Intentions Fuzzing

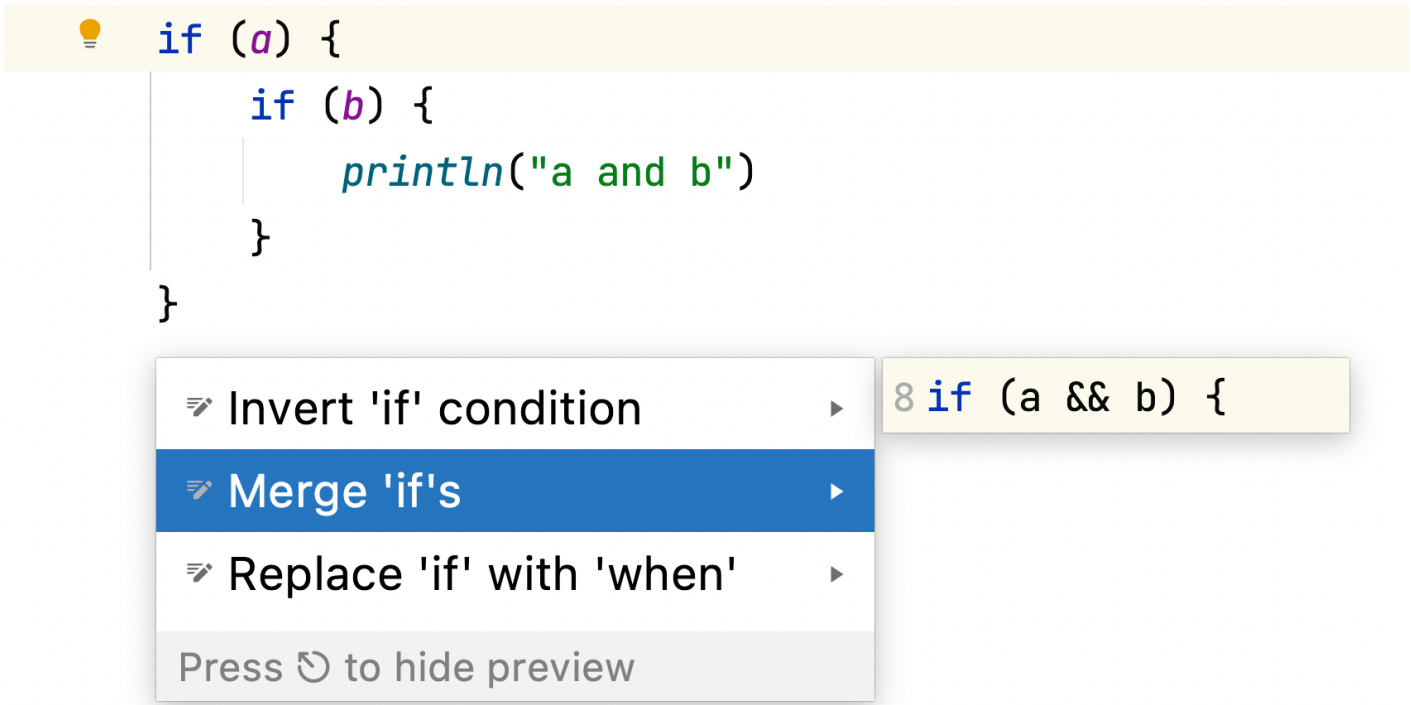
Вавилов Марк Владимирович
Ментор: Степанов Даниил Сергеевич

НИУ ВШЭ - Санкт-Петербург

18 июня 2021 г.

IntelliJ IDEA Intention Actions

Intention Actions — трансформации кода, предлагаемые IntelliJ IDEA



Как тестируются Kotlin Intentions

Для каждого intention-а есть набор файлов для тестов: программы, к которым применяются intention-ы, а также ожидаемые результаты. Тесты проверяют, что результат совпадает с ожидаемым.

addBracesForDoWhile.kt

```
1  fun <T> doSomething(a: T) {}
2
3  fun foo() {
4      <caret>do doSomething( a: "test")
5      while(true)
6  }
7
```

addBracesForDoWhile.kt.after

```
1  fun <T> doSomething(a: T) {}
2
3  fun foo() {
4      do {
5          doSomething("test")
6      } while(true)
7  }
8
```

Также проверяются случаи, когда intention нельзя применить:

```
1  // IS_APPLICABLE: false
2
3  fun <T> doSomething(a: T) {}
4
5  fun foo() {
6      <caret>if (true) {
7          doSomething( a: "test")
8      }
9  }
10
```

Фаззинг

Фаззинг — автоматическое тестирование на случайных данных.
Backend Bug Finder (BBF) – фаззер компилятора Kotlin, инструмент для поиска ситуаций, когда один и тот же код, скомпилированный под разные платформы, ведет себя по-разному.

Что делает BBF

Фаззинг компилятора начинается с конкретного файла и применяет к нему различные трансформации. После применения каждой трансформации новая программа проверяется на ошибки.

Производится трассировка, то есть в различные блоки добавляется вывод. Например, в блок catch (e: ClassCastException) добавляется println("CATCH e: ClassCastException"). Проверяется, что под разными платформами результат одинаковый.

Цель и задачи

Используя фаззер компилятора BBF, найти баги в intention-ах.

- выбрать intention-ы, для которых изменение поведения программы – ошибка
- делать проверку на компиляцию и одинаковый итог работы программ до и после применения intention-ов
- применять все возможные intention-ы во всех возможных местах программы
- запустить тесты, найти ошибки

Что делают мои тесты с каждым файлом

Если файл компилируется, то:

- производится трассировка
- во всех позициях в файле каждый тестируемый intention применяется и если результат еще не проверялся:
  - проверяется, что программа все еще компилируется
  - проверяется, что результат выполнения программы не изменился
- с вероятностью 0.5 трансформация применяется к исходной программе
- то же самое с первого шага

Итоги

Здесь появляются баги, найденные фаззером:
youtrack.jetbrains.com/issues?q=%23found-by-fuzzer%20ktij.
Сейчас там 6 багов, 1 из них уже исправлен

Репозиторий проекта

github.com/vavilovm/kotlinWithFuzzer