk” AI systems and thus be subject to higher compliance standards. On the other hand, if there is no organisational understanding of the allocation of responsibilities, AIaaS providers could provide “instructions of use” with implicit regulatory effects on the behaviour of public administrations or attempt to limit or nullify their compliance responsibilities while enabling various non-compliant and illegal AI applications used in offering public services.

This paper proposes that the distributions of compliance responsibilities related to AI applications should consider the organisational mechanisms and dynamics of the development and deployment of AI systems according to their context and nature of the parties involved.

2 Research questions

RQ1: How do different parties understand the rights, risks, and responsibilities of developing and deploying AI systems?

RQ2: How to effectively allocate regulatory compliance obligations between different parties involved in AI systems' life cycle in a way that increases trust?

RQ3: What can be considered a crisis, and how to distribute responsibilities for the faults in regulatory compliance during crises?

RQ4: Determine who should be responsible for enacting mitigation measures to minimise the risks involved in deploying AI systems in the public sector?
3 State of the art

For the most part, the literature has focused on reporting the use of AI systems in the public sector [1,11], how AI system’s outputs affect individuals and the responsibility of developers [3]. Sawhney (2022) proposed examining the rights, risks and responsibilities of all stakeholders and providers engaged in public urban AI systems [13].

Regarding the "AI Act", there are general examinations of its dispositions [5] and discussions around EU constitutional implications [15]. Meanwhile, the attempts to design models for compliance do not consider the intricacies that emerge in allocating responsibilities in private and public partnerships [6,10]. In terms of AIaaS, the literature has primarily focused on technical explanations of their architecture [9], potential tools for addressing misuse [8], and compliance with the GDPR and ECommerce Directive [4]. Thus, there is little practical work on how AIaaS should comply with the proposed "AI Act" scheme. Notably, comments to the proposed "AI Act" mention the need for clear distribution of regulatory obligations. Nonetheless, organisations are just starting to develop AI governance frameworks and ethical guidelines but still struggle to adopt solid policies given the uncertainty and variability of the legal framework and organisational structures in AI systems’ lifecycle and use cases.

4 Methodology

This research will undertake a mixed methods approach, using qualitative and quantitative tools including surveys, interviews, focus groups, ethnographical observations, participatory workshops, and case studies to understand diverse perspectives from multiple stakeholders. To answer the research questions, I will engage with different sets of individuals and institutional actors like citizen advocates, civil servants, public administrators of AI & digital services, and providers of AI & digital services. I will also examine current and proposed frameworks such as the GDPR, the AI Act, and other provisions that will influence the use, development, and compliance of digital public services using AI systems. The study aims to understand organisational dynamics in public-private partnerships, key practices, and challenges for incorporating AI-based technologies in the public sector while ensuring trust, accountability, and governance. The study’s outcomes should inform the adoption of improved policies, practices and technologies to support better accountability and compliance in public sector AI services in the future.


4 ‘Responsible AI Guidelines in Practice’, Defense Innovation Unit, Department of Defense, United Stated of America (2022).
References

METHODS FOR URBAN DATA ANALYSIS: 
Towards Safety and Inclusiveness

Cláudia Rodrigues

University of Coimbra, Center for Informatics and Systems of the University of Coimbra, Department of Informatics Engineering, Pinhal de Marrocos, Coimbra 3030-290, Portugal cbrodrigues@student.dei.uc.pt

Abstract. Urbanization is one of the most important social-economic phenomena. Due to the increase of the population in cities, it is important that they are managed in a way that guarantees safety and inclusiveness for everyone. The aim of this research is to model how people move and socialize in a city through the analysis of spatial data, with focus on understanding city dynamics. Mobile phone data is analyzed to perceive these dynamics from a mobility perspective, recognizing mobility and homophily patterns of the population. Such information can be used to sense how the space is used, and identify potentially isolated zones. This gives an overview of the safety and inclusiveness status of the areas of the city, which is crucial for decision-making and to improve the quality of living in urban areas.

Keywords: Urban Areas · Spatial Data · Safety · Inclusiveness.

1 Introduction

The urban growth and the demand for living in a safe and inclusive environment has speed up urbanization and social-economic development. As the population increases, it is more complicated to monitor and manage the dynamics of the various zones of the urban space. Usually, the main sources of data to analyze city dynamics are time-use, household, or travel diaries surveys. However, these data sources can sometimes under-represent specific sub-populations and are difficult to acquire. In contrast, given the widespread and ubiquitous aspects of mobile phones, biases associated with phone ownership are being reduced and mobile phone data can represent the insights from most population groups. The collection of this data is often made by mobile operators without requiring user participation.

The aim of this proposal is to use the analysis of spatial data to identify the different dynamics of the city’s zones. By using the information on the semantics of the areas to characterize them, and mobile phone data indicating who

* Supervisor Marco Veloso, Instituto Politécnico de Coimbra, ESTGOH, Rua General Santos Costa, Oliveira do Hospital, 3400-124, Portugal mveloso@dei.uc.pt; Co-Supervisor Carlos L Bento, University of Coimbra, Department of Informatics Engineering, Pinhal de Marrocos, Coimbra 3030-290, Portugal bento@dei.uc.pt
frequents them and when, we can have a perspective on how people move and interact across the space and identify patterns of connectivity and zones that lack inclusiveness. Ultimately, we intend to understand the city’s dynamics through the identification of mobility and homophily patterns, which are relevant for human safety assessment and inclusiveness in a city.

2 Objectives and Research Questions

This project focuses on discovering factors that impact the development of sustainable environments, mainly urban mobility, safety, and inclusiveness, through the analysis of spatial data. Due to the spatio-temporal information that mobile phone data contain, this kind of data is often used to study urban mobility. However, the use of only a specific type of this data to represent the population’s movements is impossible, because all datasets present different research challenges, such as lack of representation or spatial and temporal sparsity and irregularity. To address these limitations, various types of mobile phone data that are being collected by mobile operators need to be fused, such as Call Detail Records (CDRs) and location updates. Nonetheless, to understand the dynamics, we must add a context to the movements, which means that it is necessary to merge mobile phone data with data containing semantic knowledge of the areas, such as Points of Interest (POIs), socio-economic information, or registers of events and crimes.

Therefore, we intend to achieve a specific group of datasets, that can represent the movements and activities of the population and give contextual information about the circumstances under which they happened. We also intend to recognize and highlight the benefits of using spatial data to study the urban space, mostly mobile phone data. After the data preparation process, the main goal is to produce models that, with suitable techniques and methods, are able to recognize geo-profiles (routines, home, work, and other places frequently visited) and mobility and homophily patterns of the population across the different zones of the city. The ultimate goal is the recognition of zones that lack inclusiveness, due to distinct factors, namely safety.

Hence, there are three potential research questions to be addressed in this PhD program:

– RQ1: From the various sources of data available which ones are more effective in understanding the perceived safety and inclusiveness of urban areas?
– RQ2: What makes urban spatial data different in the study and analysis of the urban space?
– RQ3: Which strategies and methods can be applied to spatial data so that we can take insights into the safety and inclusiveness of the city and ensure that the resulting models can be used in urban planning?

The recognition of mobility patterns can contribute to enhance the public transportation structure. Yet, this research can also contribute to other sustainable actions related to social and safety aspects.
3 State-of-the-art

Mobile phone data includes geographical information and has the potential to show the spatial distribution of the population. For that reason, some authors considered it useful to identify places that are frequently visited including home, work, and other zones of interest [1] [2] [3]. Dashdorj et al. [4] also recognize the value of mobile phone data to analyze mobility dynamics. However, the authors consider that it is important to add to the general analysis, the contextual information about the circumstances under which the activities happened.

Many authors have been using the analysis of different data sources of spatial data to understand certain aspects of urban spaces. Hanaoka [5] used Global Positioning System (GPS) traces from mobile phones to study crime occurrences in a city, which revealed that the pattern of offenses and the locational characteristics of their occurrences largely differ between the hours of the day. Regarding the inclusiveness of cities, Graells-Garrido et al. [6], conducted a study using digital traces from mobile phone usage and pointed out that the over or under-presentations of certain groups of the population mainly depend on the income of the area, diversity of POIs, and the presence or absence of public transportation.

Another important subject in the field is the knowledge of how people evolve and socialize in the city. Using geotagged Twitter data, Heine et al. [7] found that socio-economic similarity is a significant predictor of connectivity between individuals. In the study, information on income, education level, and immigration history was used to characterize the areas of the city and analyze the mobility homophily of the citizens.

4 Methodology

To achieve the proposed goals, we start by reviewing approaches and the state-of-the-art. Meanwhile, we collect socio-economic information, POIs, and registers of events and occurrences of criminal activities to characterize the areas of the city. Such information will be collected from Census, statistical institutes, national authorities, and other databases. The mobile phone data will be collected from a mobile operator to identify the movements of the citizens.

Then, we begin an exploratory phase to understand which types of data are adequate to identify city dynamics based on the population’s mobility between zones. After, we will start using the mobile phone data to identify geo-profiles. In the meantime, we will also be working on the characterization of the zones of the city. Once the geo-profiles are identified and zones are characterized, we will focus our work on the final model, that will be able to identify mobility patterns and movement flows. Then, we will extract from this information the homophily between different zones of the city and zones that presented to be less secure and/or lack of inclusiveness. As we start achieving some results, we will use ground-truth data to validate and evaluate the models. Considering that the mobile phone data is anonimized, part of the ground-truth data will be provided by the mobile operator. This is going to be a cyclic phase of the models’ improvement, until we achieve meaningful outcomes.
References


Theoretical Learning Creators and Creative Scientists

Luís Espírito Santo ⋆⋆

CISUC, DEI
University of Coimbra, Portugal
lesanto@dei.uc.pt

Abstract. Can machines perform creative jobs? Such questions are in debate, as Learning Endowed Generative Systems threat to invade creative areas by recently achieving great results in several widely-accepted creative tasks. While Computational Creativity has prolifically provided us with formal tools to address such argument, systematically leaving the learning component out of the equation, Formal Learning Theory, allowed to study some of the limits of learning, yet mainly pinning these results to the language acquisition and scientific discovery problems, instead of other more widely accepted creative domains. We will endeavour to explore the parallels between these two currently disparate formal areas by identifying points of contact and clear differences and expanding both in a convergent joint transdisciplinary direction. This merged view is believed not only to spawn new studies in generative models, computability of learning, and computational creativity but also to bring new insights to some philosophical debates on the relationship between Artificial Intelligence and Computational Creativity and the nature of human creativity.

Keywords: Computational Creativity, · Learning in the Limit · Generative Models · Computability.

1 Introduction

During the last decade, we witnessed the rising of machine learning techniques with capabilities to autonomously create new realistic looking things. These are reaching the general public by providing new ways of generating faces [18], illustrations [6] and even music [12, 13]. Recently, DALL-E 2 [28] and other proceeding models [30, 23, 11] came to plunge forward the state of the art on text to

* This work is funded by national funds through the FCT - Foundation for Science and Technology, I.P., within the scope of the project CISUC - UID/CEC/00326/2020 and by European Social Fund, through the Regional Operational Program Centro 2020. The author is funded by Foundation for Science and Technology (FCT), Portugal, under the grant 2021.05529.BD.

** Joint PhD supervised by Prof. Amilcar Cardoso at University of Coimbra and Prof. Geraint Wiggins at Vrije Universiteit Brussel.
image generation systems, by creating astonishing contextualized images when provided with a single text prompt. Generative deep models such as Generative Adversarial Networks (GAN) [15], Variational Auto-Encoders (VAE) [21], Transformers [32], Diffusion Models [10] are becoming the backbone of very powerful Learning Endowed Generative Systems (LEGS). These new machine learning capabilities seem to clearly and effortlessly challenge several traditional arguments against creativity in machines, such as the one early presented by Ada Lovelace [25]: machines can only perform what we order it to perform and therefore they are not creative. This argument was originally rebutted by Alan Turing [31] in 1950, yet, for the general public, LEGS such as DALL-E 2 [28] constitute a more grounded argument. These models prove that there are machines capable of surpassing the Lovelace Test, i.e., machines that can do surprisingly more than what its creator initially intended. Our interest lies in the fact that those systems usually seem to leverage some kind of machine learning techniques.

2 Background

Computational Creativity (CC) area is a branch of AI which began the late 1990s. The CC-continuum [1] encompasses opposing approaches, ranging from practical systems that simulate creative behavior with machines, up to merely theoretical approaches that focus on modeling general creativity. Concerning modelling creativity, although authors have agreed that creativity involves novelty and usefulness [26], there are still several kinds of creativity to take into account [3, 19] and several different complex components [29]. From the several interpretations on the creative process, the Creative Systems Framework (CSF) [35, 34] deserves mentioning. This has four main components: a universe, a conceptual space, an evaluation function, and a strategy to explore that universe. There are many other references of neurological, psychological, educational, philosophical, and cognitive debates around creativity and its domains [22, 27, 33, 16]. However, and even though adaptable systems such as energy-based models have been constantly considered as a way to implement creativity in computers [1], there is still few methodical discussions around why these learning-endowed systems seem to achieve better results in creative tasks, or on how learning might enable creativity. On the other hand, most of the works that try to shed light on the role of creativity in learning lack the very insightful view provided by the most recent developments in AI and ML.

On learning, in the 1960s, Gold [14] formalizes a model for inductive learning, motivated by language acquisition in infants, and proves that not all classes of languages can be identified by every kind of learner. On top of this framework, Blum and Blum [2], Case [5, 4] and several other authors contributed to create a theory with definitions and criteria for scientists: functions that output a conjunction (a program) given a sequence of positive data. These mathematical scientists formalize the identification process of both recursive functions (scientists for functions) and recursively enumerated sets (scientists for sets) depending on the data. We refer to this theory as the Formal Learning Theory
(FLT), also known as Learning in the Limit, which is compiled in [20, 24, 17]. FLT has been used to prove some results that confront some widely spread ideas about learning and knowledge while also, according to Costa [7–9], providing a better understanding on the “large scale limitations of scientific discovery”. We believe that these insights can and should be applied to other creative domains such as music, a unique domain according to Wiggins [36], in order to also grasp the limitations of creativity. The expected results might not only provide new insights on the philosophical differences between machine and human creation, but would still help to bring both ML and CC closer together, for a joint effort to avoid another already speculatively prophesied AI winter.

3 Questions and Methodology

The main goal of this project is to shed some light on the relationship between Learning and Creativity, by attempting to formalize some definitions of creativity using FLT. With this in mind, we will endeavour to study the area of FLT and its results in depth, while keeping note on how those results might bring new insights to the CC area. Afterwards, it is important to collect a set of formal models from CC that are be promising easily integrate with learning. As a very theoretical and mathematical theory, the most laborious task will be to follow a series of though experiments aiming at creating a mapping between the several CC models and the formalized components of FLT, while translating the results from one to the other area or even proving new insightful results, while keeping in mind the current state of art of LEGS. These new ideas will be illustrated in different domains such as scientific discovery and music, so that the definitions can be understood and criticised in a simpler way. Meanwhile and throughout the full time of the project, there will be an extra effort to share the results of both FLT and CC to obtain feedback as well as disseminate the new insights that spawn from this investigation.

4 Expected results

The main output of this work will be some expanded CC models capable of better formalizing learning as part of the creative process. From this endeavour we also expect to derive different new proposals of learning paradigms, criteria, or strategies that are motivated by the creativity context. These might lead to new results on FLT and might be leveraged to better understand the limitations of learning, creativity, intelligence and their relationships. Other potential outcome is a taxonomy for LEGS based on the way they are formalized using the newly developed formal tools. Lastly, this work aims at getting some new attention towards the new insights brought by the two rather disjoint and underrated areas of FLT and CC.
References

Multi-Agent Systems
and Reinforcement Learning
Data Trading and Negotiation in Multi-Agent Systems

Hajar Baghcheband

PhD Candidate* Faculty of Engineering, University of Porto, Portugal
h.baghcheband@fe.up.pt

Abstract. Nowadays, autonomous agents, IoT and smart devices produce more and more distributed data and apply them to learn their models. The main challenge is that the local data may not be enough to learn reliable models. Data exchanging emerges to improve the locally trained model by communicating with other agents. In this paper, we propose a real-world simulation of data exchange among autonomous agents. The single agent and multi-agent systems consist of baseline and negotiation scenarios and are compared. The negotiation method is designed very basic to evaluate the main idea. The results show that the negotiation will improve the model accuracy slightly.

Keywords: Multi-Agent Systems (MAS) · Data Market · Data Trading · Machine Learning.

1 Introduction

Data collected in a distributed way by devices with computational power (small or large) create the opportunity to learn ML models locally, in those devices. However, local data may not lead to the best possible model (e.g. insufficient volume). Exchanging data with other devices may lead to better models but it has costs. Therefore, improving local ML models requires careful data exchange between devices. A Multi-Agent System approach can be used to implement this perspective of distributed ML with nontrivial processes of data exchange.

Lorenzo et al. [4] proposed a supervised data market to trade data plans and make a profit by trading the remaining data capacities by formulating the matching game with the preference ranking function. A transaction solution based on smart contract-enabled blockchain technology was designed and provided a competitive decentralized transaction way to trade data analytic services in addition to simple data trading [1, 2, 9, 3]. Oh et al. [5] designed an optimized trading model for data brokers to enable them to buy multiple types of personal data with appropriate incentives based on realistic willingness to sell and awareness of privacy. Shen et al. [6] focused on applying deep learning to extract data from the Internet of Vehicles through direct interaction between the provider and the

* Supervisors: Carlos Soares, Luis Paulo Reis
Faculty of Engineering, University of Porto, Portugal
user in the data market. Vanhaesebrouck et al. [7] investigated how similar objective agents can improve their locally trained model through communication with each other, where similarity is defined based on a given network graph. This article proposes automated data exchange between autonomous agents in distributed environments. Since data is considered a commodity, agents negotiate to exchange data with other agents.

2 Methodology and Model Definition

In this section, we present our model approach. First, we introduce a methodology and then analyze our hypotheses. The main goal of the proposed platform is to investigate a new paradigm of distributed machine learning, where distributed data is considered as a resource that is exchanged between ML agents, which we refer to as Machine Learning Data Markets (MLDM). These environments include autonomous self-directed agents that communicate with each other, negotiate data samples, add the exchanged data to their data set, and improve their machine learning model. In this paper, a simple negotiation is considered among the agents, they negotiate with the agent with the highest accuracy based on their budget. In the first phase, two types of models are defined: The Single Agent Model and the multi-agent model (MAS model). In the single-agent model, no negotiations are performed. In contrast, the multi-agent model consists of baseline scenarios and negotiation scenarios, with the only difference being that in the baseline scenario, negotiation is not allowed.

In the proposed data market, the agent $A_i \in A = \{A_1, A_2, \ldots, A_n\}$ has four components: 1- Model Component that train on training data $M = A(Tn_i)$, 2- Prediction Component that predict the precision of the model $P = A(Ts_i)$, 3- Negotiation Component to negotiate with other agents $N = A(Sample_i)$ and 4- Evaluation Component to evaluate the efficiency of the exchanged data to improve the model $E = A(Train_i \cup Sample_i)$.

All agents defined with various static features, $A_i = \{B_i, S_i, L_i\}$ where $B_i$ is the initial budget, $S_i$ is the trading strategy, and $L_i$ is the agent’s learning algorithm. Any record of data has cost as $DC$. At time $t$, the dynamic parameters of agent $A_i$ are data source, $DS_{i,t} \subset DS$ where data is partitioned horizontally, learning model, $M_{i,t}$ with performance $P_{i,t}$, perceived performance of other agents, $PA_{i,t}$ and budget, $B_{i,t} \geq 0$, $A_{i,t} = \{DS_{i,t}, M_{i,t}, P_{i,t}, PA_{i,t}, B_{i,t}\}$. At first, agent $A_i$ learns its model in the training set $Tn_{i,0} \subset DS_{i,0}$, $M_{i,1} = L_i(Tn_{i,0})$ and predicts the precision of the model based on its test set $Ts_{i,0} \subset DS_{i,0}$, $M_{i,1} = M(Ts_{i,0})$. It communicates with other agents to exchange the data, and in the negotiation stage (only in the MAS model-negotiation scenario), the agent with the highest accuracy is the main point of interest to present its data. Therefore, agent $A_i$ will send an offer to the presenter agent. If agent decides to negotiate, it will exchanged data samples with the agent $A_j$, $Tr_{i,j,t}$, pay for the sample set, $C_{i,t}$, where

$$C_{i,t} = \text{size}(Tr_{i,j,t}) \ast DC \quad \text{and} \quad C_{i,t} \leq B_{i,t}/DC \quad (1)$$
If its budget at negotiation time \( t \), \( B_{i,t} \), is less than the exchanged data cost, \( C_{i,t} \), agent will exchange some samples, otherwise it will exchange at maximum possible numbers based on its budget at time \( t \), \( size(Tr_{i,t}) = B_{i,t}/DC \).

Knowing the effect of negotiation on the accuracy of the learning model in a distributed environment is one of our main hypotheses. The initial data set size is 1% of the entire data set (\( DS_{i,0} = 0.01 \times DS \)). This value has been selected as low to check the vulnerability of the system in the case of a lack of data. In other words, if data is too small to learn the model efficiently, how data exchange will improve the learning model performance. Two evaluation perspectives are defined: Local Evaluation Perspective: the agents apply their model on a local test set (\( LT_{si,t} \)) and evaluate their model and in the negotiation step, they consider the local accuracy. Global Evaluation Perspective: the same global test set is defined for all agents (\( GT_{si,t} \)) and it is used for monitoring the behaviour of the whole system.

To analyze our proposed method, 48 data sources are selected from the OpenML platform [8], and the KNN algorithm is applied within a multi-agent environment (same machine learning algorithm for all agents). Data cost and initial budget are fixed (\( DC=1, B_i = 1000 \)). The environment consists of two agents learning their model based on their local data and negotiating to improve their learning accuracy. Our contributions are depicted in Fig. 1. The different perspectives of evaluation results over different models are gathered and the mean accuracy of all datasets is shown during different iterations. It could be concluded that negotiation can improve the learning accuracy of multi-agent systems, especially where train data are very rare. The agents started with the low accuracy of the learning model and data exchange could advance the performance. However, one single agent may have the highest accuracy which is considered the accuracy boundary for a multi-agent system. In a distributed system such as MAS or IoT network, local distributed data or the quality of data may not be enough to learn the model. Negotiation in a distributed environment will improve the accuracy of the model by adding new exchange data to local data.

Acknowledgements This work was financially supported (or partially financially supported) by Base Funding – UIDB/00027/2020 of the Artificial Intelligence and Computer Science Laboratory – LIACC - funded by national funds through the FCT/MCTES (PIDDAC) and by a PhD grant from Fundação para a Ciência e Tecnologia (FCT), reference SFRH/BD /06064/2021.

References

Reputation-based cooperation with private information

Henrique Correia da Fonseca¹

¹Group on AI for People and Society (GAIPS/INESC-ID), Instituto Superior Técnico, Universidade de Lisboa, Portugal (email: henrique.c.fonseca@tecnico.ulisboa.pt)

Abstract. Indirect Reciprocity (IR) constitutes one of the most elaborate cooperation mechanisms, relying on concepts such as social norms and reputations. IR often leans on the assumption that individuals can remember the reputations of every member of a population, a configuration that cannot always be translated into real scenarios. Thus, independent opinions on agents’ reputations will tend to diverge throughout a population. Here we investigate how memory influences the dynamics of cooperation under IR. Individuals learn how to deal with imperfect information by developing appropriate action rules and social norms with unknown reputations. Our preliminary results show that norms adopting trustful beliefs towards strangers lead to higher cooperation rates when compared with distrustful norms. Individuals naturally evolve to cooperate with strangers under the most successful norms. Intermediate cognitive skills may obtain maximal consensus and cooperation levels in the absence of complete information.

Keywords: Multiagent systems, Cooperation, Evolutionary Game Theory, Indirect Reciprocity.

1. Introduction and Problem

Indirect Reciprocity (IR) is a powerful solution to what is known as the cooperation dilemma [1,2]: How can Darwinian evolution select for altruistic behaviors? If to cooperate is to provide someone else a benefit, greater than its individual cost – as is conventionally defined as the Donation Game – then reputations can make cooperative acts worthwhile. By cooperating an individual may receive a good reputation, which increases the chances of receiving help from others in the future. Actions, in turn, are judged by social norms, which corresponds to incipient moral rules, defining what a good or a bad action is. This idea has also a long tradition in artificial intelligence (AI), constituting an appealing tool that can be used to efficiently steer behaviors towards desirable states [3].

The complexity of social norms can be arbitrarily high, depending on the number of previously taken actions one takes into account when performing a moral evaluation. Regardless, it has been argued that simple social norms are often the most effective [4,5] from an evolutionary perspective. The social norm Stern-Judging (SJ), for instance, can be summed up to “help good people and refuse help otherwise, and we shall
be nice to you; otherwise, you shall be punished” [5]. This moral evaluation rule is often crowned as a flagship of IR for two main reasons: (i) its inherent low complexity of memorization and execution in face of the promoted high levels of cooperation [4,5]; and (ii) its biological foundations in pre-verbal infants [6].

Despite this, the known benefits of IR often rely on simplifying assumptions regarding how well information is disseminated. Perfect information systems are unlikely to persist, as information is often noisy and humans do not always agree on shared information. This has been studied as a potential downfall of IR: when interactions are not observed by a whole population, opinions diverge and random reputations are assigned, thwarting the purpose of IR: what some see as sanctioned punishment of bad individuals is regarded by others as unfounded defection [7-9].

2. Proposed Model and Methodology

Incomplete information may result from different factors. Most works addressing this issue as a problem of observability: interactions are not observed by every agent in a population [7-9]. It is reasonable to assume that, although actions may not be fully observed within a small hunter-gatherer tribe, the role of gossip and conversation would be to fill in those individuals left out of such interactions [10]. Gossip and empathy have been studied as possible alternatives to perfect information in games of IR [11,12]. But as human population sizes grew, memorizing and making sense of all reputations may be cumbersome [13], as it happens in the case of direct reciprocity [14,15].

While most literature on IR studies the dynamics of binary reputations, here we argue that one cannot study incomplete information without a third possible label: the unknown reputation. While one can find literature regarding the study of ternary reputation systems [16,17], it always accounts for the third reputation as a middle ground between good and bad, often named the neutral reputation, a notion we avoid for its inherent ordinality: the unknown represents lack of information, rather than a stepping stone from good to bad, or vice-versa. By limiting the memory of agents, we allow them the freedom to avoid randomly attributing a good or bad reputation to undeserving agents by equipping them with the appropriate action rules and social norms. Thus, we pose the following research questions: (1) Can IR’s flagship social norms support cooperation in a scenario of private information due to cognitive limitations?; and (2) How do trustful-(towards strangers)-norms fare compared to distrustful ones promoting cooperation?

To answer such questions, we propose a computational model based on Evolutionary Game Theory [18] and previous literature [5,19-21] was developed, in which a finite sized number of agents (Z) plays the donation game, an economic game consisting on randomly selecting a donor and a recipient and allowing the donor to choose whether to provide a benefit b to the recipient at a personal cost c. The donor’s action is determined by its strategy, which evolves through social learning (imitation of successful agents) or exploration (random mutation) and determines the donor’s action – to cooperate or defect – according to the recipient’s reputation. The existing binary strategies and social-norms studied in previous literature [4,5,7,8,19,20] are expanded in order to account for a third reputation, yielding us with trustful and distrustful variations of each
strategy and norm. For each game, actions are observed by the population, judged according to the underlying social-norm and opinions are stored in an Image Matrix (IM), which stores every agent’s opinion regarding everyone else. However, the number of non-known opinions one can have is determined by a cognitive capacity $\lambda$. Every time an agent witnesses an interaction while having its memory at full capacity, a random opinion is to be forgotten in order to make room for the latest moral evaluation, creating imperfect and incomplete information. We shall analyze the following outputs of our numerical simulations: (i) the Average Cooperation Ratio – the total number of cooperative acts divided by the number of interactions; (ii) the Average Consensus Level – an adaptation of the Rice Index which dictates how polarized is the Image Matrix; and (iii) the frequency of each different strategy, giving insight into which actions are more popular given the simulation parameters.

3. Preliminary Results and Conclusions

Running the developed model for each of the mainly studied social norms and different values of cognitive capacity $\lambda$ under a fixed population size, simulations show that significant cooperation levels can be maintained with incomplete information under IR. Results also suggest that simulations tend to evolve into states where cooperation towards strangers is a dominant and evolutionarily stable strategy, and that such simulations attain the highest levels of cooperation. This is because of two main findings: (1) Under SJ, the system evolves in such way that its trustful and distrustful variations become the same trustful norm, by inverting the labels good and bad; and (2) The trustful variations of Simple Standing (SS) and Shunning (SH) largely outclass their distrustful variations when it comes to promoting information consensus and cooperation. Additionally, all simulations under trustful norms (including the wrongly named Distrustful SJ) present trustful strategies as dominant and evolutionarily stable. However, under SJ, the social norm that yields the highest levels of cooperation, having a larger but imperfect memory capacity appears to be detrimental to cooperation, causing a discontinuity for the highest $\lambda$ values. This happens since the number of strangers in the population is vestigial (because of a larger $\lambda$, yet different than $Z$), polarization is maximal and cooperation levels are minimal, since an action rule regarding strangers does not have enough selection pressure to evolve. This result suggests that natural selection may favor the evolution of moderate cognitive skills in the studied scenarios.
References

Artificial intelligence for zero-defect manufacturing in laser-based processes

João Paulo Sousa\textsuperscript{1,2} \* \*,\textsuperscript{[0000−0003−3879−6908]}

\textsuperscript{1} Faculty of Engineering, University of Porto (FEUP), Artificial Intelligence and Computer Science Laboratory (LIACC), Porto, Portugal.
\textsuperscript{2} Institute of Science and Innovation in Mechanical and Industrial Engineering (INEGI), Porto, Portugal.

Abstract. Laser-based processes (LBP) such as laser metal deposition (additive manufacturing), laser welding and laser cutting are characterised as toolless, precise and very energy efficient compared to the traditional processes. As agile and green manufacturing processes, their appeal in industry and research has been increasing over the last decade. Our industrial robotic cell and others showed the potential and added value of these extreme flexible processes in repairing components, welding batteries, tube processing, etc. Although, as LBP are difficult and complex due to the non-linear behavior and high dimension dynamics, even with the development of high-fidelity simulations, it requires substantial time and highly specialised human resources for its correct tuning and monitoring. Therefore, we propose to apply novel developments in artificial intelligence (AI) models and methods to in-situ monitoring and control, not only to minimise waste, increase quality and reliability but also to improve and simplify human-process interaction in a user-friendly fashion.

Keywords: Artificial Intelligence · Deep Learning · Laser-based processes · Monitoring and Control · Reinforcement Learning

\* Luís Paulo Reis is an Associate Professor at FEUP and Director of LIACC. He has been consolidating a track record on Artificial Intelligence, Intelligent Robotics, Machine Learning and Serious Games, and is considered a reference in the field both at a national and international levels. Also, is the co-director of the Artificial Intelligence and Data Science degree at the Faculty of Sciences of the University of Porto (FCUP), and has a vast experience as professor/supervisor at FEUP.
\*⋆ Ana Reis is an Assistant Professor at FEUP and a researcher at INEGI where she’s the Director of the Advanced Manufacturing Technologies Unit. She is responsible for several research projects in process monitoring, control, simulation, and material characterization in areas as casting, forming, molding, additive, and subtractive manufacturing.
1 Introduction

Modern factories create a huge amount of real-time data. Due to the strength of AI methods in automatically and efficiently extracting patterns and information from data, these can be applied to implement innovative and scalable monitoring and control strategies based on cyber-physical systems – Digital Twin [1, 2].

Process monitoring and control is an essential step in manufacturing because it ensures the quality and efficiency of the process [3–6]. Therefore, it raised attention in the research community for monitoring and controlling the main process attribute, i.e., the melt-pool, which consists of measuring the morphology and thermal action resulting from the interaction between high power lasers and the (metal) material. The shape, intensity, and temporal aspects of the melt pool are usually measured using IR sensors - cameras or pyrometers [7–9].

Concerning the crucial quality assessment of melt pool features, the use of ML and AI models has been increasingly applied in monitoring and predicting melt pool temperature, morphology or defects, based on images such as XGBoost and LSTM [10], physics-informed neural networks [11], Recurrent Neural Network (RNN) [12], custom Deep Learning model with a Convolutional Neural Network (CNN) [13–15], artificial neural network (ANN) [16, 17], and VGG16/Xception as a transfer learning approach [18]. Computer vision is also used to determine shapes and enhance image features [19]. Despite this effort, these approaches are limited as: (i) they are trained on a very small dataset (little focus on how to increase the amount of labelled data); (ii) are based on customized models such as a "black box", without using Explainable AI (XAI); or (iii) rely on architectures that are not scalable, being difficult to be replied or finetuned in other setups. Moreover, these do not report their performance or required computation in real-time monitoring, particularly in the pre-processing methods.

The evaluation of the process parameters’ influence, through experiments with real and reliable data, allows us to optimize processes and calibrate simulations [20]. Nevertheless, it is limited to a small batch of experiments, process conditions and equipment used [21, 22]. Most of the authors still use classical control such as PDIs or Fuzzy controllers [23, 24]. While these static models provide a basic understanding of the process, they are not suitable for designing advanced model-based controllers, e.g., model predictive control (MPC), because it requires a dynamic model of the process. Advanced data-driven models such as Koopman Operator [25], SINDy [26], and deep neural networks [27] can be used for dynamics system’ identification for process control. Although these approaches have been designed for robot control, many of them can be promising methods in manufacturing applications because of their accuracy and efficiency when training samples. In process control, besides the issues of cost and time limitation, the question is how to couple the monitoring/system models with control models in order to generalise in the processing of different materials, mainly where it is difficult to monitor and the variety of sensors with different outputs. The difficulty of AI application in laser-based applications can be summarized in the following requirements: (i) comparing with human-level performance, how to get good results with few data? (ii) how to automate data labelling? due to
A long-standing ambition of AI has been to create programs that can instead learn for themselves from first principles. Reinforcement Learning (RL) has demonstrated the ability to learn from experience in both games and the field of intelligent robotics [28]. Despite these advances, its use in industrial processes has not yet been explored, with only a previous study [29] applying it to the laser welding process.

2 Methodology

Having many parameters and time-dependent phenomena involved in laser-based processes, makes it practically impossible to reliably find an optimized parameter set to generalize a specific processing material or geometry. Currently, an acceptable parameter set is mainly found by pulling together the experience and intuition of skilled people within the present production system with limited experimental data. However, such methods do not scale to the mass customization needs, and it has become critical to develop ways to transfer such human experience and intuition to a more scalable setting - the cyber-space.

To overcome this technological gap and develop a methodology to automate AI model feeding in laser processes, we will focus on automated data acquisition systems coupled with state-of-the-art AI methods. Overall, this project aims to apply AI in laser processes to (i) reduce the number of trial-and-error experiments in their tuning; (ii) reduce waste and resources; and (iii) democratise laser processes by moving them towards autonomy and be used by non-expert users. Accordingly, we propose to:

- Create a digital twin capable of synchronous data acquisition, monitoring, and control, important for performing data-driven simulations and training models;
- Data labelling using human expertise in a small dataset and automate with a computer vision or deep learning model;
- Extra: apply a semi-supervised model;
- Apply AI for in-situ defect detection with a transfer learning approach enabling an in-depth knowledge of the process;
- Extra: Combine data-driven model with physics-driven for monitoring;
- Develop a controller for temperature and geometry of the melpool: (i) first with a reactive controller, and later with a more intelligent approach - coupled with the monitoring models to achieve robust control;
- Explore the application of Reinforcement Learning in laser-base processes with high-fidelity simulations and finetunning into real world.
Fig. 1. Project diagram.

References


9. Peiyu Zhang, Xin Zhou, Haijiang Ma, Jiawei Hu, Yixuan He, Xuefei Wang, and Yucong Duan. Anomaly detection in laser metal deposition with photodiode-based melt pool monitoring system. *Optics and Laser Technology*, 144(June):107454, 2021.


20. Roya Darabi, André Ferreira, Erfan Azimpour, Jose Cesar de Sa, and Ana Reis. Thermal study of a cladding layer of Inconel 625 in Directed Energy Deposition
Offline RL: Towards a wider application of RL methods in real-world domains

Pedro P. Santos\textsuperscript{1,2}\textsuperscript{*}

\textsuperscript{1} INESC-ID
\textsuperscript{2} Instituto Superior Técnico, University of Lisbon

Abstract. In this work, we aim to study new techniques to improve RL algorithms under off-policy settings, particularly under offline RL settings. We intend to propose new techniques to stabilize the training of RL algorithms by explicitly taking into account the interplay between the data distribution and the learning algorithm. We aim at proposing new techniques to mitigate distributional shift, the major challenge while learning in offline settings. Furthermore, we aim to explore how offline RL methods can contribute towards a wider application of RL algorithms in real-world domains such as adaptive traffic signal control or healthcare.

Keywords: Machine Learning · Reinforcement Learning.

1 Introduction

Despite recent advances in the field, reinforcement learning (RL) methods still feature a narrow range of applications due to the fact that the learning process involves iteratively collecting experience by interacting with the environment [12]. Such interaction is impractical in most real-world domains because data collection is dangerous and expensive. Adaptive traffic signal control (ATSC) is an example of an application domain that could benefit from the powerful tools provided by RL methods [1], as we show in our previous work [17]. However, one of the key challenges of RL-based ATSC is related with the difficulty of data acquisition; even in simulated settings, data acquisition is costly. Furthermore, due to the simulation-reality gap, no RL-based ATSC system has been deployed into the real-world. Offline RL methods, on the other hand, seek to learn utility-maximizing behavior using previously collected datasets of experience, possibly removing the need for simulation-based training. Thus, offline RL could greatly contribute towards a wider application of RL methods in real-world domains, by taking advantage of the several datasets that are readily available [8, 6, 10, 13].

Offline RL [12] recently provided the first tools that allow to learn utility-maximizing behavior from previously collected datasets of experience. However, as studies suggest, offline learning revealed to be a hard task, for which current RL methods are not suitable due to different limitations. Precisely, off-policy RL methods often cannot learn effectively from entire offline data, without any

\textsuperscript{*} Supervised by Prof. Francisco S. Melo and Prof. Alberto Sardinha
additional data collection, due to a problem generally known as distributional shift [12, 11]: while the learned function approximator (policy, value function, or dynamics model) might be trained under one distribution, it will be evaluated under a different distribution due to the change in the frequency of visitation of state-action pairs induced by the new learned policy.

In this work, we aim to develop new techniques to stabilize off-policy learning methods by better taking into account the distribution shifts that occur both during the training of RL algorithms, but also at deployment-time. Two research questions we aim to address are:

– How can we develop RL methods to robustly learn utility-maximizing behavior under distributional shifts?
– How can we develop RL methods to robustly learn utility-maximizing behavior using previously collected datasets?

2 Related work

Early works studied the application of variants of the well-known Q-learning algorithm with function approximation in an offline setting [5, 14]. More recently, new lines of research specifically target the development of methods to be used under offline settings. The two main lines of research can be categorized as follows:

– approximate dynamic programming (ADP)-based approaches, which estimate value functions, while attempting to mitigate distributional shift. Policy constraint-based methods mitigate the distributional shift by ensuring that the new learned policy is kept relatively close to the policy used to collect experience, according to an f-divergence metric [18, 7]. Uncertainty-based methods attempt to estimate the epistemic uncertainty of the learned value functions, thus detecting and mitigating distributional shift [11, 2]. Despite conceptually attractive, uncertainty-based methods are currently outperformed by policy-constraint methods, mostly due to the fact that current uncertainty estimation methods are not accurate enough [12]. On the other hand, policy-constraint methods propose solutions that are often too limited;
– model-based approaches, which estimate an approximate dynamics function that can be used to additionally incorporate a planning component to the agent. In order to account for distributional shift, proposed algorithms aim at quantifying the risk imposed by imperfect dynamics models [19, 3, 9], such as by incorporating a reward penalty based on an estimate of the model error. While this class of approaches can be more straightforwardly used under the offline RL setting, current methods can still greatly benefit from improved uncertainty estimation techniques. Moreover, model-based approaches usually struggle with very high-dimensional state spaces and long horizons [4].

3 Methodology & objectives

In this section, we briefly describe three research directions.
3.1 Offline RL and distributional shift

The developed work will be focused on making offline RL methods as robust as possible to state and action distributional shift. We will focus our attention to ADP and model-based RL methods. Different works consensually identify distributional shift as the major challenge for offline RL methods [12, 19]. Studies show that if distributional shift is not carefully taken into account, it can seriously impede learning and hurt the performance of the learned policy [15, 11]. As previously surveyed in Sec. 2, a good number of approaches to offline RL reside on uncertainty estimates to detect and mitigate distributional shift [11, 2, 19]. We aim to improve current methods for uncertainty estimation, both with respect to value functions and dynamics models, with the aid of Bayesian uncertainty estimation techniques (as an example, by using uncertainty-aware neural networks [3]). We aim to propose new offline RL algorithms that combine ADP and model-based methods, leveraging the strengths of both approaches. As pointed out by Levine et al. [12], techniques from causal inference [16] and distributional robustness/invariance can also provide powerful and novel tools to address and mitigate distributional shift in the context of offline RL. For empirical evaluations, we will use standard benchmarks [6, 8].

3.2 Improving online RL methods by leveraging existing datasets

We aim to study how we can improve online RL methods by leveraging readily available datasets of experience collected by other (possibly unknown) policies. Particularly, we aim to understand whether it is possible to improve the sampling efficiency and/or robustness of RL algorithms by incorporating offline data to the standard online learning process. Additionally, we also want to understand if we can take advantage of previously collected datasets of experience to predict the performance of the learnt policies at deployment time.

3.3 Offline RL for adaptive traffic signal control

We aim to study the application of offline RL methods under the ATSC problem. As previously described, RL-based ATSC could help to improve urban mobility. We intend to investigate how offline RL techniques can make the resulting controllers more robust and, possibly, removing the need for simulation-based training (e.g., by taking advantage of previously collected datasets of experience). Up to our knowledge, no previous work studied the application of offline RL techniques under the ATSC domain.

References

Natural Language Processing
Paraphrase Generation with Meaning Representations

Afonso Sousa

Faculdade de Engenharia, Universidade do Porto, Portugal
Laboratório de Inteligência Artificial e Ciência de Computadores (LIACC)
amlss@fe.up.pt

Abstract. Understanding that different wordings may share the same meaning is essential for language understanding. In this work, we will research on how to exploit structures of meaning to embed additional knowledge into paraphrase generators. We believe that by exploiting those meaning representations we can produce semantically similar paraphrases with more syntactic variation. We will also look at ways to evaluate such generations more effectively. Furthermore, explore means to extract meaning structures from user-generated content, which may be poorly structured or written.

Keywords: Paraphrase generation · Meaning representations · Natural Language Processing.

1 Introduction

Paraphrases are a restatement of the meaning of a text or passage using other words. Understanding that the question How far is X from Y? could be phrased as What is the distance between X to Y? without loss of meaning is important for various Natural Language Processing (NLP) tasks: question answering (QA) systems [5] may give multiple correct paraphrased answers to the same question; machine translation [19] may produce multiple paraphrase excerpts deemed good translations for a given source; semantic parsing [3] should map multiple paraphrases to the same logical predicates. Paraphrasing has also been used to great success for data augmentation [6].

Besides recent breakthroughs in Deep Learning and, in particular, in NLP [16], it is still hard to extrapolate all the embedded information contained in unstructured data such as input text. Current state-of-the-art models still provide limited reasoning capabilities for intentional language use. The lacklustre machine-generated responses contrast with knowledge-rich human responses, using commonsense or pre-acquired knowledge to answer. Therefore, it is often the case that knowledge beyond the input sequence is required to produce informative output text.

* Supervised by Henrique Lopes Cardoso, FEUP/LIACC.
Explicitly encoding structured representations of the semantic relationships in the text has two major advantages: it can facilitate the connection of relevant subjects and events spanning across multiple sentences, preserving the global context [9]; it should help text generators more easily converge to good solutions, as opposed to building billion-parameter models in hopes to absorb the intricate nuances of good paraphrases.

Moreover, semantic information can unravel cross-sentence dependencies that will help produce better quality long text paraphrases. While most paraphrase systems focus on generating paraphrases of individual sentences, we feel that paragraph-level paraphrase generation (which seeks to rewrite longer multi-sentence sequences without affecting their original meaning) is much more beneficial.

We also intend to explore paraphrasing for user-generated text. This kind of text source carries the added challenge of possibly being poorly written. In this scenario, it may not be possible to properly extract the semantic information of a sentence. In this case, we will resort to preprocess the text by employing style transfer models trained to convert poorly-written into well-written text, in hopes to achieve well-structured text from which to extract structures of meaning.

2 State-of-the-Art

In recent years, approaches for paraphrase generation have shifted from the classical approaches [15] to neural network-based systems. Most of the existing paraphrase generation approaches are based on sequence-to-sequence models [18] consisting of an encoder – which encodes the source texts into a contextualised vector representation – and a decoder – which generates paraphrases based on the vectors given by the encoder. Earlier works employed recurrent neural networks [17]. Currently, the most prominent architectures are Transformer-based [8].

The neural network-based approaches proposed to tackle paraphrase generation can be categorised into (i) model-focused approaches agnostic to paraphrase attributes and (ii) attribute-focused approaches that target specific aspects of paraphrase generation [22]. The most relevant model-focused approaches are attention [1], a mechanism that enables the decoder to focus on some words/phrases that are of high relevance when generating a word, and the copy mechanism [7], which copies a span of elements from the input sequence decided by the attention mechanism directly into the output. As for the attribute-focused ones: there are approaches targeting the diversity of generated paraphrases [21]; approaches targeting the granularity level of the generated paraphrases (i.e. changing words [4], changing sentences or multi-level [13]); and approaches targeting the syntax. The works employing the latter approaches encode auxiliary knowledge sources to enhance generations [10]. These works use syntactic constituency graphs, i.e., graphs representing syntactic relations between words. Dependency information captures long-distance dependency constraints and parent-child relations for different words [2]. Other knowledge sources used to enhance text generation can be found in works addressing neighbouring text generation tasks, namely: seman-
tic dependency graph, which represents predicate-argument relations between content words in a sentence [11]; internal knowledge graphs, which are knowledge graphs constructed solely based on the input text [9]; Keyword interaction graphs entail building a graph by decomposing a source passage into several keyword centred clusters of text and building the edges between nodes based on the semantic relationship between the keywords [12].

Automatic evaluation is often used for paraphrase generation systems because of the costly endeavour of human evaluation. The commonly used automatic metrics enable fast development cycles, but they are not sufficient for final quality assessment. They reward homogeneous predictions to the training target, which conflicts with the paraphrasing goal of word variation. Many works [20, 14] showed that predictions receiving low scores from these metrics are not necessarily of poor quality according to human evaluation. More reasonable metrics to specifically evaluate paraphrase generation are of utmost importance.

3 Methodology

We hypothesize that formulating paraphrase generation as a knowledge-enhanced text generation task assisted with meaning representations can improve the quality of the generated paraphrases. To test our hypothesis, we formulate the following research questions: (1) How can we exploit meaning representations specifically to enhance paraphrase generation? We will use meaning representations to address paraphrase-specific features like semantic consistency and lexicon variety. We will focus on understanding the best representations and how to best model them. (2) How can meaning representations be used for paragraph/document-level paraphrase generation? We will target multiple sentence generation and how to maintain the coherence between them. (3) How can we extract semantics in user-generated content? We want to account for the nuances of user-generated input and how to extract meaning from them. (4) How can we better evaluate generated paraphrases? The evaluation is always a primordial step in any research work, and it is a challenging endeavour for paraphrase generation. As such, we make one of our goals to try to improve the available solutions for automated paraphrase evaluation. The development of the proposed work will culminate in a prototype for paraphrasing sentences or paragraphs robust to user-generated content.

4 Conclusions

This work will focus on improving paraphrase generation enhancing it with meaning structures. We bring together a comprehensive list of challenges in paraphrase generation and our prospects of addressing some of the raised problems in the current literature. Our contributions should improve the current paraphrase generation state-of-the-art, both on the quality of the generations and the evaluation of these systems.
References

1. Bahdanau, D., Cho, K., Bengio, Y.: Neural machine translation by jointly learning
2. Bastings, J., Titov, I., Aziz, W., Marcheggiani, D., Sima’an, K.: Graph convolu-
tional encoders for syntax-aware neural machine translation. In: EMNLP (Sep
2017)
4. Cao, Z., Luo, C., Li, W., Li, S.: Joint copying and restricted generation for para-
answering. In: EMNLP (Sep 2017)
generation. In: ACL (Jul 2020)
7. Gu, J., Lu, Z., Li, H., Li, V.O.: Incorporating copying mechanism in sequence-to-
8. Hosking, T., Lapata, M.: Factorising meaning and form for intent-preserving para-
ration with semantic-driven cloze reward. In: ACL (2020)
10. Iyyer, M., Wieting, J., Gimpel, K., Zettlemoyer, L.: Adversarial example generation
tive summarization. AAAI (Apr 2020)
12. Li, W., Xu, J., He, Y., Yan, S., Wu, Y., Sun, X.: Coherent comments generation
for Chinese articles with a graph-to-sequence model. In: ACL (Jul 2019)
In: ACL (Jul 2019)
on paraphrase generation datasets. In: EMNLP-IJCNLP (Nov 2019)
15. McKeown, K.R.: Paraphrasing questions using given and new information. Com-
put. Linguist. (Jan 1983)
16. Min, B., Ross, H., Sulem, E., Veyseh, A.P.B., Nguyen, T.H., Sainz, O., Agirre,
E., Heinz, I., Roth, D.: Recent advances in natural language processing via large
paraphrase generation with stacked residual LSTM networks. In: COLING (Dec
2016)
18. Sutskever, I., Vinyals, O., Le, Q.V.: Sequence to sequence learning with neural
19. Thompson, B., Post, M.: Automatic machine translation evaluation in many lan-
guages via zero-shot paraphrasing. In: EMNLP (Nov 2020)
EMNLP (Nov 2021)
Biomedical Information Extraction in Domain-Specific Texts

André João S. S. Gonçalves* [0000−0002−8581−0218]

Faculdade de Engenharia, Universidade do Porto, Portugal
Laboratório de Inteligência Artificial e Ciência de Computadores (LIACC)
up201404724@fe.up.pt

Abstract. Literature mining in the biomedical domain is becoming an important task to not only aid in the condensation and systematization of information in subject-specific areas, but also in real scientific knowledge discovery. The present project aims at developing a comprehensive framework capable of adaptively extracting pertinent, relational information from scientific texts under a wide range of domains within biomedical sciences, while providing the user with a concise yet informative visualization of the mined information – ideally reducing the burden of manual literature research in the biomedical scope.

Keywords: Natural Language Processing; Biomedical Named Entity Recognition; Relation Extraction; Network Biology; Artificial Intelligence.

1 Introduction

Over the last two decades, Biomedical Sciences have undergone an unprecedented surge of progress in a variety of fields, bringing about an advent of revolutionary theories, methodologies and applications. The vast amount of knowledge generated by high-throughput technologies has transpired across numbers in biomedical literature, which has grown in volume to a point where its manual curation is steadily becoming unfeasible for expert researchers, even in niche domains [2]. As a result, advanced techniques in Information Retrieval, Data Mining and Natural Language Processing are being increasingly employed in different tasks surrounding biomedical literature, including document retrieval, question answering and database generation [6]. Among these, and in light of the recent successes in the forefront of the Biotext Mining field [4, 8, 10, 12], biomedical information extraction is being increasingly perceived as not only useful, but rather essential for the foreseeable future of biomedical research [13].

2 Project Overview

The present project aims at developing an integrative framework that automatically extracts terms of interest from scientific reports under the scope of

* Supervised by Henrique Lopes Cardoso (FEUP/LIACC) and Luís Paulo Reis (FEUP/LIACC).
biomedical sciences, while also capturing and categorizing the biological relations between said entities; the extracted knowledge should then be formalized by means of graph structures, providing a practical visualization scheme along with an analytical framework for large volumes of mined information. As such, three main research questions are considered: 1) **How may current BioNER strategies be improved upon, namely across different types of biological entities?**; 2) **How can the various relations between bio-entities be detected, mapped and ascribed into knowledge graphs?** and 3) **What degree of similarity can be expected between biological networks and literature-mined graphs?**

3 Main Steps in Biomedical IE

3.1 Biomedical Named Entity Recognition (BioNER)

The BioNER task focuses on identifying specific terms in text bearing interest to medical research, which normally occur in the form of named genes, proteins, drugs, metabolites, pathogens, diseases, cell lines and cellular compartments. BioNER is the basis for many downstream tasks in BioNLP, such as document linkage, text classification or relation extraction (among others) [10].

Early BioNER methods consisted of dictionary- and rule-based approaches, soon after followed by feature-based supervised learning techniques – all of which heavily reliant on manually predetermined features [11]. Conversely, approaches based on deep learning have become incredibly popular in recent years due to their autonomous apprehension of useful representations from underlying features in raw input data. Among these, CNNs, RNNs and Bi-LSTMs coupled with Conditional Random Fields achieved State-of-The-Art performance for some time [4], and eventually paved the way for the currently dominant transformer-based models, most famously represented by BERT [3]. BERT utilizes bidirectional transformers pre-trained on a Masked Language Model task to learn the context of individual words based on their left and right surroundings; furthermore, by pre-training said models in domain-specific benchmark corpora, and fine-tuning them on representative biomedical text mining tasks (namely those mentioned in this paper), different researchers attained better classification results with the BioBERT and SciBERT models, among others [1, 5, 8].

3.2 Biological Relation Extraction (BioRE)

BioRE refers to the detection and classification of semantic/contextual relations among different biomedical concepts within the literature, with the goal of detecting occurrences of pre-specified types of relations between entity pairs [10, 12]. Similarly to BioNER, this task is typically addressed by methodologies relying on CNNs, LSTMs and, more lately, previously discussed transformer-based models like BERT, SciBERT and BioBERT, under adequate fine-tuning [1, 3, 8]. Nevertheless, the BioRE step remains a demanding challenge, mostly due to the frequent emergence of new and unseen bio-entities engaging in convoluted (and sometimes conflicting) n-folded causal interactions with multiple entities [12].
3.3 Graph construction & Network analysis

In Network Biology, graphs can capture the associations between any biological entities such as proteins, genes, metabolites, diseases, drugs and organisms, at levels of complexity ranging from molecule to system; in the resulting networks, nodes typically correspond to entities and edges represent the relations between them [10]. As a result, following any BioNLP Information Extraction pipeline, Graph Theory provides powerful tools to display, integrate and analyse large volumes of information mined from text. By employing a combination of metrics and methodologies that are native to Network Science, such as centrality measures, clustering metrics, modularity values and subgraph motifs, it is possible to both extract additional information regarding the relative importance of biological mediators within a system, and establish unforeseen connections between seemingly distant entities [7,9].

4 Methodology

The present project seeks to tackle the biomedical IE task with an all-encompassing framework for bio-entities and biological relations, interpreting it as a problem of numerous entity classes being tied by few macro-relation types. The envisioned methodology for this project entails four main steps:

1) Corpus preparation and annotation: to support the ensuing pipeline, a novel annotation scheme featuring 12 entity classes and 5 major relation types will be implemented in the curation of a new corpus of English scientific abstracts for Biotext Mining; in it, the sets of relations that are permitted and forbidden between each pair of classes are predetermined, so as to confidently favor valid associations between a higher number of nuanced bioentity types.

2) BioNER: holding as a premise the idea that the majority of relevant biomedical information is concentrated around formal bioentities in text, NER will be conducted via transformer-based, task-specific models such as BioBERT, due to their superiority in assimilating contexts when detecting terms of interest;

3) BioRE: similarly to BioNER, the RE task will be addressed via BERT-based models, shown to produce leading results in this area. Moreover, by pre-determining which macro-relations can be established between each pair of entity classes, the algorithm may draw insight from the types of BioNE it connects, as well as detect mistakes in the classification of relations or entity types – enabling a back-and-forth iterative approach that learns relations based on entity types, and adjusts BioNEs based on probable relations.

4) Graph representation and network analysis: as a final step, the automatically extracted information will be integrated in the form of knowledge graphs, and basic network analysis will be conducted, aiming at detecting eventual distinctive patterns and address their potential predictive power. Importantly, by expanding the analysis to collections of texts instead of individual documents, it will be possible to synchronously accommodate, compare and confront scientific assertions pertaining to a multitude of scientific reports, and therefore streamline the burdensome process of manual literature research.
References

Machine Translation for Emakhuwa of Mozambique

Felermino D. M. A. Ali∗

Faculdade de Engenharia, Universidade do Porto, Portugal
Laboratório de Inteligência Artificial e Ciência de Computadores (LIACC)
Faculdade de Letras, Universidade do Porto, Portugal
Centro de Linguística da Universidade do Porto (CLUP)
up202100778@fe.up.pt

Abstract. Emakhuwa is a Mozambican language under the low-resource category despite being widely spoken in Mozambique (i.e. over 6 million speakers). To the best of our knowledge, no Machine Translation tools exist for Emakhuwa. However, in recent years, there has been a huge collaborative effort from African Natural Language research communities to develop techniques for Neural Machine Translation adequate to African Languages. This led to the development of corpora, text representation techniques, pre-trained models, and Neural Network Architectures, all of which are benchmarks for improving current Machine Translation of low-resourced languages, and in particular the African language family. Therefore, this study aims to investigate how this development can be helpful to assist Machine Translation of Emakhuwa, and also propose a suitable approach and resources to develop such system.

Keywords: Emakhuwa · Neural Machine Translation · Low-resource settings · African Language.

1 Introduction

Unlike previous approaches, Neural Machine Translation is data-driven and requires the existence of a large amount of data. For instance, commercial Neural Machine Translation systems on the market have been trained with over a million examples. However, it is unrealistic to expect to find a similar amount of data on underrepresented languages (also known as low-resourced). In fact, only a few languages have a strong web presence and possess resources for Natural Language Processing (NLP). Therefore, there is a huge disproportional focus of research on the so-called high-resource languages, a group which is dominated by English.

Emakhuwa is one of these underrepresented languages. Despite being widely spoken in Mozambique, it has little presence on the web, and few resources and tools. Therefore, the goal of this study is to develop resources with a particular

* Supervised by Henrique Lopes Cardoso (FEUP/LIACC) and Rui Sousa-Silva (FLUP/CLUP).
focus to investigate how Neural Machine Translation (NMT) can be applied to Emakhuwa.

Emakhuwa (also known as Makua, Macua or Makhuwa) is a Bantu language spoken in northern and central Mozambique, i.e., Niassa, Cabo Delgado and Nampula as well as in some parts of Zambezia province. It is estimated that approximately 25% of the country’s population of 30 million people use the language daily as an alternative to Portuguese [15]. The language is also spoken in neighbouring countries, such as Tanzania and Malawi with a relatively small number of speakers.

2 Related Work

In general, low-resource settings impose challenges which require adopting different strategies from the ones used in high-resource settings. In many cases, the best option in low-resource settings is to enrich the amount of data, by collecting more data, but data collection is a very expensive and time-consuming task. That is why others use ways to generate synthetic data either via data augmentation techniques or by investing in automatic generation methods such as weak or distant supervision [7, 10]. However, these methods usually tend to introduce noise and if not properly handled may be more harmful than helpful. Therefore, proper ways to enrich data are still an open question in NLP. Similarly, general machine learning can be adapted to low-resource scenarios. Due to the unavailability of data, many researchers proposed ways to perform NMT using unsupervised or semi-supervised learning [21, 5, 17, 18]. Also, different Neural Network architecture have been proposed to suit low-resource settings [9]. However, one area that brings promising results is transfer learning, which reuses what has been learned in other languages to initialize a child model (i.e., downstream), in a process known as pre-train and fine-tune. The advantages of transfer learning are the reduction of the amount of time taken to train and the amount of data while guaranteeing better performances over training the child model from scratch. In NMT for low-resource settings, this approach is a game-changer, especially on typological similar languages as it captures shared linguistic representation between similar languages and therefore enables cross-lingual transfer and zero-shot learning [8, 6, 12, 4]. Therefore, we survey the literature on pre-trained Language Models (PLM) covering African languages [20, 8, 1, 13], and although Emakhuwa is not covered in any of them, we see a huge opportunity in leveraging NMT by exploiting the shared representation of similar Bantu languages.

3 Research Objectives

The main aim of this research is to investigate how Neural Machine Translation can be applied to translate from/to Emakhuwa. To achieve this, the research questions explored in this work are as follows:

– What is the effect of automatic data augmentation on translation quality?
To what extent can unsupervised Neural Machine Translation be leveraged for Emakhuwa NMT?

How does cross-lingual transfer learning from PLM on African languages improve Emakhuwa NMT?

To what extent can zero-shot from/to Emakhuwa be achieved using multilingual NMT?

4 Methodology

The goal of this study is to develop resources to facilitate Machine Translation for Emakhuwa, which includes data and tools. We will use the following parallel corpora: Portuguese-Emakhuwa [2], Xitsonga-English [11], and Portuguese-English ParaCrawl [3]. English and Xitsonga data are collected for the zero-shot experiments. In addition, we will also enrich the Portuguese-Emakhuwa dataset by adding data from other domains including news, legal documents, radio transcripts and Wikipedia articles. Due to the difficulty in finding Xitsonga to Portuguese sentence pairs, we will machine-translate the English part of the second dataset [11] to Portuguese, therefore generating Xitsonga-Portuguese training examples.

We will train Transformer-based models [19] as baseline models for Emakhuwa to Portuguese translation. Then, we will investigate the effects of data augmentation on translation quality. Here we will experiment with state-of-art augmentation techniques by training Transformer-based models using the augmented data and comparing its performance against the baseline.

Next, the experiments will be further subdivided into two sets. The goal of the first one is to assess the performance of the NMT with the Conditional Sequence Generative Adversarial Network proposed by Yang et al. [21]. Conversely, the second set of experiments is to adapt available multilingual pre-trained models to fine-tune on machine translation using the data collected above. Here, we will follow the approach proposed by Adelani et al. [1]. Also, using the same multilingual model we will assess the zero-shot capabilities of the models. To assess the effectiveness of the models we will use BLEU [14] and ChrF [16].

5 Conclusion

Neural Machine Translation is a prominent approach for Machine Translation. However, Neural Machine Translation has the constraint of being data-hungry. Thus, over the past years, many different approaches have been proposed in the literature to be able to apply Neural Machine Translation in low-resource settings. Emakhuwa is one of these underrepresented languages in the context of Machine Translation research. Therefore, this project aims to develop resources for Emakhuwa Machine Translation and investigate how to perform quality Neural Machine Translation even without the availability of a large quantities of data.
References


Automatic Dialogue Flow Extraction and Guidance

Patrícia Ferreira*

CISUC, Universidade de Coimbra
patriciaf@dei.uc.pt

Abstract. Nowadays, human agents are often replaced by conversational software agents, designed to communicate with humans through natural language, often based on Artificial Intelligence, namely Natural Language Processing (NLP) and Machine Learning (ML). This work will have as one of the main goals the improvement of communication between customers and human agents in a call-center to make this work more efficient or, not only in call-centers but in a common conversation between actors, suggesting appropriate responses, thus anticipating their interventions. You will start by identifying and annotating sets of dialogues, written in Portuguese. The guidance given can be supported by a history of interactions, where information is extracted and frequent dialog flows are discovered, allowing a representation of them to guide humans. The approach will be divided into three components: the Extraction component to process dialogues and use the information to describe interactions; the Representation component to discover the most frequent dialogue flows, represented by interaction graphs; and the Guidance component to guide the agent during a new dialogue.

Keywords: Natural Language Processing · Dialog Analysis · Dialog Information Extraction · Representation of dialog flows · Assisted guidance

1 Background and Related Work

A dialog is composed of utterances, which instantiate dialog acts (DAs), that is, abstract representations of intentions. There are several dialogue datasets, mainly for English [2], however, this work will focus on Portuguese, where public dialogue datasets are scarce.

There are several approaches for automatic classification of DAs (DAC) [1]. Most are based on supervised learning, with models trained in dialog datasets where the DAs are manually annotated [3]. Others use traditional classification [3][4]. However, since there may be a dependency between the current interaction and previous ones, DAs can be tackled as a sequence classification problem, with methods such as Hidden Markov Models (HMM) [5] or Conditional Random Fields (CRF) [6]. DAs and transition graphs between them are

* Supervised by Hugo Gonçalo Oliveira (hroliv@dei.uc.pt), Catarina Silva (catarina@dei.uc.pt) e Ana Alves (ana@dei.uc.pt)
useful representations of dialogs. When applied to large sets of dialogs, models trained will allow the discovery of different types of interactions and the most common dialog flows. These flows can even be discovered without annotating DAs, through unsupervised approaches (clustering) [8]. Furthermore, as real-time call monitoring, these flows will be useful to help interpret the dialog and support the participants. [9] [10].

2 Methodology

Overall, this work consists of researching, implementing and testing a solution that aims to improve communication between participants in a dialog by guiding their actions, which can be supported by previous interactions, where information should be automatically extracted and where frequent dialog flows. Besides task-oriented dialogues experiments will be extended to conversations between common users, such as, in a social network, where it will be possible to analyze communication trends.

The experiments will be conducted with data in Portuguese, which will be a differentiating factor from the state of the art. They will also be limited to written text, i.e., written conversations or transcripts of oral communication.

The data can be created following the Wizard-of-Oz (WOZ) [11], where a conversation takes place between two participants with different roles. One plays the role of an ordinary user who is assigned a certain task and must interact, using natural language, with another that will have access to information about the domain (e.g., a database) and will be able to provide appropriate answers.

Data can also result from available transcriptions of existing dialogues into Portuguese, such as CORAA [12]; from customer support services, such as conversations with telecom operators on Twitter; or from movie subtitles [13]. One last possibility will be the translation of English datasets (e.g., DailyDialogue [14], MultiWOz [15]) into Portuguese, from where existing annotation can be imported.

The data will be used in the development of a framework consisting of three components. The first will process real dialog transcripts and extract useful information from them to represent interactions, such as keywords, entities or actions. The extraction of some of these items may resort to an NLP pipeline [16]. The extracted information can be used to better describe the utterances, by classifying intentions and filling slots. However, the performance of these tasks is usually based on supervised learning, which implies data annotation. The extracted information can also be used to group similar utterances, using clustering. This process can also resort to Sentence Embedding techniques [17].

The second component will aim at discovering the most frequent dialog flows, represented by graphs, where the vertices represent speech classes or clusters, and the arcs represent transitions between them, with associated probabilities. In this component one can apply the classification of interactions into more generic classes or, if there is a lack of data to make the system less domain-dependent, perform a clustering that approximates these acts.
Finally, the guidance component will take advantage of past dialogs, represented according to previous components. In each interaction, previous interactions will be considered, while anticipating the next interaction. This component will analyze the ongoing dialog, using an NLP pipeline, and, whenever possible, map an expression and its context, represented by previous interactions, to expressions represented in the dialog flow graph. This mapping can be done through Semantic Textual Similarity [19] mechanisms, using techniques that consider only the words used and their relevance (e.g. TF-IDF based [20]). When this mapping is successful, the possible transitions from that expression will be collected and presented to the agent. Techniques used by Recommender Systems [21] to make recommendations given a context will be explored.

A final evaluation of the results of integrating the three components into the framework should be done, as the approaches explored will be evaluated on the data gathered and created using metrics for classification when annotations are produced, or metrics for clustering when they are not.

3 Objectives and Expected Results

The main objective of this work is to investigate and develop approaches to improve communication in a dialog, in Portuguese, supporting guidance of human agents, such as for example supporting a human in a call-center.

NLP techniques will be explored, focusing on dialog modeling [18], in order to, based on the history of interactions, identify the most common ones in each application domain, discover and interpret flows, and take advantage of the latter to guide interlocutors, who may thus anticipate their interventions. The dialog modeling will focus on dialog and intent classification acts as well as flow discovery in a scenario where there is no annotated data.

We aim at approaches, applicable to written dialogues, e.g. between users of a social network, or to transcriptions of task-oriented dialogues (e.g., call-center) to assist call-center operators in providing more efficient service.

We believe that the work will result in innovative approaches, and highlight the fact that, regardless of the possible adaptation to other languages, it will be focused on Portuguese. The work will be divided into some specific objectives, namely: identify and create sets of dialogues, in Portuguese; study, develop and experiment approaches for extracting structured dialogue information from the various interactions; for representing interactions and dialog flows extracted from those interactions; for guiding the human by exploiting the knowledge extracted from dialogues, dialogue type and interactions, and common flows.

To achieve the defined goals, the following tasks were established: 1. To deepen the study of the state of the art; 2. Definition of the data to be used; 3. Exploring approaches for the three components; 6. Proposed framework encompassing the approaches explored; 7. Testing and final evaluation; 8. Writing of the thesis and dissemination papers. The approaches resulting from task 3 will be evaluated independently during their respective tasks, but a final evaluation of the results of their integration into the framework will be required. The ex-
periences are regularly described in writing in the doctoral thesis. We further believe that from tasks 2 to 7 will result contributions relevant to write papers.

References


