Towards Robust and Adaptive Machine Learning

Machine learning (ML) is widely used in various disciplines as a powerful tool for developing predictive models to analyze diverse variables. In the digital era, the abundance of data has created growth opportunities, but it also brings challenges due to the dynamic nature of data. One of these challenges is concept drift, the shifting data distributions over time. Consequently, traditional static models are inadequate for handling these challenges in the online world. Concept drift, with its intricate aspects, presents a challenge for learning algorithms. Analyzing model performance and detecting substantial shifts in data distributions are crucial for integrating adaptive methodologies to update ML models in response to data dynamics, maintaining effectiveness and reliability in evolving environments. In this dissertation, a fresh perspective is offered on the robustness and adaptivity of ML models in non-stationary environments. This research explores and organizes existing literature, analyzes ML model performance in the presence of drift, and proposes innovative methodologies for detecting and adapting to drift in real-world problems. The aim is to develop more robust and adaptive ML solutions capable of thriving in dynamic and evolving data landscapes.
Towards Robust and Adaptive Machine Learning

A Fresh Perspective on Evaluation and Adaptation Methodologies in Non-Stationary Environments

Firas Bayram
Towards Robust and Adaptive Machine Learning - A Fresh Perspective on Evaluation and Adaptation Methodologies in Non-Stationary Environments

Firas Bayram

LICENTIATE THESIS

Karlstad University Studies | 2023:23

urn:nbn:se:kau:diva-95645

ISSN 1403-8099


© The author

Distribution:
Karlstad University
Faculty of Health, Science and Technology
Department of Mathematics and Computer Science
SE-651 88 Karlstad, Sweden
+46 54 700 10 00

Print: Universitetstryckeriet, Karlstad 2023

WWW.KAU.SE
Towards Robust and Adaptive Machine Learning

A Fresh Perspective on Evaluation and Adaptation Methodologies in Non-Stationary Environments

Firas Bayram
Department of Mathematics and Computer Science
Karlstad University

Abstract

Machine learning (ML) has become ubiquitous in various disciplines and applications, serving as a powerful tool for developing predictive models to analyze diverse variables of interest. With the advent of the digital era, the proliferation of data has presented numerous opportunities for growth and expansion across various domains. However, along with these opportunities, there is a unique set of challenges that arises due to the dynamic and ever-changing nature of data. These challenges include concept drift, which refers to shifting data distributions over time, and other data-related issues that can be framed as learning problems. Traditional static models are inadequate in handling these issues, underscoring the need for novel approaches to enhance the performance robustness and reliability of ML models to effectively navigate the inherent non-stationarity in the online world. The field of concept drift is characterized by several intricate aspects that challenge learning algorithms, including the analysis of model performance, which requires evaluating and understanding how the ML model’s predictive capability is affected by different problem settings. Additionally, determining the magnitude of drift necessary for change detection is an indispensable task, as it involves identifying substantial shifts in data distributions. Moreover, the integration of adaptive methodologies is essential for updating ML models in response to data dynamics, enabling them to maintain their effectiveness and reliability in evolving environments. In light of the significance and complexity of the topic, this dissertation offers a fresh perspective on the performance robustness and adaptivity of ML models in non-stationary environments. The main contributions of this research include exploring and organizing the literature, analyzing the performance of ML models in the presence of different types of drift, and proposing innovative methodologies for drift detection and adaptation that solve real-world problems. By addressing these challenges, this research paves the way for the development of more robust and adaptive ML solutions capable of thriving in dynamic and evolving data landscapes.

Keywords: Machine learning, concept drift, covariate shift, performance robustness, evaluation methodology, adaptive learning
Acknowledgements

You were the first home I belonged to. The home that sheltered me, fed me, and taught me my first words. You were, still are, always there whenever I need that dose of comfort, strength, and inspiration- because you never fail to give. Mom, Aisha, to you I credit everything I have achieved in my life. You are the cornerstone of my existence, the home I always go back to. To the cherished memory of the warrior, my beloved late grandmother, Helwa, who instilled in me the essence of hard work and resilience, and who tirelessly embraced the role of a superhero, expecting nothing for unshakeable dedication. The thrilling tales you told, the meals you made, and the invaluable lessons you imparted- all of which I hold dear in my heart. To my brother, Ahmed, I was fortunate enough to witness a truly unique and inspiring journey as you grew from a young child into a beacon of success. Your charitable ventures have not only touched many lives but also become a guiding example for me. I owe you a significant part of whatever I achieve in this life.

I extend my deepest gratitude to my supervisor, Bestoun. Your unconditional guidance and support have played a pivotal role not only in my research but also in a relationship that extends beyond the realms of academia. Your mentorship has been instrumental in shaping my academic journey for the best part of the last two years. I am truly grateful for the knowledge and personal growth I have gained under your guidance. I would also like to express my sincere thanks to my examiner, Andreas Kassler, for the valuable suggestions, assistance, and expertise.

I would also like to convey my sincere appreciation to my uncle, Adeeb, for the profound life advice you have shared with me ever since I was a kid. Your ageless wisdom has been a constant light, undimmed by distance, undeterred by years of conflict you’ve weathered. To my loving sisters, Rasha and Hala, you both are a blessing. You have given my journey a special flavor. I would also like to extend my heartfelt appreciation to Dr. Zakaria for his steadfast support and words of encouragement. Spending time with you has been a precious learning experience that has expanded my horizons.

To my dear friend Rose, it is truly remarkable how our paths converged once again at the same university, a full 12 years since our first encounter. The serendipity of our reunion adds a beautiful layer to the tapestry of our friendship. To the rest of my friends and colleagues Amal, Freysteinn, Mahdi, Manal, Phil, and Zdravka, each of you has contributed to making my journey incredibly interesting and fulfilling. I wouldn’t trade our conversations, camaraderie, and shared meals for the world.

Lastly, I would like to express my heartfelt gratitude to my sporting and life heroes, Andy Roddick, Sir Alex Ferguson and the late Kobe Bryant. Your unwavering examples have taught me that discipline, commitment, and hard work are the foundation of any successful career. Following your achievements as I grew up has been an immense source of inspiration, motivating me to strive for excellence and reach my full potential in my endeavors.

Karlstad, October, 2023
Firas Bayram
1 Introduction

1.1 Motivation

Machine learning (ML), drawing inspiration from the learning processes of human brains, has been widely adopted in various applications and fields, spanning a diverse range of disciplines. Just as humans adapt their learning strategies in response to the underlying prevalent conditions, ML models also need to adapt dynamically to evolving contexts and data in changing environments. In general, ML models infer knowledge from historical data snapshots. However, the assumption that the upcoming data will resemble the past may not always hold in dynamic environments, causing the learned knowledge to become outdated. As data distributions shift over time, ML models may face the phenomenon of concept drift, where the underlying relationships between variables change, leading to performance degradation; this change in relationships is often reflected in shifts of data distributions [1].

Concept drift has been intensively studied in a wide range of fields and applications [2, 3], including healthcare systems [4], fraud detection [5], natural language processing (NLP) [6, 7], and finance [8]. Addressing concept drift is crucial in these applications to ensure the persistent accuracy and reliability of ML-based decisions. Concept drift poses significant challenges in these domains due to the critical nature of applications that require continuous monitoring and adaptation of ML models to changing data distributions [9]. For example, in healthcare systems, accurate predictions and timely decision-making are critical to patient care and treatment planning. In fraud detection, detecting evolving fraud patterns is crucial to preventing financial losses [10]. Similarly, language understanding capabilities must be maintained in NLP despite language usage changes over time. Moreover, in industrial processes, such as manufacturing and quality control, the adaptation of ML models is crucial to ensure high reliability and optimize production efficiency [11]. In finance, an accurate prediction of market trends is essential to make informed investment decisions. Overcoming these challenges requires effective techniques for detecting, handling, and adapting to concept drift to maintain the performance robustness of ML models in real-world applications [12].

Developing robust ML systems with high predictive performance is essential for trustworthy artificial intelligence (AI) applications [13]. This is emphasized by the International Organization for Standardization (ISO)¹ and the International Electrotechnical Commission (IEC)² (ISO/IEC), which have published a report that outlines the characteristics of trustworthy AI systems [14]. Specifically, the report has generally defined the robustness property as “the ability of a system to maintain its level of performance under any condition.” In the context of dynamic environments with shifting data distributions, this definition implies that for an ML system to be robust in a non-stationary environment, it should maintain its performance consistently, regardless of

¹https://www.iso.org/home.html
²https://iec.ch/homepage
1.2 Overarching Themes

The underlying framework of this dissertation revolves around the intricate analysis and scrutiny of learning processes within the dynamic context of non-stationarity. This dissertation explores the challenge of concept drift, which refers to shifting data distributions over time [16]. It also explores innovative approaches to mitigate the adverse effects of these shifts on the robustness of ML models.

1.2.1 Context

The contextual backdrop of any research conducted in non-stationary environments encompasses the ever-evolving nature of data and the inherent challenges that arise from these dynamic changes [17]. The rapid shifts and variations in data distributions require specialized methodologies to ensure the adaptability and robustness of machine learning models [18]. Designing the algorithms of learning solutions for non-stationary environments entails a distinct set of challenges and requirements compared to traditional learning paradigms [19]. It involves considering various aspects and factors specific to non-stationary scenarios, such as concept drift, evolving data distributions, and the need for adaptive learning algorithms [20]. A deeper understanding of the unique characteristics of non-stationary learning can be achieved by comprehending the context and intricacies associated with these challenges. This understanding lays the groundwork for exploring novel approaches and developing tailored strategies that effectively address the complex dynamics of non-stationary environments, going beyond the limitations of traditional learning paradigms.

1.2.2 Problem Description

Learning in non-stationary environments can be formalized as a framework that tackles the challenges of learning when probability distributions change over time. In this framework, the objective is to develop ML models that can continuously adapt to dynamic scenarios. In conventional learning frameworks, it is typically assumed that the data are sampled from an unknown fixed probability distribution \( p_t(x, y) \), at some time point \( t \) [21], where \( x \) represents the feature vector and \( y \) denotes the corresponding output label. However, the underlying probability distribution \( p_t(x, y) \) governing the data generation
process is not static in non-stationary environments. It can vary over time due to various reasons such as changes in user preferences, shifts in the environment, or evolving trends [22]. Additionally, concept drifts can arise due to the dependence of the concept of interest on underlying hidden contexts, which are not explicitly provided as predictive features [23]. This means that certain factors influencing the concept may not be directly observable or included in the available data.

The literature on concept drift suffers from ambiguity and inconsistent terminology, which can create confusion in the research area. However, concept drift formally occurs when \( p(x, y) \) is not the same at different time points [24]. This can be induced by changes in the conditional distribution \( p(y|x) \), where the relationship between the target variable \( y \) and the input features \( x \) varies over time. It can also be caused by changes in the marginal distribution \( p(x) \), where the marginal distribution of the input features itself evolves over time. The decomposition of the joint probability distribution using Bayesian learning theorem as \( p(x, y) = p(y|x) \cdot p(x) \) provides a framework to analyze concept drift from both conditional and marginal distribution perspectives [25]. Additionally, concept drift can take different forms, each with its own characteristics. Sudden shifts occur when there is an abrupt change in the distribution, leading to an immediate difference in the data patterns. Gradual drifts involve a gradual change over time, where the distribution gradually deviates from the initial distribution. Recurring patterns refer to cyclical or seasonal changes in the distribution, where certain patterns or behaviors repeat periodically [26].

Each type of concept drift requires a different approach for handling and adaptation. Recognizing the specific type of drift can guide the selection of appropriate algorithms and techniques to cope with the changing distribution [27]. Therefore the solutions to address concept drift are highly dependent on accurately identifying the type of drift and selecting suitable methods to handle it. Addressing concept drift also involves considering the trade-off between adaptability and stability, also known as the stability-plasticity dilemma [28]. Over-adaptation to every change in the data may lead to model instability and poor generalization. On the other hand, excessive stability may result in models being less responsive to actual changes. Finding the right balance is crucial in maintaining model performance. Furthermore, the concept drift handling methods should be scalable to large-scale datasets and computationally efficient, as real-world applications often involve high-dimensional and streaming data [29, 30]. These considerations form the foundation for designing effective solutions to address concept drift in dynamic learning scenarios.

### 1.2.3 Handling Concept Drift

In the context of non-stationarity, concept drift emerges as a prominent manifestation that demands specialized approaches for accurate detection and effective handling, ensuring the performance robustness of ML models in the long run. Any learning methodology that is employed to address the challenges of
changing data distributions encompasses three main phases [31], as illustrated in Figure 1:

- **Concept drift analysis and understanding**: This phase involves a comprehensive analysis and a deep understanding of several aspects that characterize drift in the system [32]. This includes examining the sources of change, such as external factors or natural evolution, and understanding how these changes affect different regions of the system [33]. It also involves inspecting the severity of the drift, ranging from minor fluctuations to significant shifts in underlying data distributions, and determining the period over which these changes occur and remain active [34]. Also, quantifying the magnitude of drift is essential to better understand the nature and impact of changes, enabling appropriate resource allocation and the adoption of adaptive techniques. Thorough analysis and understanding of these aspects facilitate effective decision-making and the development of strategies to mitigate the impact of concept drift [35].

- **Concept drift detection**: Identifying changes is crucial to diagnosing the evolving characteristics of the system [36]. This component utilizes statistical methods and algorithms that accurately detect concept drift occurrences in real-time or near real-time [37]. By monitoring relevant indicators, such as statistical properties, changes in covariate distributions, or degradation in model performance [38]. Specifically, a family of drift detection methods is based on the comparison of statistical properties of the data distribution at different time points [39]. Measures such as the Kolmogorov-Smirnov statistic, Kullback-Leibler divergence, and Jensen-Shannon divergence can quantify the dissimilarity between probability distributions and indicate the presence of drift [40]. These methods provide a quantitative assessment of
the changes and enable the system to flag alarms or warnings based on the magnitude of drift. Another family of drift detection approaches focuses on monitoring the performance of ML models over time. Degradation in model performance, as measured by metrics such as accuracy, error rate, or F1 score, can indicate concept drift [41]. When the predictive performance of the model drops below a predefined threshold, it suggests that the underlying data distribution has changed, triggering the signal for adaptation. This information allows for proactive adjustments in ML models, ensuring their continued robustness and adaptability in dynamic environments.

- **Concept drift adaptation:** This phase focuses on responding to concept drift occurrences within the system [42]. It involves developing adaptive techniques and algorithms that allow ML models to adjust effectively and align with changing data distributions. These techniques encompass various methods such as model retraining, incremental and online learning, ensemble methods, and data adaptation and refinement [43]. In particular, model retraining is an approach that involves periodically updating the ML model using newly available data. This process allows the model to capture the latest patterns and trends. Similarly, incremental and online learning methods provide another way to handle concept drift by continuously updating the model using new incoming data. These techniques update the model on-the-fly without requiring access to the entire historical dataset [44]. In contrast, ensemble methods, such as bagging, boosting, or stacking, leverage the collective knowledge of multiple models to handle concept drift. By maintaining a diverse set of models and adjusting their weights or selection criteria, ensemble methods can effectively mitigate the impact of the potential bias of individual models [45]. Data adaptation and refinement techniques aim to modify the training data to align with the current data distribution [46]. Approaches such as importance weighting, where the importance of instances is dynamically adjusted based on their relevance to the current concept, can effectively handle drift by assigning higher weights to recently observed instances [47]. This weighting scheme allows the ML model to prioritize learning from more relevant data. Using these strategies, ML models can react to changes and incorporate new information that allows ML models to remain up-to-date and effective in decision-making tasks.

As a final remark, it is essential to emphasize that these phases of concept drift analysis, detection, and adaptation are not isolated steps but rather intertwined and interdependent in practice to maximize system efficiency. They form a continuous feedback loop where each dimension informs and influences the others [48]. The analysis and understanding phase provides valuable insights for the detection phase, and the detected drift instances activate the corresponding adaptation technique. Similarly, the knowledge gained from the adaptation phase contributes to deeper analysis and understanding, enhancing the effectiveness of concept drift detection [49]. This dynamic interaction and interconnectedness create a two-way path between these dimensions, enabling a holistic and iterative approach to handle concept drift and ensuring
1.3 Synopsis

The primary aim of this dissertation is to enhance the reliability and trustworthiness of ML systems that operate in dynamic environments, enabling them to adapt and evolve seamlessly. To achieve this research aim, this dissertation consists of four papers that contribute to different phases of the drift handling methodology. The alignment of these papers with the corresponding phases is illustrated in Figure 2. In Paper I, the literature on concept drift is revisited and organized in a consolidated taxonomy that groups the various drift types according to their mathematical definitions. This taxonomy aims to provide a clearer and more concise overview of the types of concept drift and their sources, which can help researchers overcome the inconsistencies and ambiguities in the definitions used in the literature. Furthermore, paper I presents a comprehensive review of existing approaches to detect concept drift using model performance degradation and analyzes current trends in the research area.

Paper II proposes a novel evaluation framework to assess the robustness of ML models in the case of distributional changes in input data. The evaluation framework includes comprehensive experiments that measure the degradation rates of conventional ML models under covariate shift in various settings of classification problems. Moreover, an evaluation methodology is introduced by decomposing the input space based on the ratio of test-to-training input
densities. This methodology enables the evaluation of model performance per domain-region, providing a more detailed analysis of model robustness.

**Paper III** presents a novel drift-adaptive Long Short-Term Memory (DA-LSTM) learning framework. This framework integrates passive and active drift adaptation techniques and includes a dynamic active drift detection methodology that identifies changes in the data distribution without a fixed drift magnitude threshold. Additionally, an adaptive LSTM network is designed in **Paper III** to handle concept drift by quickly adapting to new trends in load consumption while retaining learned consumption patterns. An extensive evaluation against baseline models is conducted to demonstrate the effectiveness of the proposed DA-LSTM framework, and a trade-off analysis is performed to suggest the appropriate adaptation approach based on prediction performance and computational cost.

**Paper IV** proposes an automated and adaptive approach to address the scalability of ML systems in real-world manufacturing applications. The study focuses on an Electroslag Remelting (ESR) use case process from the Uddeholms AB steel company[^3], specifically predicting the minimum pressure value for a vacuum pumping event. The challenge lies in efficiently integrating new machines into the existing ML software system and accommodating changes in the production environment while maintaining adaptability. To overcome this challenge, the proposed approach utilizes a drift handling technique called importance weighting.

The roadmap of this dissertation and its research attributes, which will be discussed in more detail in the subsequent sections, are summarized in Figure 3.

1.4 Challenges

The literature has presented several challenges that have motivated this work to achieve its research aim. These challenges can be summarized as follows:

**Challenge 1 (C1): Characterizing and organizing concept drift types.** The literature reveals that the existing terminology for concept drift types is inconsistent and ambiguous. This leads to different definitions for the same type of drift and the same definition for different types, resulting in confusion for researchers in the field [50].

**Challenge 2 (C2): Understanding the relationship between concept drift and model degradation.** One of the obstacles in research involves comprehending the way concept drift influences the performance of ML models, leading to their degradation over time [51, 52]. The interplay between concept drift and model degradation is an active area of research that should be investigated.

[^3]: https://www.uddeholm.com/
Figure 3: Connecting the dots: Mapping research questions to key findings and research challenges to the objectives of this dissertation.
1 INTRODUCTION

Challenge 3 (C3): Analyzing the performance robustness of ML models across different regions of the input space. Another challenge in the literature is to scrutinize the performance of ML models across different domain regions of the data input space. It is essential to investigate whether the models trained in one region perform well in other input regions [53]. This challenge is of high importance as it can help identify the regions where the models are expected to fail and the factors that contribute to such failure. Understanding the factors that cause a model to fail in a specific region can help improve the model and develop remedial strategies to overcome these limitations [54].

Challenge 4 (C4): Evaluating performance robustness degradation of ML models in presence of distributional changes. Another challenge in the field is to assess the degradation in the predictive performance of ML models when subjected to distributional shifts, particularly in the context of real-world applications. The ability of a model to maintain its overall efficacy in the face of evolving data is pivotal for its practical utilization, and evaluating its robustness to distributional shifts is necessary to ensure its reliability in the dynamic and often unpredictable scenarios of real-world settings [55].

Challenge 5 (C5): Pre-determining a significance threshold to detect drifts. A challenge in detecting concept drift is the need for a predefined threshold to identify change points in the data. However, this threshold should not be fixed and may need to be adjusted during the evolution of the system, posing a significant challenge [56]. The selection of the threshold is critical, as it can significantly affect the performance of the predictive ML solution [57].

Challenge 6 (C6): Developing adaptive strategies to handle concept drift in real-world applications. In practical settings, ML models often encounter constraints and limitations that make adaptation more challenging compared to controlled experimental environments [58]. These constraints can include resource limitations, computational efficiency requirements, and domain-specific constraints [59]. This challenge involves developing techniques and methodologies, while respecting these constraints, that enable models to handle changes in data distribution without performance loss. Overcoming this challenge requires innovative approaches that strike a balance between adaptability, scalability, computational efficiency, and the specific requirements of the application domain.

1.5 Research Questions

To achieve the research aims of this dissertation, a set of research questions (RQs) is established based on the challenges outlined in the preceding section as follows:
**RQ1** *What inconsistencies and ambiguities exist in the literature regarding the terminology and mathematical definitions used to describe different types of concept drift?*

This research question is set to explore the existing literature concerning the various types of concept drift (C1), along with the mathematical formulations that define each type. The objective is to organize the different types in mathematical representations. The goal is to identify any issues that could cause confusion or hinder the development of accurate solutions for concept drift.

**RQ2** *How is the predictive performance of the model used to track and detect concept drift, and what are the common techniques employed to validate the model’s performance in the context of concept drift and its relation to model degradation over time?*

This research question is formulated to understand how the predictive performance of a model is used to monitor and identify changes in data distributions and what techniques are frequently incorporated to evaluate the model’s performance in cases of concept drift (C2). Furthermore, it investigates the relationship between concept drift and model degradation over time, which can help develop more effective solutions for detecting and addressing concept drift.

**RQ3** *How do different ML algorithms perform in terms of robustness under different drift scenarios, and how does the performance of the algorithms vary across different regions of the input space based on the test-to-training density ratio?*

This question centers around the capabilities of various ML algorithms to sustain high performance levels across diverse drift situations (C3). Moreover, it investigates how these algorithms demonstrate their robustness in different parts of the input space, especially when decomposed based on the test-to-training density ratio. This analysis can provide insight into the strengths and weaknesses of different algorithms under different conditions and help select the most suitable algorithm for a given problem. Furthermore, by analyzing the performance of ML algorithms in different regions of the input space based on the test-to-training density ratio, we can identify the regions where the model tends to fail or perform poorly (C4). This information can be utilized to develop a more robust solution in those regions and improve the overall performance of the model.

**RQ4** *How can a dynamic drift-adaptive framework be developed that can improve performance without relying on a fixed drift threshold?*

This research question is designed to build a flexible and adaptable framework that can adjust the ML models to changes without the need of a predetermined drift threshold (C5). The framework is designed to adapt to changing drift magnitudes in real-time without requiring manual ad-
justments, making it more flexible and efficient than existing approaches. This research question can help in adopting adaptable and scalable solutions for concept drift that are robust to changing conditions over time.

**RQ5** How can adaptive strategies be developed to handle concept drift in real-world applications, considering practical constraints and limitations? This research question focuses on developing adaptive strategies for handling concept drift in real-world applications (C6). It considers the constraints and limitations often encountered in practical settings, such as resource limitations, computational efficiency requirements, and domain-specific constraints. The goal is to devise innovative techniques and methodologies that enable models to adapt to changing data distributions while respecting these constraints.

### 1.6 Contributions

This dissertation makes several contributions to the field of robust ML in non-stationary environments. The main research objectives and findings for each paper are summarized in this section.

#### 1.6.1 Research Objectives

The primary research objectives of this study, referred to as Research Objectives (Objs), are:

**Paper I**

- **Obj1**: To revisit the literature on concept drift and consolidate the various types of drift based on their mathematical definitions to provide a clear and concise overview of concept drift for researchers in the field.

- **Obj2**: To analyze and present a comprehensive review of the existing methods for detecting concept drift using model’s performance degradation and identify current trends in the research area.

**Paper II**

- **Obj3**: To propose a novel tractable evaluation framework that assesses the robustness of ML models under distributional changes in input data across various classification problem settings.

- **Obj4**: To introduce an evaluation methodology that decomposes the input space based on the ratio of test-to-training input densities to provide a detailed analysis of model robustness per domain-region.
1.6 Contributions

Paper III

Obj5: To propose a dynamic drift-adaptive framework for LSTM (DA-LSTM) models that integrates both passive and active drift adaptation techniques.

Obj6: To develop a dynamic active drift detection methodology that identifies changes in the data distribution without a fixed drift magnitude threshold.

Obj7: To evaluate the proposed DA-LSTM framework against baseline models and conduct a trade-off analysis to suggest the appropriate adaptation approach based on prediction performance robustness and computational cost.

Paper IV

Obj8: To provide a solution for scalable industrial processes to address the challenge of adapting the ML systems to accommodate changes quickly, specifically in the context of the Electroslag Remelting (ESR) use case.

Obj9: To propose an automated and adaptive approach based on a drift handling technique called importance weighting to enable the adaptability attribute of the ML system in the ESR use case.

1.6.2 Overview of Research Findings

The following points summarizes the key Research Findings (RFs) from the papers:

Paper I

RF1: A standardized mathematical definition should be used to refer to specific concept drift types to enhance clarity and precision in setting the problem context, eliminating potential confusion.

RF2: Most existing drift detection methods rely on monitoring the error rate of the model, but recent advances have introduced new performance metrics, such as pseudo-error, to evaluate the model’s performance.

RF3: Hoeffding Trees and Naive Bayes are the most commonly used base learners in existing solutions, while neural networks are emerging as a potential alternative.

RF4: Currently, there remains a lack of definitive evidence regarding the optimal drift detector to be employed for a particular problem or context.
Paper II

RF5: Random Forests is the most robust algorithm for distributional shifts in the low-dimensional experiments, showing the lowest degradation rates in the evaluation metrics.

RF6: The complexity of the classification rule holds the most significant impact on performance in high-dimensional experiments among other factors.

RF7: The decomposition of the input space domain into regions based on the test-to-training density ratio can diagnose the models’ performance on subpopulations of the data points and can be used to develop a covariate shift solution based on region-based importance weights.

Paper III

RF8: The proposed DA-LSTM framework can dynamically detect and adapt to changes without requiring a fixed drift threshold, which improves the adaptability and robustness of the solution.

RF9: The evaluation of the solution in terms of prediction performance and computational costs demonstrates its efficiency compared to conventional LSTM and other popular baseline methods.

RF10: An analysis of the trade-off between performance and costs provides suggestions for adopting the appropriate approach in real-life problems.

Paper IV

RF11: The use of the importance weighting technique allows the ML system to adapt to changes and accommodate the addition of new furnaces to the production process efficiently.

RF12: The adaptability of the proposed approach opens new opportunities for industries to integrate expandable solutions into scalable processes by adapting the knowledge extracted from similar previous tasks.

1.7 Conclusions and Outlook

1.7.1 Final Remarks

In this dissertation, we have explored the challenges associated with concept drift in the context of robust ML and proposed a series of research questions to address these challenges. We have noted that there is a lack of consistency and clarity in the terminology used to describe different types of concept drift, which calls for the need to organize the literature and establish a clear taxonomy for the field. We also highlighted the need to evaluate the robustness of ML models to distributional changes and analyze their performance across different regions of the input space. Finally, the importance of developing a dynamic
solution to detect drifts is discussed in the context of real-world applications and use cases.

To achieve the research objectives, a thorough literature review is conducted on concept drift and model degradation, allowing us to identify the key challenges associated with these issues. In addition, a series of experiments are performed to assess the performance of various ML algorithms in different drift scenarios and with varying test-to-training density ratios. Furthermore, a dynamic drift-adaptive framework is proposed that does not require a fixed drift magnitude threshold to detect changes. This approach provides a more flexible and robust solution to concept drift detection and management, which has the potential to significantly enhance the continuous reliability and performance of ML models. Finally, we have shown how to leverage a drift-adaptive technique to solve the issue of integrating new machinery in industrial settings.

1.7.2 Future Directions

Our research has identified several potential future directions to improve the performance robustness of ML models in non-stationary environments. First, further research is needed on the performance of different drift detection methods in various datasets and in specific domains. This will help practitioners select the most appropriate method for the problem, given that no single drift detector outperforms all others in every scenario [60, 61]. Second, based on our observations, a promising avenue for future research involves developing a covariate shift solution based on region-based importance weights that may solve the drawbacks of the point-wise density ratio estimation method [62]. Furthermore, investigating the effects of models’ hyperparameters on coping with distributional changes and evaluating the use of real-world datasets in the evaluation environment are important study directions [63]. This could provide insight into the robustness of ML models in practical scenarios. Moreover, to further validate the conclusions drawn from conventional ML models, future research could focus on evaluating deep learning-based models in non-stationary environments. Finally, the proposed DA-LSTM framework for load forecasting use cases can be extended to other ML-based predictors and data types. For example, the divergence metric can be calculated based on a multivariate probability density function in the multivariate case [64]. Moving forward, pursuing these future directions could lead to significant advancements in the field of ML model robustness, ultimately improving the performance and reliability of ML models in non-stationary environments.
References


List of Publications

The main body of this dissertation consists of the following publications:


Author’s Contribution

I (Firas Bayram) was the main driver and contributor of the all papers. A summary of the contributions is presented in Table 1.

<table>
<thead>
<tr>
<th>Role</th>
<th>Paper I</th>
<th>Paper II</th>
<th>Paper III</th>
<th>Paper IV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conceptualization</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Data curation</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Formal Analysis</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Investigation</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Methodology</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Validation</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Visualization</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Writing - original draft</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Table 1: The individual contributions of this thesis’ author to the appended publications.
Towards Robust and Adaptive Machine Learning

Machine learning (ML) is widely used in various disciplines as a powerful tool for developing predictive models to analyze diverse variables. In the digital era, the abundance of data has created growth opportunities, but it also brings challenges due to the dynamic nature of data. One of these challenges is concept drift, the shifting data distributions over time. Consequently, traditional static models are inadequate for handling these challenges in the online world. Concept drift, with its intricate aspects, presents a challenge for learning algorithms. Analyzing model performance and detecting substantial shifts in data distributions are crucial for integrating adaptive methodologies to update ML models in response to data dynamics, maintaining effectiveness and reliability in evolving environments. In this dissertation, a fresh perspective is offered on the robustness and adaptivity of ML models in non-stationary environments. This research explores and organizes existing literature, analyzes ML model performance in the presence of drift, and proposes innovative methodologies for detecting and adapting to drift in real-world problems. The aim is to develop more robust and adaptive ML solutions capable of thriving in dynamic and evolving data landscapes.