

RQ1: Type Accuracy

This experiment is in the `Section V-B Accuracy of Type Reasoning` of our paper. The goal of this experiment is to measure the accuracy of the type information inferred by TYPEORACLE. The result is shown in the `TABLE I: Accuracy of type reasoning` in our paper. We analyzed 251 binding calls for Adobe Reader and 193 for Foxit Reader. In this dataset, the number of parameters ranges from 0 to 40 (1.9 per binding call on average), and the number of parameter types ranges from 0 to 5 (1.3 per binding call on average). TYPEORACLE has almost 100% precision and around 96% recall. As a comparison, type reasoning by using error message provides moderate precision but poor recall (<30%), while using path length provides both low precision and recall (<40%). This demonstrates the need for sophisticated feature (rather than the shallow ones) in type reasoning.

TABLE I: Accuracy of type reasoning.

	Inferred by TYPEORACLE						Inferred by Error Message						Inferred by Path Length					
	Boolean	Number	String	Array	Object	Total	Boolean	Number	String	Array	Object	Total	Boolean	Number	String	Array	Object	Total
# of correctly reported	112	80	329	16	6	543	3	19	6	2	0	30	8	35	21	4	0	68
# of reported cases	112	80	330	16	6	544	6	19	6	2	0	33	27	189	34	258	31	539
# of actual cases	115	81	337	19	6	558	115	81	337	19	6	558	115	81	337	19	6	558
precision	100.0%	100.0%	99.7%	100.0%	100.0%	99.8%	50.0%	100.0%	100.0%	100.0%	0.0%	90.9%	29.6%	18.5%	61.8%	1.6%	0.0%	12.6%
recall	97.4%	98.8%	97.6%	84.2%	100.0%	97.3%	2.6%	23.5%	1.8%	10.5%	0.0%	5.4%	7.0%	43.2%	6.2%	21.1%	0.0%	12.2%

(a) on Adobe Reader

	Inferred by TYPEORACLE						Inferred by Error Message						Inferred by Path Length					
	Boolean	Number	String	Array	Object	Total	Boolean	Number	String	Array	Object	Total	Boolean	Number	String	Array	Object	Total
# of correctly reported	77	53	140	17	3	290	6	26	48	6	1	87	12	31	61	12	2	118
# of reported cases	77	53	140	17	3	290	6	26	48	6	1	87	21	81	67	104	31	304
# of actual cases	78	60	144	18	4	304	78	60	144	18	4	304	78	60	144	18	4	304
precision	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	57.1%	38.3%	91.0%	11.5%	6.5%	38.8%
recall	98.7%	88.3%	97.2%	94.4%	75.0%	95.4%	7.7%	43.3%	33.3%	33.3%	25.0%	28.6%	15.4%	51.7%	42.4%	66.7%	50.0%	38.8%

(b) on Foxit Reader

folder structure

We use three methods to infer the type information, which are `ErrorMessage`, `PathLength` and `TypeOracle`.

`ErrorMessage`: the type that can cause exception when being executed will not be considered as the inferred type.

`PathLength`: the type which has the longest path length will be considered as the inferred type.

`TypeOracle`: the type which cover the type indicator in the differential results will be considered as the inferred type.

The following is the folder structure.

```
ErrorMessage (the method to infer type information)
- adobe reader (information of adobe reader)
  - data/
    - inferred_type/: type information generated by ErrorMessage
    - ground_truth/: correct type information (from reverse engineering)

- utility/
  - cmp_arg.py: the script file to compare type information

- result/
  - adobe.txt: accuracy log file (the detail of accuracy comparasion)
```

- foxit reader (information of foxit reader)
 - data/
 - inferred_type/: type information generated by ErrorMessage
 - ground_truth/: correct type information (from reverse engineering)
- utility/
 - cmp_arg.py: the script file to compare type information
- result/
 - foxit.txt: accuracy log file (the detail of accuracy comparasion)

PathLength (the method to infer type information)

- adobe reader (information of adobe reader)
 - data/
 - inferred_type/: type information generated by PathLength
 - ground_truth/: correct type information (from reverse engineering)
- utility/
 - cmp_arg.py: the script file to compare type information
- result/
 - adobe.txt: accuracy log file (the detail of accuracy comparasion)
- foxit reader (information of foxit reader)
 - data/
 - inferred_type/: type information generated by PathLength
 - ground_truth/: correct type information (from reverse engineering)
- utility/
 - cmp_arg.py: the script file to compare type information
- result/
 - foxit.txt: accuracy log file (the detail of accuracy comparasion)

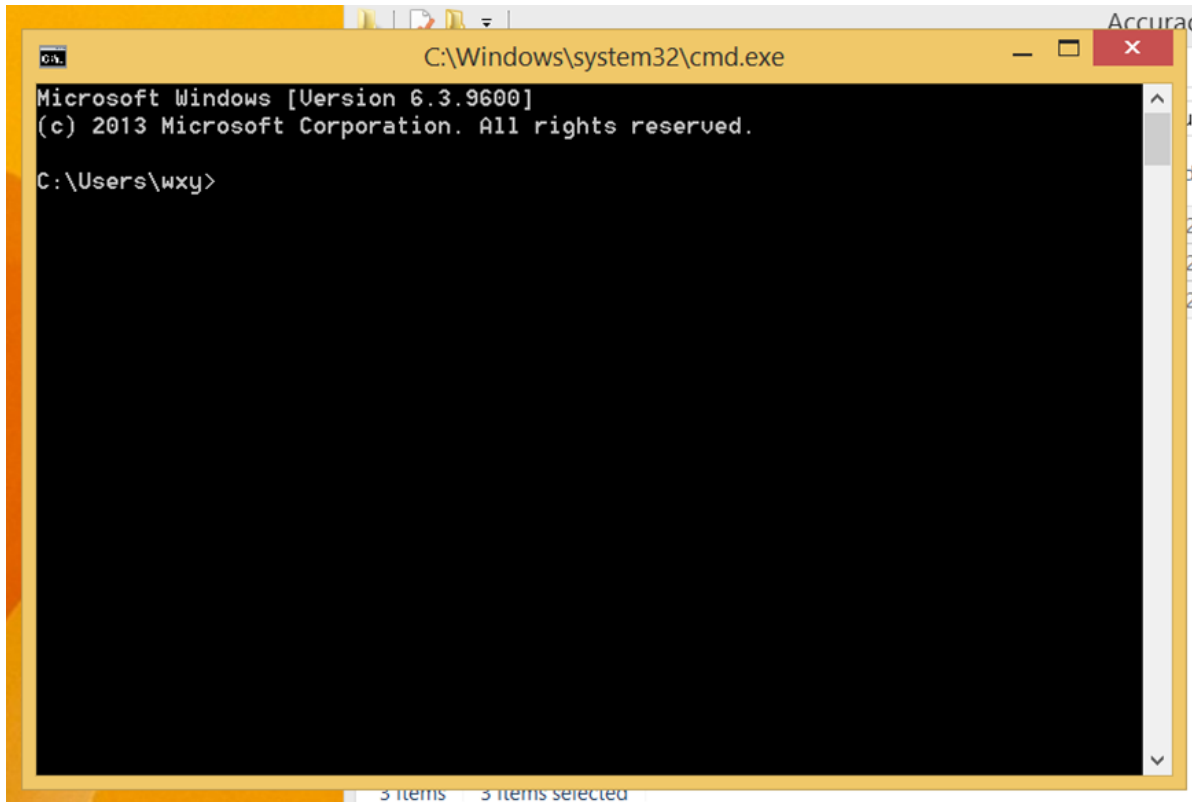
TypeOracle (the method to infer type information)

- adobe reader (information of adobe reader)
 - data/
 - inferred_type/: type information generated by TypeOracle
 - ground_truth/: correct type information (from reverse engineering)
- utility/
 - cmp_arg.py: the script file to compare type information
- result/
 - adobe.txt: accuracy log file (the detail of accuracy comparasion)
- foxit reader (information of foxit reader)
 - data/
 - inferred_type/: type information generated by TypeOracle
 - ground_truth/: correct type information (from reverse engineering)
- utility/
 - cmp_arg.py: the script file to compare type information
- result/

- foxit.txt: accuracy log file (the detail of accuracy comparasion)

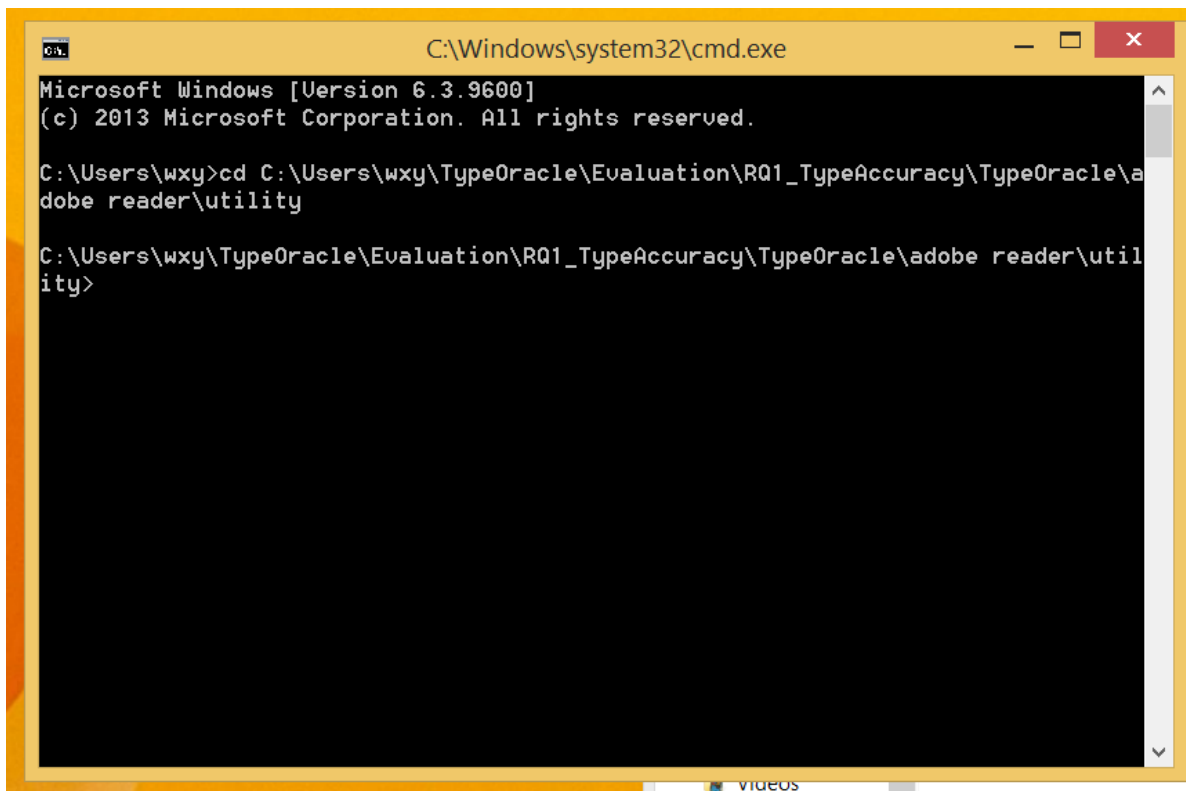
how to reproduce

1. open cmd.exe



2. cd to the utility folder (we use TypeOracle as an example)

```
cd C:\Users\wxy\TypeOracle\Evaluation\RQ1_TypeAccuracy\TypeOracle\adobe  
reader\utility
```



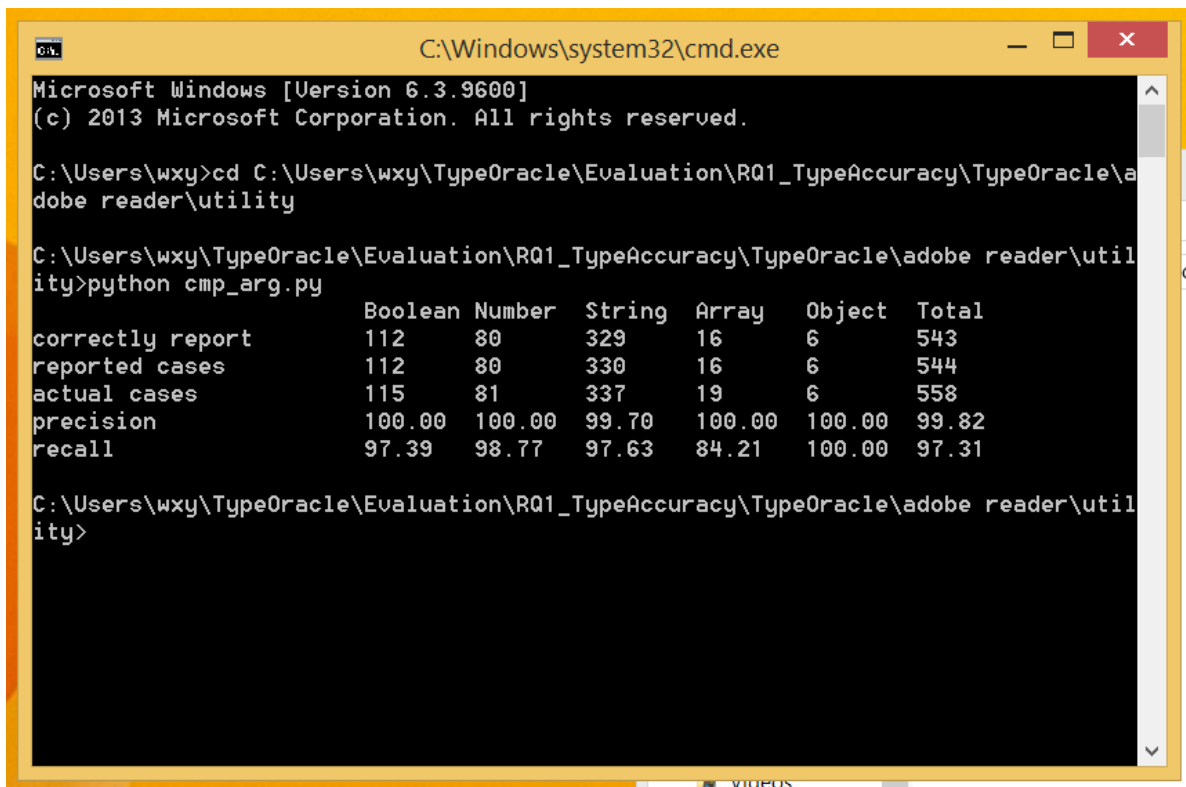
```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\wxy>cd C:\Users\wxy\TypeOracle\Evaluation\RQ1_TypeAccuracy\TypeOracle\adobe reader\utility

C:\Users\wxy\TypeOracle\Evaluation\RQ1_TypeAccuracy\TypeOracle\adobe reader\utility>
```

3. execute the following command and you will see the result.

```
python cmp_arg.py
```



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\wxy>cd C:\Users\wxy\TypeOracle\Evaluation\RQ1_TypeAccuracy\TypeOracle\adobe reader\utility

C:\Users\wxy\TypeOracle\Evaluation\RQ1_TypeAccuracy\TypeOracle\adobe reader\utility>python cmp_arg.py

correctly report      Boolean Number  String  Array  Object  Total
reported cases       112      80     329    16      6     543
actual cases         115      81     337    19      6     558
precision            100.00  100.00  99.70  100.00  100.00  99.82
recall               97.39   98.77   97.63  84.21   100.00  97.31

C:\Users\wxy\TypeOracle\Evaluation\RQ1_TypeAccuracy\TypeOracle\adobe reader\utility>
```

4. you can see the details of comparison from adobe.txt/foxit.txt(in the same directory)

```
C:\Users\wxy\TypeOracle\Evaluation\RQ1_TypeAccuracy\TypeOracle\adobe reader\utility\adobe.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
binding call: this.Collab.AFCheckSubmitButtonStatus
- parameter0:
- inferred type: String
- ground_truth: String
binding call: this.Collab.AFPPrepareFormForDistribution
- parameter0:
- inferred type: String
- ground_truth: String
binding call: this.Collab.AVUMAddStringToPayloadWrapper
- parameter0:
- inferred type: String
- ground_truth: String
- parameter1:
- inferred type: String
- ground_truth: String
binding call: this.Collab.AVUMLogEventWrapper
- parameter0:
- inferred type: String
- ground_truth: String
- parameter1:
- inferred type: String
- ground_truth: String
- parameter2:
- inferred type: String
- ground_truth: String
binding call: this.Collab.AVUMStartPayloadWrapper
- parameter0:
- inferred type: String
- ground_truth: String
- parameter1:
```