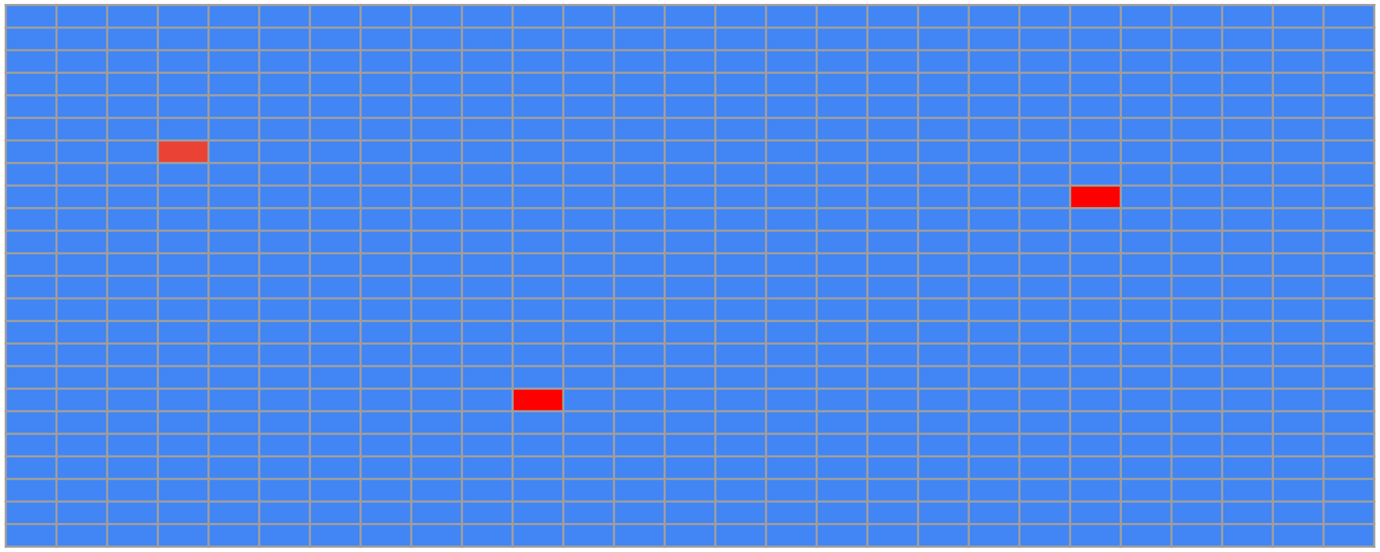
Towards making formal methods normal: Meeting developers where they are

Alastair Reid, Shaked Flur, Luke Church, Sarah de Haas, Maritza Johnson, Ben Laurie

Google Research

HATRA 2020, 18–19 November 2020. https://arxiv.org/abs/2010.16345

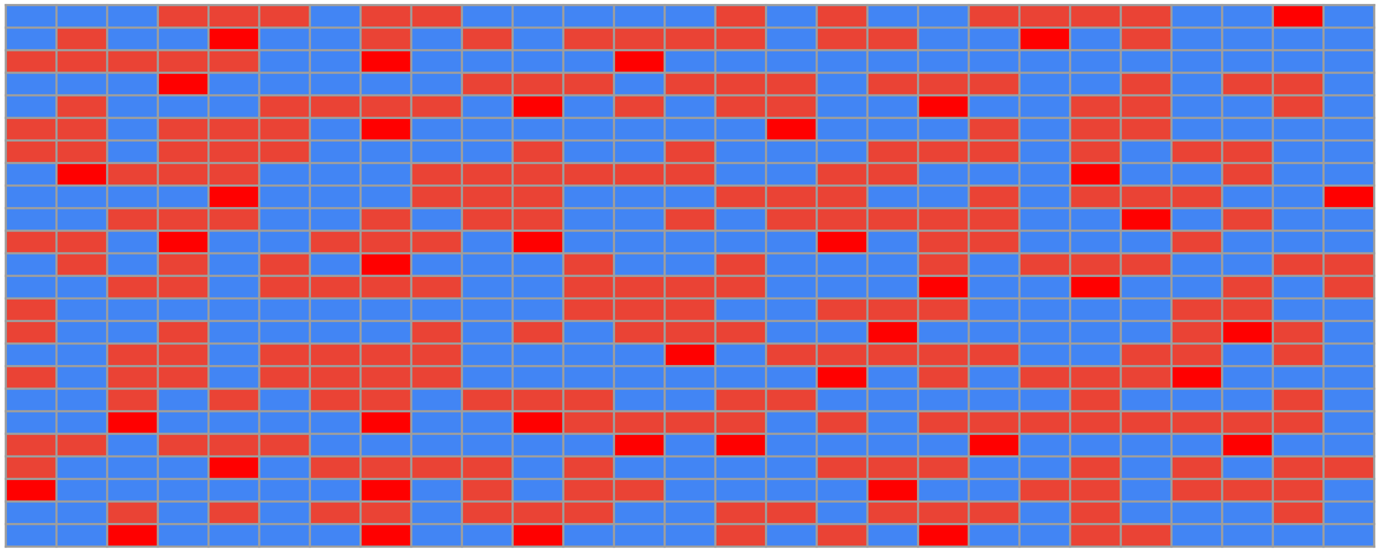
How many developers use formal methods?


Artists impression

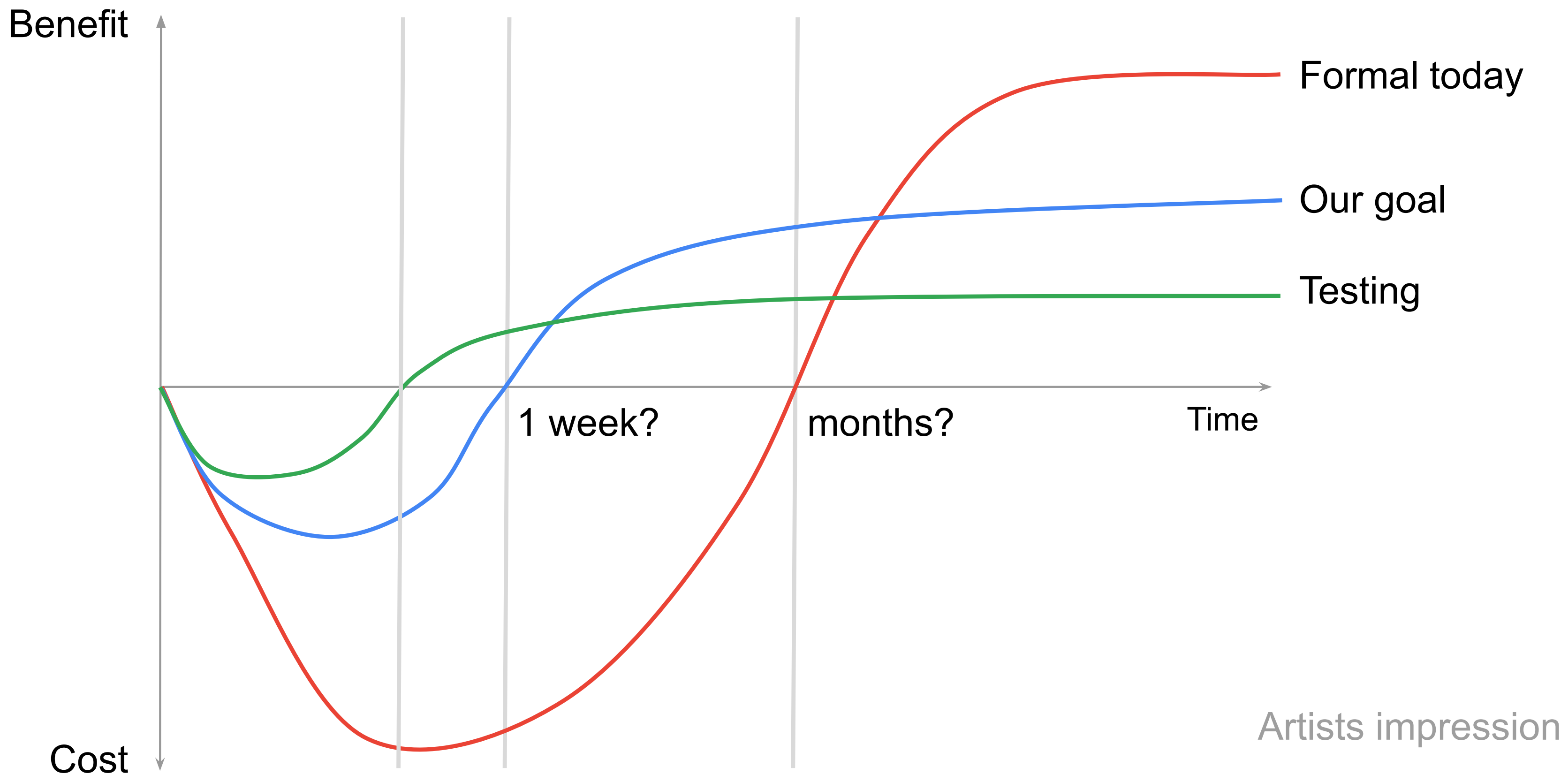
Google Research

could productively

How many developers ^ use formal methods?



Artists impression



Artists impression

Google Research

Meet developers where they are

What do developers do?

- Design
- Coding
- Testing
- Fuzzing
- Static analysis
- Code review
- ...

Google Research

Meet developers where they are

What do developers do?

- Design
- Coding
- **Testing**
- **Fuzzing**
- Static analysis
- Code review
- ...

Property-based fuzz-testing harness

```
proptest! {
    #[test]
    fn multiply(a in 1..=1000u32, b in 1..=1000u32) {
        let r = a*b;
        assert!(1 <= r && r <= 1000000);
    }
}
```

(Overly simple example)

$\forall\, a \in [1..1{,}000], b \in [1..1{,}000].$
$(a \ *_{u32}\ b) \in [1..$
$1{,}000{,}000]$

proptest link

Formal verification harness

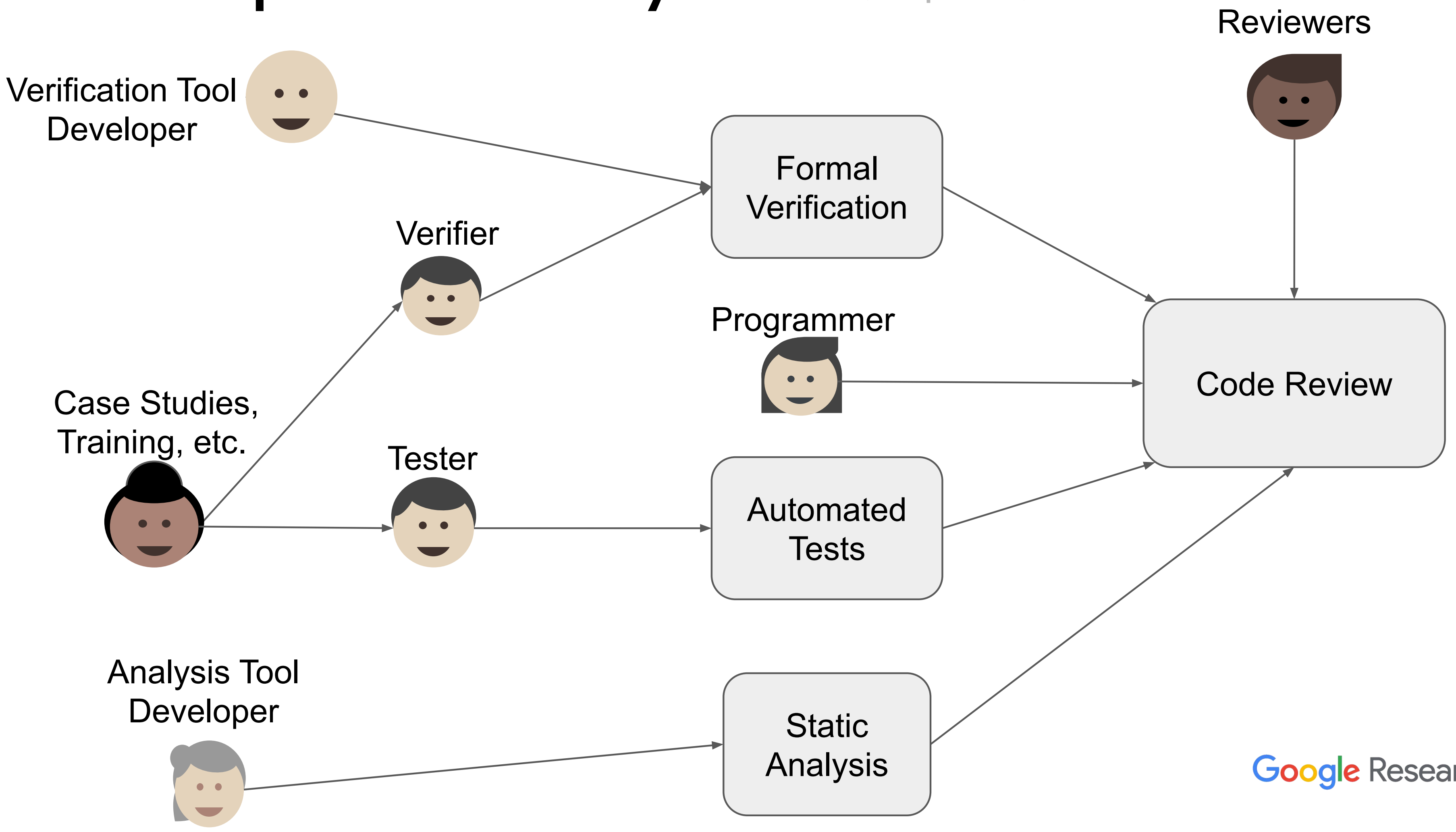
```
proptest! {
    #[test]
    fn multiply(a in 1..=1000u32, b in 1..=1000u32) {
        let r = a*b;
        assert!(1 <= r && r <= 1000000);
    }
}
```

(Same overly simple example)

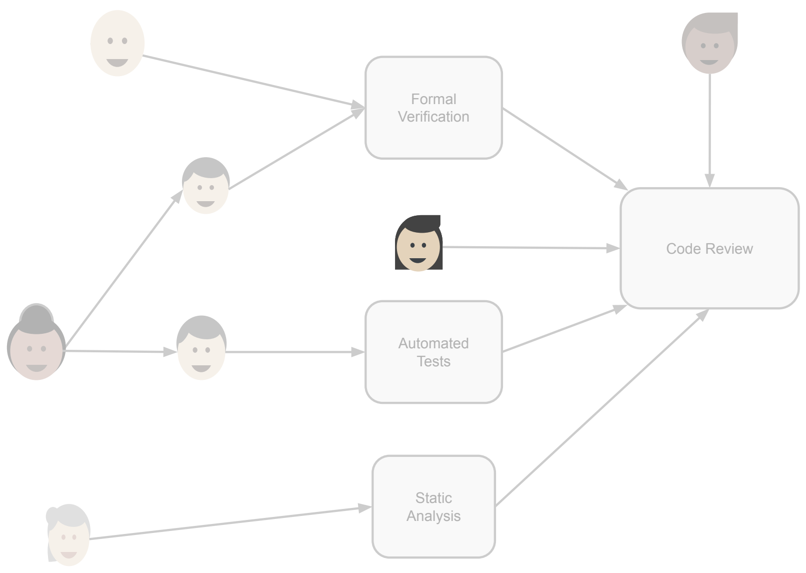
Released Sept 2020: https://github.com/project-oak/rust-verification-tools

Google Research

Development ecosystem (simplified)



Google Research



Onboarding issues

Overcome preconceptions

Tool configuration complexity

Integration into build system

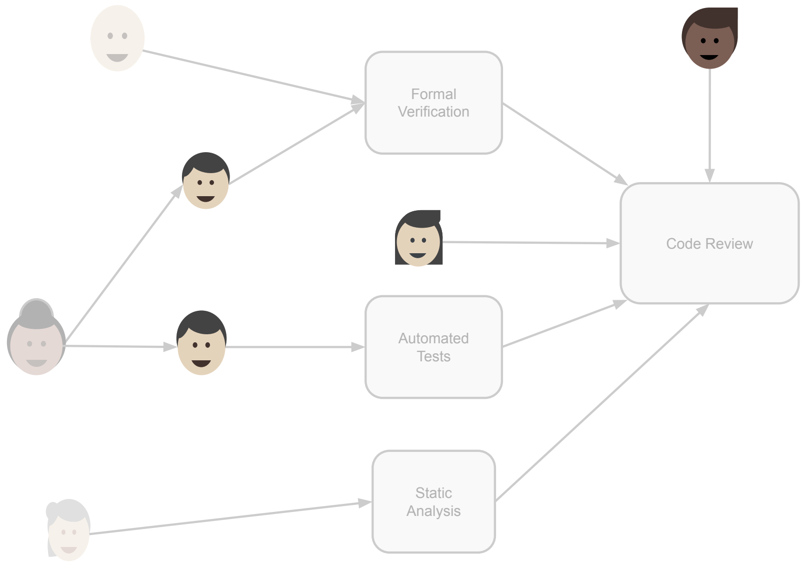
Recurring issues

Weekly cost-benefit ratio

Bug localization

...

Google Research



Surfacing results

Continuous Integration tools?

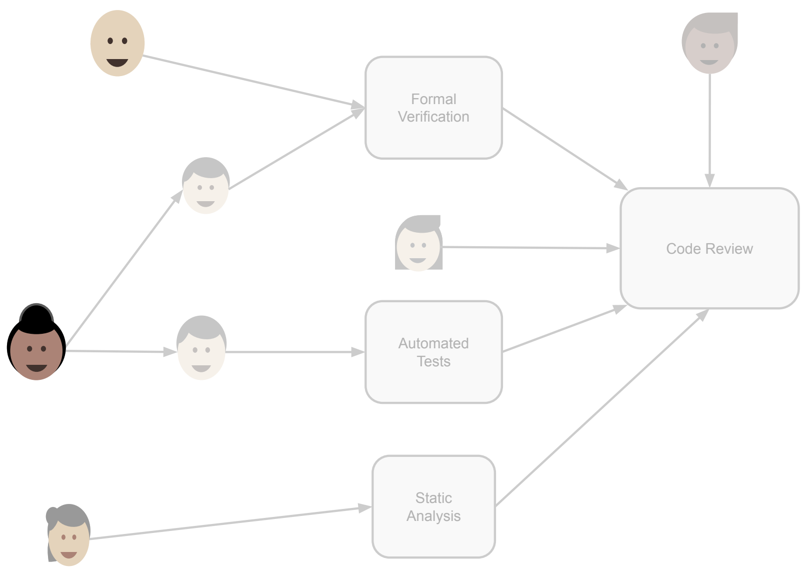
Code Review?

Team organization

Tracking results

Standardizing tool configurations

Google Research



Planning

What kind of verifier?
When to use? What tools?
vs. {test, static analysis,
code review, ...}
⟶
case studies, metrics, ...

Google Research

Technical challenges

Tool specialization

- Allows better usability
- Enables optimization for purpose
- Tension: local optimization vs. global optimization

Decidability ceiling

- Tension: Predictability vs. power
- How to improve consistency?
- Profiling to find verification hotspots?

Google Research

More detail in paper

Meeting the developer where they are

Build on what developers are already doing: testing

- (our work is at an early stage)

Focus: payback within a week (stretch goal!!!)

Ecological challenges

Technical challenges

Google Research

Thank you

Alastair Reid (@alastair_d_reid)
Staff Research Scientist

Google Research