Comparing Natural Language Embeddings for Libc Functions as Rich Labels

Bachelor defense

Ruben Triwari

Ludwig Maximilian University Munich

19, February 2025

Outline

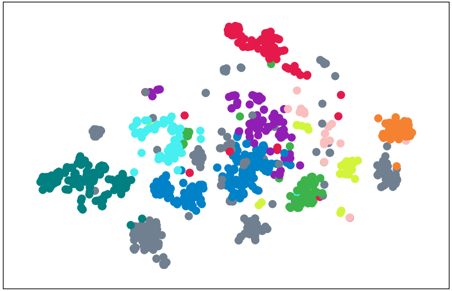
Motivation & Research Objective

Methodology

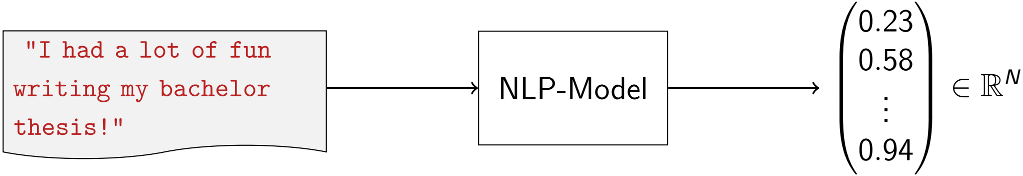
Results

Limitations

Conclusion & Future Work

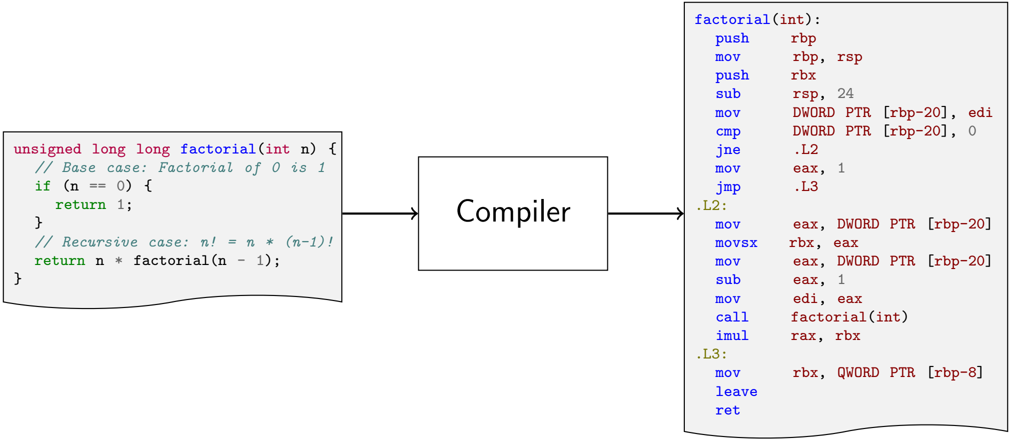


Motivation


"I had a lot of fun writing my bachelor thesis!"
NLP-Model
$\begin{pmatrix} 0.23 \\ 0.58 \\ \vdots \\ 0.94 \end{pmatrix} \in \mathbb{R}^N$

- ⇝ Encoding natural language was a huge factor in recent nlp advancements
- ⇝ Information described as a vector can be used in many downstream task
- ⇝ That motivates encoding binary code and describing them as a vector
- ⇝ That motivates using NLP tools to encode binary code

Motivation



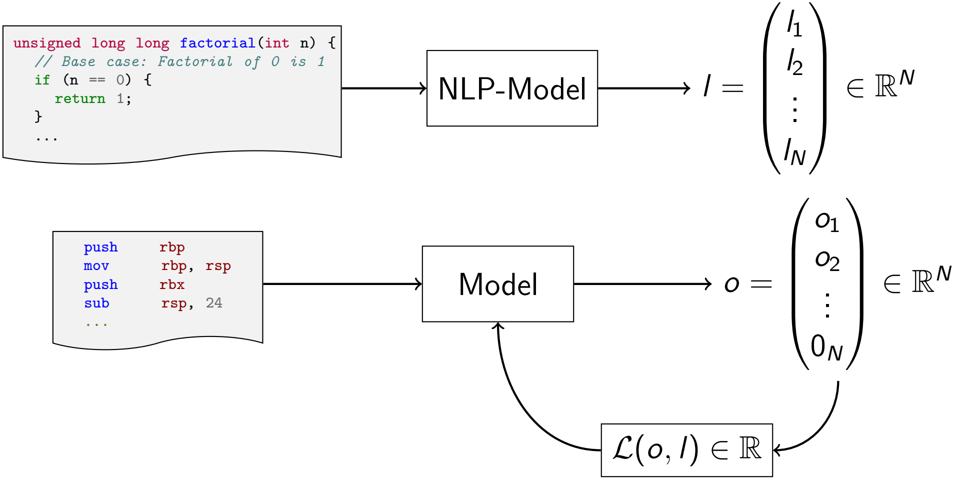
```
unsigned long long factorial(int n) {
  // Base case: Factorial of 0 is 1
  if (n == 0) {
    return 1;
  }
  // Recursive case: n! = n * (n-1)!
  return n * factorial(n - 1);
}
```

Compiler

```
factorial(int):
  push    rbp
  mov     rbp, rsp
  push    rbx
  sub     rsp, 24
  mov     DWORD PTR [rbp-20], edi
  cmp     DWORD PTR [rbp-20], 0
  jne     .L2
  mov     eax, 1
  jmp     .L3
.L2:
  mov     eax, DWORD PTR [rbp-20]
  movsx   rbx, eax
  mov     eax, DWORD PTR [rbp-20]
  sub     eax, 1
  mov     edi, eax
  call    factorial(int)
  imul    rax, rbx
.L3:
  mov     rbx, QWORD PTR [rbp-8]
  leave
  ret
```

⇝ Compiler removes important inforamtion in natural language

Motivation



```
unsigned long long factorial(int n) {
  // Base case: Factorial of 0 is 1
  if (n == 0) {
    return 1;
  }
  ...
```

$$l = \begin{pmatrix} l_1 \\ l_2 \\ \vdots \\ l_N \end{pmatrix} \in \mathbb{R}^N$$

```
    push      rbp
    mov       rbp, rsp
    push      rbx
    sub       rsp, 24
    ...
```

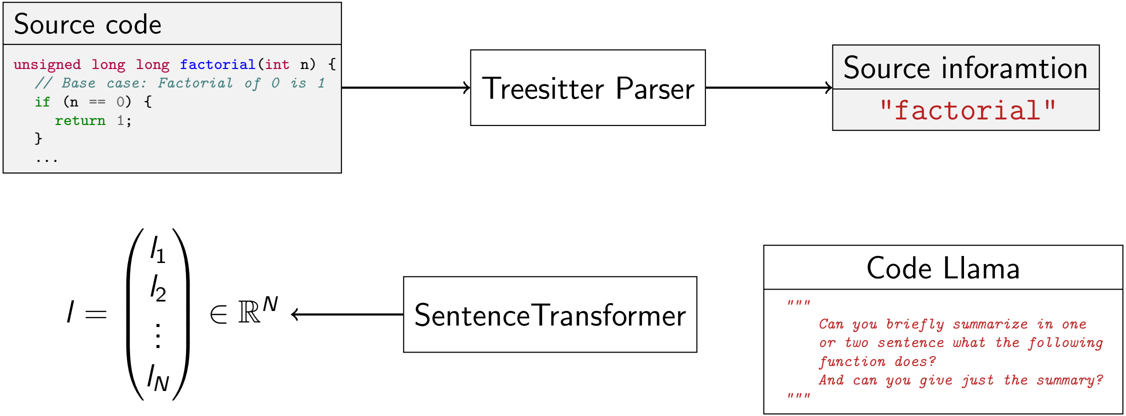
$$o = \begin{pmatrix} o_1 \\ o_2 \\ \vdots \\ 0_N \end{pmatrix} \in \mathbb{R}^N$$

$$\mathcal{L}(o, l) \in \mathbb{R}$$

Research Objectives

- Compare diffrent approaches generating an Embedding with NLP tools
  1. Embed function names with SentenceTransformer
  2. Embed function comments with SentenceTransformer
  3. Embed Code-Llama code summaries with SentenceTransformer
- Compare NLP approach to the existig Code2Vec Model
- Propose a new way comparing embedding spaces

Architecture



```
unsigned long long factorial(int n) {
  // Base case: Factorial of 0 is 1
  if (n == 0) {
    return 1;
  }
  ...
```

```
"""
    Can you briefly summarize in one
    or two sentence what the following
    function does?
    And can you give just the summary?
"""
```

$$I = \begin{pmatrix} I_1 \\ I_2 \\ \vdots \\ I_N \end{pmatrix} \in \mathbb{R}^N$$

Denotational Semantics

HALLO

HALLO

Discussion