Deep Learning to Detect Novel Behaviours in Traces

Quentin Fournier

Polytechnique Montréal
Laboratoire DORSAL

Roadmap

1. Learn a representation of traces[1]
2. Detect novel behaviours in traces
3. Classify novel behaviours as normal or abnormal

[1] On Improving Deep Learning Trace Analysis with System Call Arguments

Desirable Properties

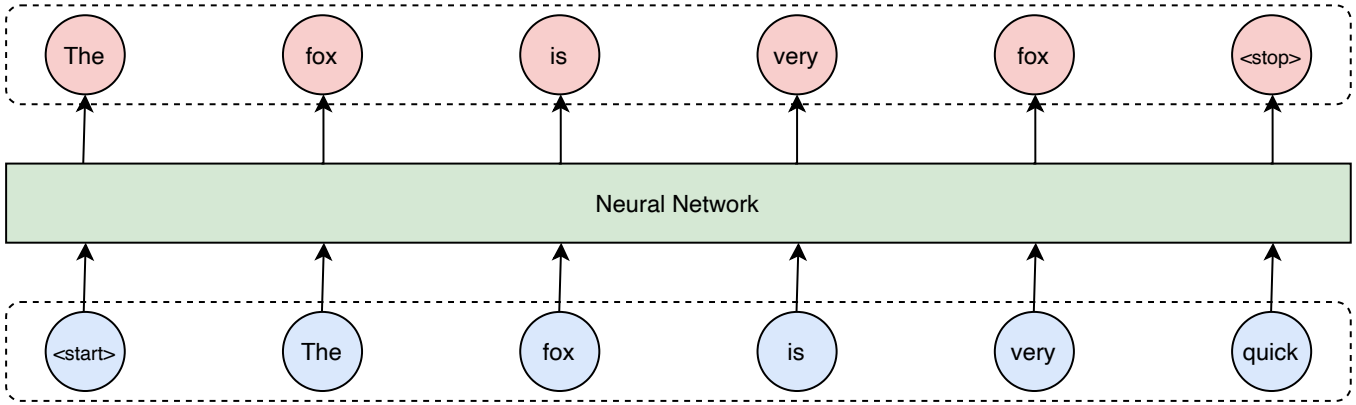
- Unsupervised:
  - Labelling is time consuming and error-prone
  - Labels may change over time
- Robust:
  - Traces are noisy
  - Systems change rapidly
- Transparent:
  - Models may remember the data instead of solving the task
  - Models may fail in rare cases

Methodology

- State-of-the-art neural network called Transformer
  - Flexible enough to model complex interactions in traces
  - Memory intensive and sensitive to hyperparameters
- Considers the event arguments
  - Improves the prediction accuracy
  - Maybe improve the robustness
  - Requires more data to train

Methodology

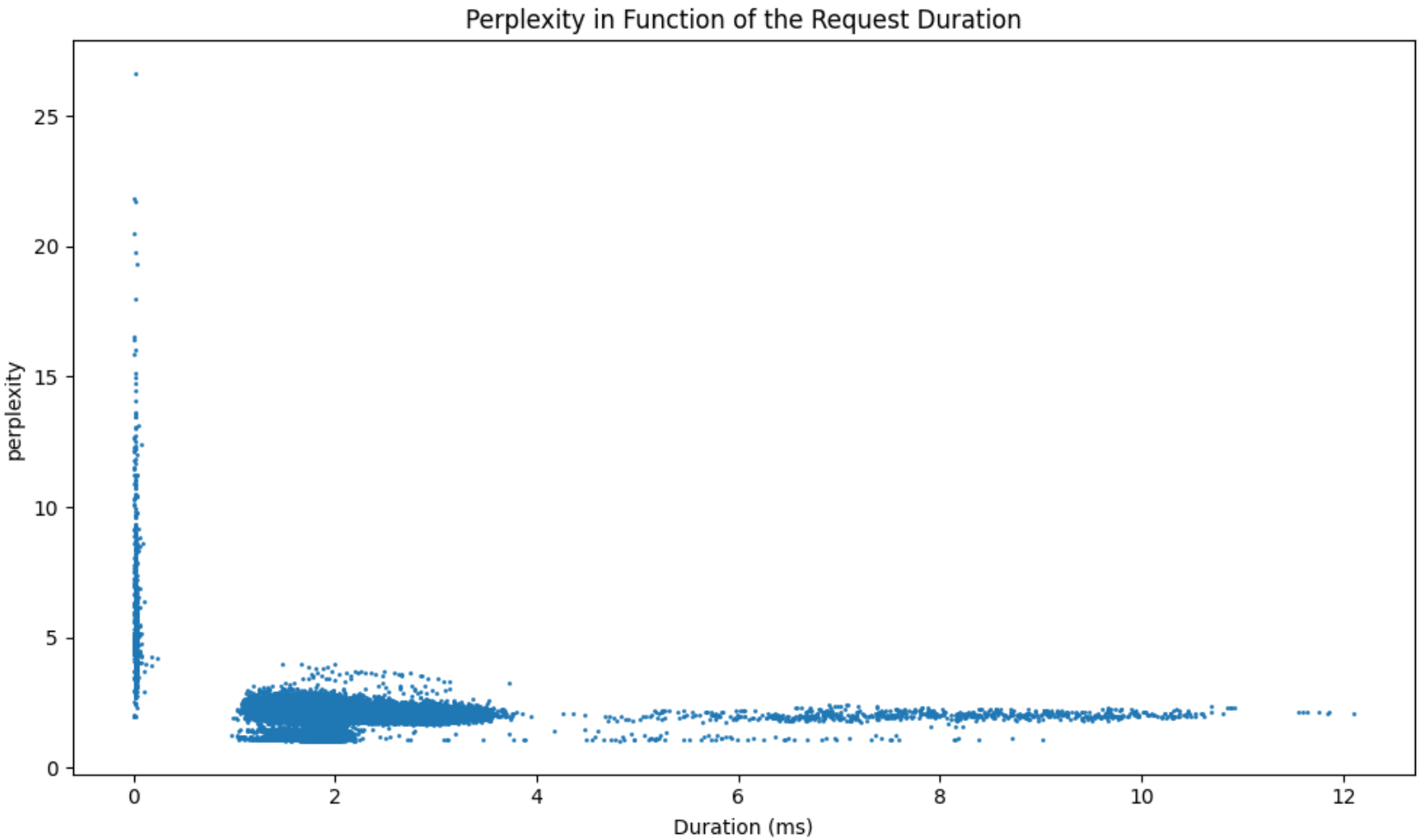
- Unsupervised language model objective
  - Computes the likelihood of sequences
  - Detects unexpected sequences with low probability



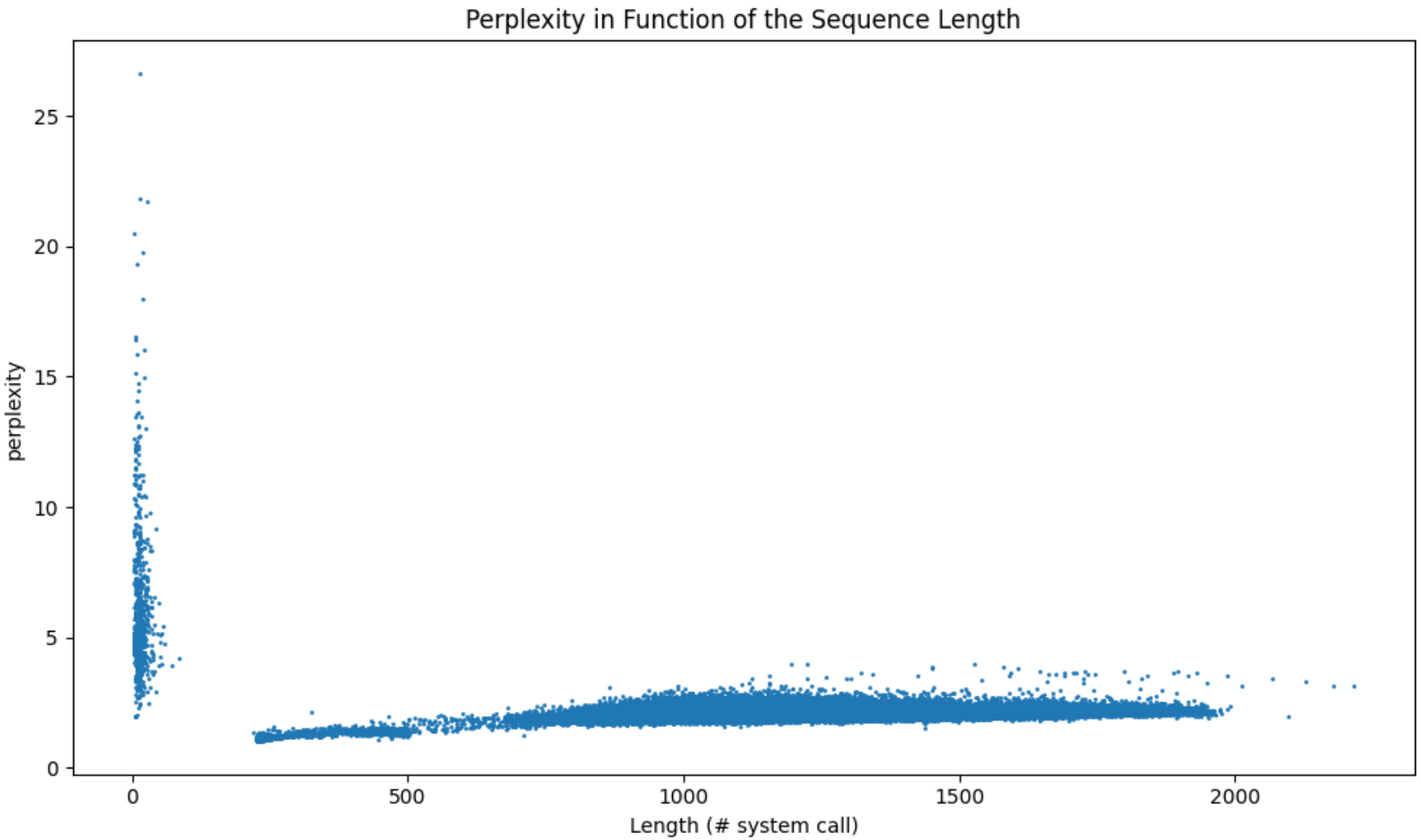
Methodology

- Large dataset collected in a controlled environment
  - 500,000+ web requests
  - Simple enough to evaluate the methodology
  - Too simple to represent real-world use cases
- I am looking for use cases !

Preliminary Results



Preliminary Results



Thank You