学 位 論 文 内 容 の 要 旨

博士の専攻分野の名称　博士（情報科学）　氏名　BAO Jiaqi

学 位 論 文 題 名

On the Reliability and Robustness of Linear Generalized Regression Algorithms for Classification
（識別のための線形一般化回帰アルゴリズムの信頼度とロバストネスに関する研究）

Machine Learning (ML) continues to progress in various application areas such as healthcare, finance, and autonomous vehicles, where the accuracy of ML models is crucial due to the severe consequences that errors can cause, including harm to humans. The reliability of these models is paramount, particularly when dealing with imperfect data, which is often compromised by various factors: insufficient information due to the high costs associated with manual labeling, data bias stemming from changing environments and privacy concerns, label noise caused by human or sensor errors, and vulnerability to attacks like adversarial noise and distribution shifts.

Despite substantial research efforts in addressing imperfect data challenges in ML, the existing methods have several limitations, such as unsupervised outlier removal can eliminate anomalies but may discard valuable data, reducing classification accuracy. Robust loss Huber loss, known to be effective in regression, performs less well in classification. Regularization techniques mitigate overfitting but struggle with noise. This thesis presents methodologies equipped with robust loss functions that are effective in both classification and regression. Noise-against-regularization techniques and strategies for handling label noise are also addressed. It is structured into three distinct parts, each focusing on addressing specific imperfections in real-world data: Part I focuses on Semi-Supervised Learning (SSL) under limited labeled data, Part II on Transfer Learning (TL) across different data domains, and Part III on Learning with Label Noise, for improving ML model precision and generalizability.

For Part I of the thesis, Semi-Supervised Learning (SSL) frequently confronts the challenge of having only a limited amount of labeled data available for training. Furthermore, the presence of data noise, arising from various sources such as measurement errors or data collection imperfections, can undermine the accuracy of SSL models. To tackle these issues, we introduce Robust Embedding Regression (RER). RER achieves this by constructing a robust graph that adaptively adjusts weights for each data point, effectively reducing the influence of data noise on the learning process. Additionally, RER incorporates a low-rank representation to enhance the utilization of limited labeled data and mitigate the impact of redundant features. Further robustness is achieved through the introduction of appropriate norms to both reconstruction and regularization terms, facilitating feature and sample selection. Our method has been proven through extensive experiments to maintain a classification rate of over 46.67% on datasets with varying degrees of random noise or continuous noise, representing a 32.67% improvement over comparative semi-supervised methods.

In Part II, domain shift introduces disparities and variations in the data that can hinder effective knowledge transfer. To address the imperfections resulting from domain shift, we introduce the Redirected Transfer Learning (RTL) approach. By reconstructing target samples using the lowest-rank

representation obtained from source samples, RTL effectively mitigates the impact of domain shift on data imperfections. Additionally, RTL incorporates the $L_{2,1}$-norm sparsity on the reconstruction and regularization terms to enhance robustness against data variations. RTL also introduces a redirected label strategy that transforms binary labels into continuous values, aiding adaptation to the diverse data distributions resulting from domain shift. The superiority of our method in classification tasks is confirmed on several cross-domain datasets, for example, RTL attained about 5%-10% improvements on average compared to the latest published methods.

Part III of the thesis tackles challenges in Partial Multi-Label Learning (PML), where instances are associated with the incomplete labeling of data, making it difficult to build accurate predictive models. Traditional PML methods, which utilize pre-defined graphs for label disambiguation, lack adaptability to changing data relationships and diminished effectiveness in scenarios with label uncertainty. Common two-step graph-based approaches, involving static graph construction and subsequent label propagation, often result in suboptimal label confidence learning. Addressing these limitations, our research proposes a novel framework named Adaptive Dual Graph Embedding (ADGE) that simultaneously learns dual adaptive graphs and a sparse projection matrix. These graphs, one capturing feature interrelationships and the other focusing on label correlations, are dynamically updated to better handle label noise and enhance label confidence. The integration of an $L_{2,1}$ norm in the projection matrix introduces structured sparsity, prioritizing crucial features for improved model interpretability and robustness against feature noise. Additionally, the sparsity of projection potentially contributes to reducing label ambiguity, further refining the label disambiguation process in PML. Extensive experiments conducted on various partial multi-label databases have confirmed the superiority of the proposed methods.