Верификация программ

.NET

Марк Шевченко

Программист

Московский клуб программистов

Wildberries

Ошибки

Как бороться с ошибками?

- Ревью кода, парное программирование
- Тесты
- Статические и динамические анализаторы
- Верификация

Проблемы Code Review

```
builder.RegisterType<Worker>();
```

Проблемы Unit Tests

```
bool IsOutOfInterval(double x, double start, double end)
{
  throw new NotImplementedException();
}
```

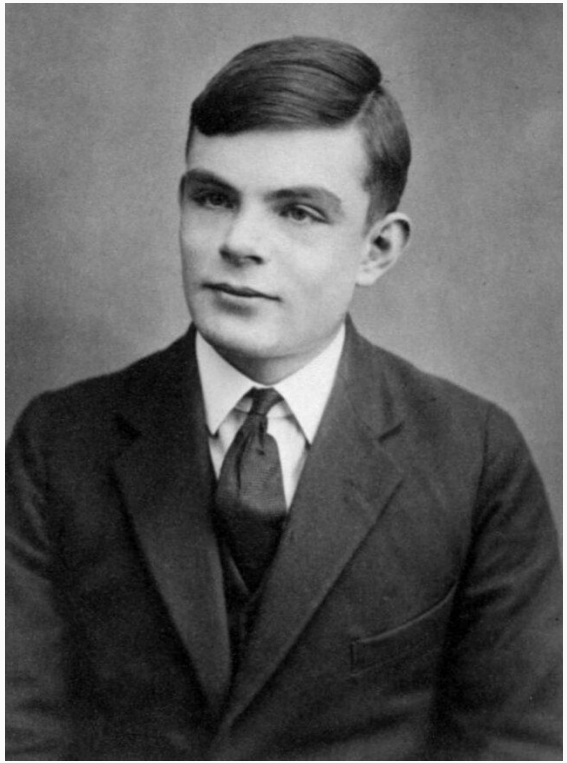
Проблемы Unit Tests

```
bool IsOutOfInterval(double x, double start, double end)
{
  throw new NotImplementedException();
}

Assert.True(IsOutOfInterval(-2, -1, 1));
Assert.True(IsOutOfInterval(-1, -1, 1));
Assert.False(IsOutOfInterval(-0.5, -1, 1));
```

Проблемы Unit Tests

```
bool IsOutOfInterval(double x, double start, double end)
{
  return x <= start || x >= end;
}

Assert.True(IsOutOfInterval(-2, -1, 1));
Assert.True(IsOutOfInterval(-1, -1, 1));
Assert.False(IsOutOfInterval(-0.5, -1, 1));
```

Проблемы верификации



$$\neg(p \wedge q) \equiv \neg p \vee \neg q$$

$$\neg(p \wedge q) \equiv \neg p \vee \neg q$$

p	q	$\neg(p \wedge q)$	$\neg p \vee \neg q$	$\neg(p \wedge q) \equiv \neg p \vee \neg q$
0	0	1	1	1
0	1	0	0	1
1	0	0	0	1
1	1	0	0	1

Proof Assistants

~~Coq~~ Rocq

- Интерактивные доказательства
- Автоматизация, где возможно
- Библиотеки готовых теорем
- Поиск подходящих теорем


Португалия
Греция
Турция
Туркмен
Сирия
Ирак
Иран
Тунис
Марокко
Алжир
Ливия
Египет
Западная Сахара
Саудовская Аравия
Оман
Мавритания
Мали
Нигер
Чад
Судан
Йемен
Буркина-Фасо
Нигерия
Гана
Эфиопия
Сомали
Кения
Габон
ДР Конго
Танзания
Ангола
Замбия
Мозамбик
Намибия
Зимбабве
Ботсвана
Мадагаскар
Южная Африка

Задача

Задача

30000

Задача

30000

Январь	2500
Февраль	2500
Март	2500
Апрель	2500
Май	2500
Июнь	2500
Июль	2500
Август	2500
Сентябрь	2500
Октябрь	2500
Ноябрь	2500
Декабрь	2500

Задача

40000

Январь	?
Февраль	?
Март	?
Апрель	?
Май	?
Июнь	?
Июль	?
Август	?
Сентябрь	?
Октябрь	?
Ноябрь	?
Декабрь	?

Задача

40000

Январь	
Февраль	
Март	
Апрель	
Май	
Июнь	?
Июль	?
Август	?
Сентябрь	?
Октябрь	?
Ноябрь	?
Декабрь	?

Формулы

```
monthsInYear = 12
month = 6 // июнь
```

Формулы

```
monthsInYear = 12
month = 6
count = monthsInYear - month + 1 // 7 месяцев до декабря
```

Формулы

```
monthsInYear = 12
month = 6
count = monthsInYear - month + 1
yearAmount = 40000
partialAmount = count * yearAmount / monthsInYear
```

23333

Формулы

```
monthsInYear = 12
month = 6
count = monthsInYear - month + 1
yearAmount = 40000
partialAmount = count * yearAmount / monthsInYear
monthAmount = partialAmount / count
```

Формулы

```
monthsInYear = 12
month = 6
count = monthsInYear - month + 1
yearAmount = 40000
partialAmount = count * yearAmount / monthsInYear
monthAmount = partialAmount / count
decemberAmount = monthAmount + partialAmount % count
```

Проверка

```
partialAmount
  = (count - 1) * monthAmount
  + decemberAmount
```

23333

3333

6

3335

Пример

Что мы сделали?

- Написали критичную бизнес-логику на Coq
- Доказали правильность реализации
- Транслировали код на OCaml/F#
- Написали обвязку для вызова из C#
- Использовали проверенный код в кровавом энтерпрайзе

Ссылки

- Антон Стеканов, Евгений Каратаев. Введение в Coq
- ROCQ
- Software Foundations
- COQ theorem prover online IDE
- Towards formal verification of TLS network packet processing written in C
- Verified Software Toolchain
- A computer-checked proof of the Four Colour Theorem
- Исходный код

Где применять

- Код, который дорого исправлять
- Код, ошибки в котором дорого стоят

Содержание

- Код-ревью и проблемы
- Тестирование и проблемы
- Тьюринг, Чёрч, проблема разрешения
- Законы Моргана, перебор
- Proof Assistant
- ~~Coq~~ Rocq
- Проблема четырёх красок
- Бизнес-задача
- Coq IDE
- Рекурсивные функции
- Арифметика Пеано
- Тактика reflexivity
- Тактика ring
- Поиск подходящих теорем
- Извлечение
- OCaml == F#
- Обвязка для вызова из C#
- Используем в кровавом энтерпрайзе