Week 3: Influencing Thought for Fun or Profit

Nate Bachmeier

TIM-8150: Artificial Intelligence

October 4, 2020

Northcentral University

# Influencing Thought for Fun or Profit

The NCU Political Action Committee (NPAC) seeks to promote its ideology through highly targeted censorship. Modern censorship does not restrict free speech; instead, it increases the noise and drowns the signal (Thomas, 2019). One critical challenge the organization faces is its ability to scale-out personalized communications with potential voters. Traditionally, businesses approach these problems by either hiring armies of people or resorting to mass marketing campaigns. However, NPAC lacks funding to employ a large staff, and modern spam filters reduce email blasts’ effectiveness.

Instead, NPAC chooses to modernize its tactics and focus solely on Natural Language Processing (NLP) and social media graphs. “[…] NLP is an interdisciplinary field [that] studies and develops algorithms and systems, enabling computers to understand and perform tasks involving human language (Sintoris & Vergidis, 2017, p. 135).” NPAC plans to use these technologies to both parse free form text and also produce novel commentary. Maximizing the resonation of custom content with the audience requires a personalized voice. For instance, the manner that people speak in an academic forum differs from Facebook or Twitter. NLP language models can assist in these situations as well by adopting different vocabularies and alternative sentence structures.

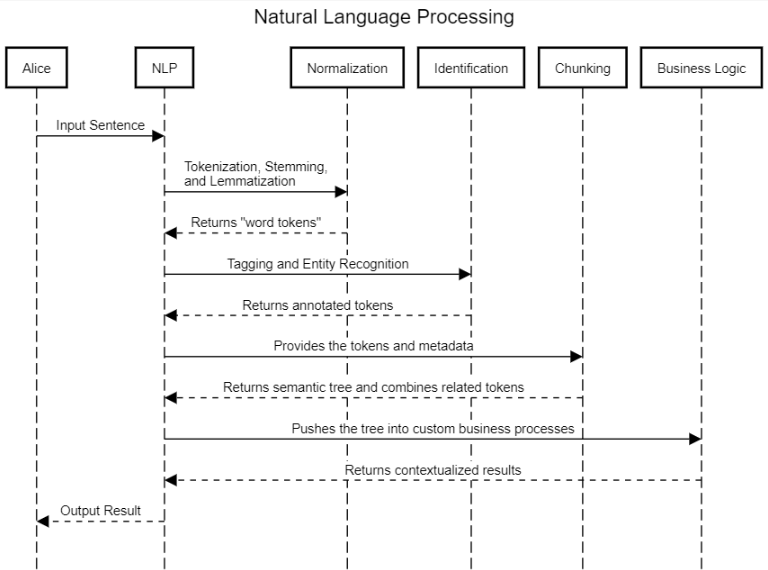
# How does NLP work

Natural Language Processing (NLP) sits at the intersection of artificial intelligence, human language, and computer science.

## Language Parsing

NLP systems typically follow sentence normalization, token annotation and combining, and finally perform custom business logic (see Figure 1) (Edureka, 2018). Using strategies like Lemmatiziation and Stemming enables the parsers to reduce the variability between sentences, such as removing verb-tensing. Next, the words collect annotations by subsystems like Named Entity Recognition (NER) to discover the sentence’s critical components. After chunking related tokens together, the scenario-specific business logic can operate on a semantic representation of the text. Depending on the use-case, these steps could be massive subsystems or single lines of code.

Figure 1: NLP Process



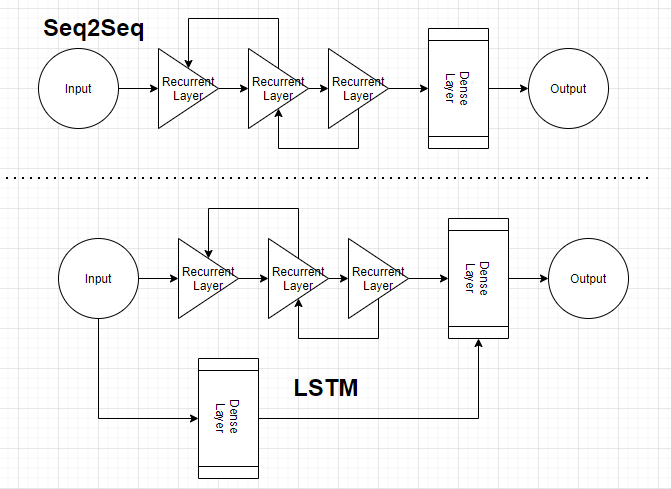
## Deep Learning

NLP appears across a wide range of use cases like language translation, speech-to-text, and sentiment analysis. In biology, animal brains accomplish these tasks through meshes of neurons that transmit signals across connected synaptic (transforming) and activation (filtering) links (Keller, Liu, & Fogel, 2016). Computer scientists mimic this behavior with Deep Learning on Neural Networks, which are essentially weighted graphs. Generally, the network architecture implements a Recurrent Neural Network (RNN) structure, which means that connectivity loops exist in the graph (see Table 1). More advanced designs include subnets for memory retention (see Figure 2), encoding and decoding segments, and greater parallelization from attention vectors (Fu, 2019). Researchers and engineers can add or remove these subsystems to optimize for a specific use-case.

Table 1: Example Algorithms of NLP

|  |  |
| --- | --- |
| Algorithm | Description |
| seq2seq | Simple Recurrent NN (RNN) for a token sequence to sequence prediction. These systems are easy to implement but lack memory |
| Long Short Term Memory | Extends the seq2seq by including a “long term” cache to hold context information |
| Transformers | State of the art solution for massively parallel NLP through attention vectors and position encoding |

Figure 2: Abstract Diagram of Differences

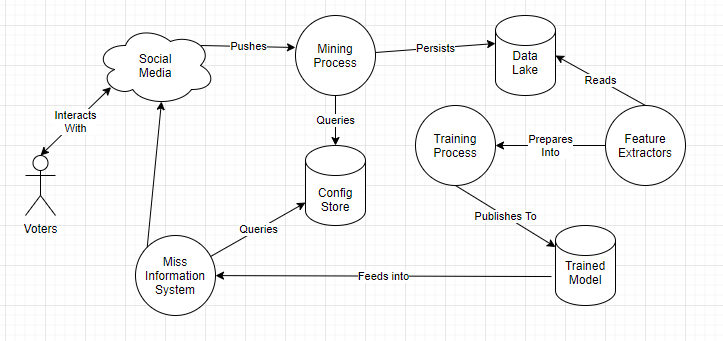


# Resources and Implementation

## Ingestion Subsystem

NPAC operates a distributed system that is continuously mining social media platforms and persisting that information into a data lake (see Figure 3). This aspect of the system utilizes WebSockets to stream updates into the big data system. When these results arrive in the data lake, they are semi-structured JSON (JavaScript Object Notation) with numerous opaque strings. Additional details of this subsystem are outside the scope of this paper.

Figure 3: System Design



## Feature Extraction Process

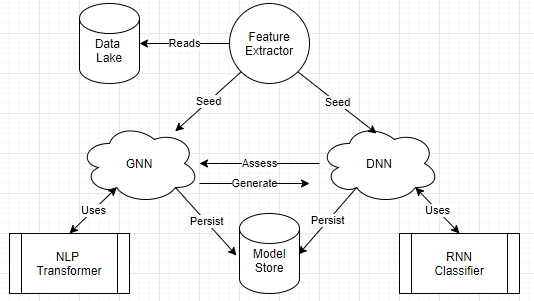
The first steps to any business intelligence problem are identifying the specific questions and locate facts that support answers (Snee, 2015). When researchers ignore this preparation, it produces in garbage-in/garbage-out results. For instance, Alsudias et al. (2014) built an NLP system for predicting where the user was during the submission (e.g., restaurant or night-club). Their approach extracts keywords from Yelp reviews (using term frequency), business metadata (e.g., name and location), and tweet metadata (e.g., timestamp). These features flow into a random forest classifier that determines the location with a 74% accuracy. However, using only the business metadata produces an 88% accuracy, indicating that these additional details provide negative value.

NPAC has specific requirements to model social media users’ speech patterns and then create new content in their voice. The Feature Extraction Process must therefore consider the user’s metadata (e.g., age and locale), the online community properties (e.g., forum name), the posted content, and any quality ratings (e.g., Facebook Likes). There are several considerations to augment this process. For instance, adding a filtration step to remove comments with negative ratings might create more well-liked personalities. However, it could also be advantageous to generate trolls that argue an alternative position, reinforcing NPAC’s position that the other side is illegitimate or less sophisticated.

## Training Process

Around 2014, GAN (Generative Adversarial) Networks became the state-of-the-art approach to produce high-quality fabricated content (Fridman, 2020). These systems utilize a feedback loop between a Generative NN (GNN) and Discriminator NN (DNN). Each iteration outputs a ‘Deep-Fake’ asset and assesses its likelihood of being legitimate. This process enables both systems to learn from one another, continuously improving. According to Fridman (2020), it an arms race to detect Deep Fakes because any advances in DNN naturally improve GNN results. NPAC leverages this methodology for self-teaching its systems to deliver more accurate content (see Figure 4). The organization’s solution uses the NLP transformer to improve parallelization over LSTM and a second RNN classification network. During the training process, periodic snapshots archive the content and model state for offline troubleshooting use cases.

Figure 4: Training Configuration



## Inference Process

The last stage of NPAC’s misinformation system is a crawler that pushes its message across social media. Publishing content first collects metadata about an online thread, the participant’s demographic details (e.g., age group), and summarizing most liked comments. Having these details aids in making the generation more relevant, improves the chances of being upvoted, and increases user impressions. This aspect of the publishing pipeline is still in the early stages, but initial tests seem promising.

# Future Advances