D2.1 - Report on Initial Upstream IR Systems

Project: NEREO - Neural Information Retrieval and NLP Systems
Grant Agreement: PRIN 2022
Deliverable ID: D2.1
Work Package: WP2 - Upstream IR Systems
Due Date: M12
Lead Beneficiary: UNIPI

---

1. Executive Summary

This report documents the activities, methodologies, and results of **Work Package 2 (Upstream IR Systems)** during the first year of the NEREO project. The overarching goal of WP2 is to evolve Information Retrieval (IR) from a standalone tool for human users into a robust, "upstream" component for cascading AI systems. In Year 1, we successfully addressed critical limitations regarding **robustness** (L2) and **stability** (L1), laying the groundwork for safe integration with downstream NLP reasoners. Key achievements include the characterization of neural ranker vulnerability to data poisoning, the mitigation of cold-start issues via GNNs, and the formulation of new stability metrics.

2. Detailed Research Activities

2.1 Robustness and Security in Neural Ranking (Task 2.2)

Related Publications: ECIR 2024, IIR 2024, Neural Networks 2024, RobustRecSys 2024

Neural ranking models, particularly those based on Transformers (e.g., BERT4Rec, SASRec), have shown superior performance but lack the robustness required for automated pipelines.

- **Data Poisoning Analysis:** In *"Investigating the Robustness of Sequential Recommender Systems Against Training Data Perturbations"* (ECIR 2024), we conducted the first comprehensive study on how "negatively relevant" (poisoned) training data affects sequential recommenders. We simulated attacks where adversaries inject malicious interaction sequences to manipulate the model's output. Our findings reveal that Transformer-based models are highly sensitive to these perturbations, with performance drops of over 30% under targeted attacks.
- **Defensive Strategies:** We proposed and evaluated several defense mechanisms, including **robust training paradigms** that dynamically weight training samples based on their likelihood of being adversarial. This directly addresses the project's **Limitation L2** (Lack of proper modelling of negatively relevant documents).
- **Topological Loss Analysis:** To understand *why* these vulnerabilities exist, we employed techniques from Algebraic Topology. In *"A topological description of loss surfaces based on Betti Numbers"*, we mapped the loss landscape of neural networks, identifying that "sharp" minima (often associated with poor generalization and robustness) correlate with specific Betti numbers. This theoretical insight guides the design of more stable architectures.

2.2 Addressing Data Sparsity and Cold Start (Task 2.1)

Related Publications: CIKM 2024, WWW 2024

For an upstream IR system to effectively feed a downstream reasoner, it must be able to retrieve relevant information even when user history or item metadata is sparse (Cold Start).

- **Graph Neural Networks (GNNs) for Represenation:** In *"Mitigating Extreme Cold Start in Graph-based RecSys through Re-ranking"* (CIKM 2024), we tackled the "extreme cold start" problem (users with <5 interactions). We developed a hybrid architecture that constructs a user-item interaction graph and applies a GNN to propagate collaborative signals from high-degree nodes to sparse nodes.
- **Re-ranking Strategy:** Crucially, we implemented a post-hoc **re-ranking stage** that refines the GNN output. This two-stage approach ensures that the "upstream" signal sent to the user (or downstream system) maximizes utility even in data-scarce environments.
- **Industrial Scalability:** The efficacy of these graph-based methods was further validated in a huge-scale deployment at Spotify (*"Personalized Audiobook Recommendations at Spotify"*, WWW 2024), proving that Heterogeneous GNNs can model complex, multi-modal interactions (users, audiobooks, authors) efficiently.

2.3 New Metrics for Ranking Stability (Task 2.3)

Related Publications: IIR 2024 (FRBO)

In cascading systems, if the upstream ranker is unstable (i.e., small changes in query/index produce large changes in ranking), the downstream NLP component suffers from inconsistent context.

- **Finite Rank-Biased Overlap (FRBO):** We introduced FRBO to address the shortcomings of existing overlap measures (like RBO) which do not properly handle finite lists or varying lengths. FRBO provides a mathematically rigorous way to quantify the **consistency** of retrieved lists. This metric is now used to evaluate effectively the stability of our upstream models, contributing directly to **Objective O1**.

3. Impact on NEREO Objectives

The activities in Year 1 have advanced the NEREO agenda significantly:

1. **Objective O2 (Modelling Damaging Documents):** By quantifying the impact of "poisoned" data, we have taken the first step towards explicitly modeling "negative relevance" in the training loop.
2. **Objective O3 (End-to-End Optimization):** The GNN re-ranking work optimizes the *quality* of the retrieved set in difficult conditions (cold start), ensuring that the cascading system (WP3) receives the best possible "context" to reason over.
3. **Limitations Addressed:** We have directly tackled **L2** (lack of robust modeling) and **L4** (industry adoption) through our reproducibility and industrial application papers.

4. Conclusion and Next Steps

WP2 has successfully transitioned from "standard" neural IR to "robust and stable" neural IR. The models developed in Year 1 (Robust SASRec, GNN-Rec) are now ready to be used as reliable inputs for the Cascading IR/NLP experiments in WP3. Year 2 will focus on **efficiency** (Task 2.1 continuation) and **interpretability** of these upstream representations.

---

5. Scientific References

2024

- **Mitigating Extreme Cold Start in Graph-based RecSys through Re-ranking.**
  Alessandro Sbandi, Federico Siciliano, and Fabrizio Silvestri.
  CIKM 2024.
  [DOI: 10.1145/3627673.3680069]

- **Investigating the Robustness of Sequential Recommender Systems Against Training Data Perturbations.**
  Filippo Betello, Federico Siciliano, Pushkar Mishra, and Fabrizio Silvestri.
  ECIR 2024.
  DOI: 10.1007/978-3-031-56060-6_14

- **Finite Rank-Biased Overlap (FRBO): A New Measure for Stability in Sequential Recommender Systems.**
  Filippo Betello, Federico Siciliano, Pushkar Mishra, and Fabrizio Silvestri.
  IIR 2024.
  URL

- **Personalized Audiobook Recommendations at Spotify Through Graph Neural Networks.**
  Marco De Nadai, Francesco Fabbri, Paul Gigioli, Alice Wang, Ang Li, Fabrizio Silvestri, Laura Kim, Shawn Lin, Vladan Radosavljevic, Sandeep Ghael, David Nyhan, Hugues Bouchard, Mounia Lalmas, and Andreas Damianou.
  WWW 2024.
  DOI: 10.1145/3589335.3648339

- **A topological description of loss surfaces based on Betti Numbers.**
  Maria Sofia Bucarelli, Giuseppe Alessio D'Inverno, Monica Bianchini, Franco Scarselli, and Fabrizio Silvestri.
  Neural Networks, 178, 106465.
  DOI: 10.1016/j.neunet.2024.106465