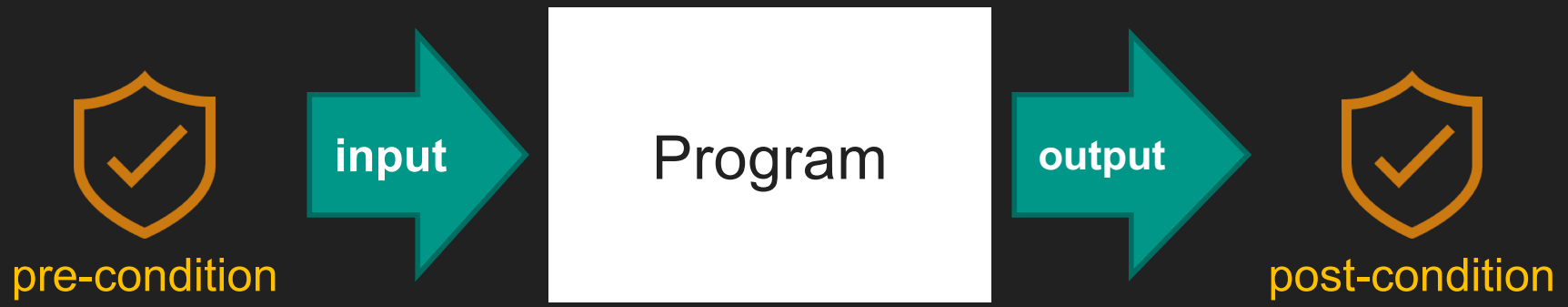
FormalZ : Playful Formal Method

Wishnu Prasetya, Craig Leek, Orestis Melkonian, Jorris ten Tusscher
Universiteit Utrecht

IMPRESS Project
https://impress-project.eu/

ERASMUS+
Project 2017-1-NL01-KA203-035259

Why is it difficult to write bug-free software?



Unfortunately in practice people do not make these “guards” explicit enough.

Benefit of formal specifications

- One source of truth
- General, as opposed to concrete value test oracles
- Facilitate automated testing
- No, it does not require separate tooling --with λ-expression we can write specifications in-code.

- But yes... it does require some learning to appreciate it and become proficient with it.

Example of in-code specifications

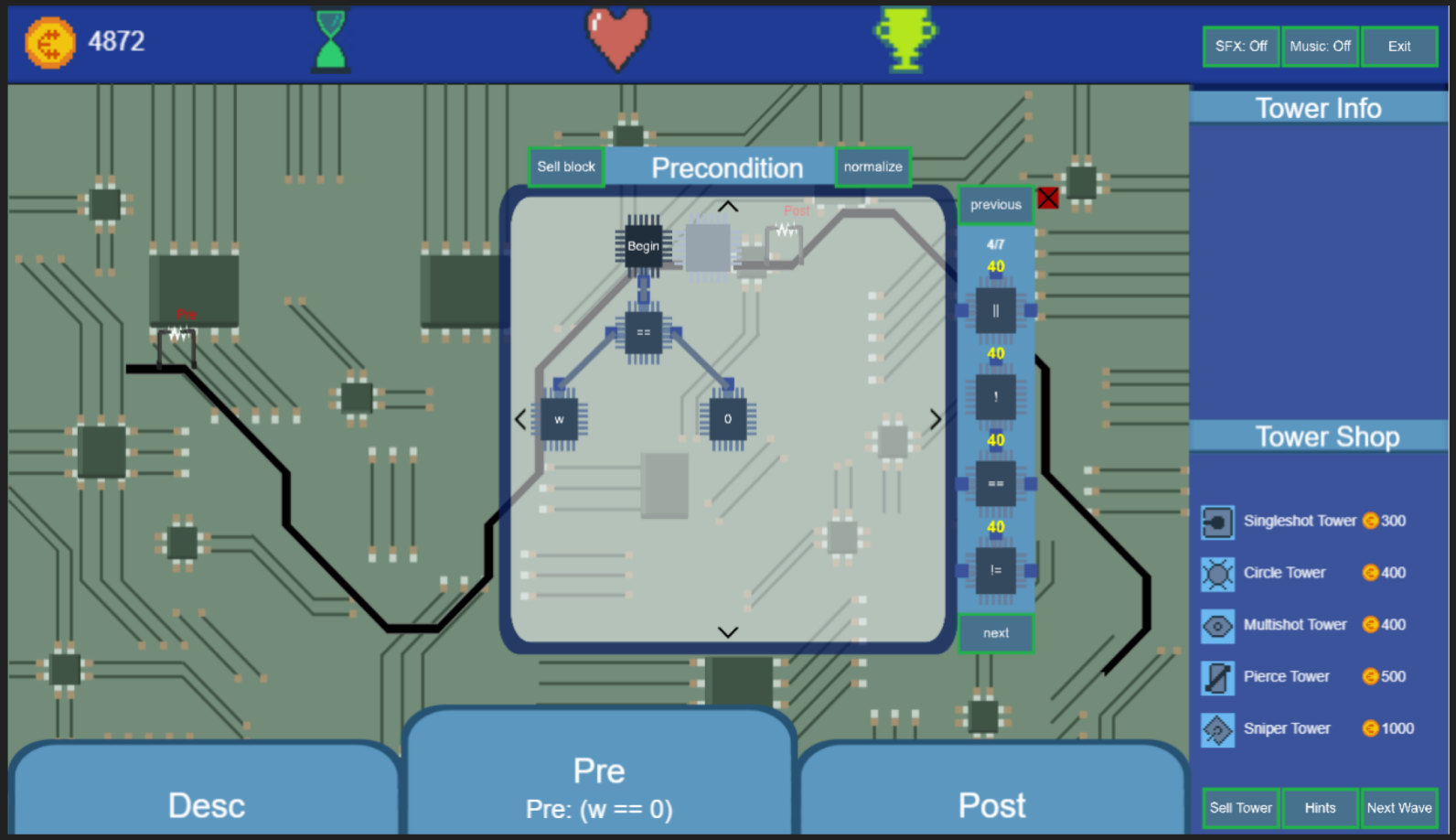
```
public static void getMax_spec1(int[] a) {
    // preconditions
    pre(a != null);
    pre(a.length > 0);

    // call the actual function implementation
    int retval = getMax(a);

    // postconditions
    post(exists(a, i -> a[i] == retval)); // A
    post(forall(a, i -> a[i] <= retval)); // B
}
```

A lesson in writing formal specifications

- A **formula** is either:
  - a simple formula
  - ∀identifier∈simple-expression● formula
  - ∃identifier∈simple-expression● formula
- For example:
  - ∀x∈Students● x.age ≥ 16
  - ∃x∈Students● x.age = 16

A lesson in writing formal specifications

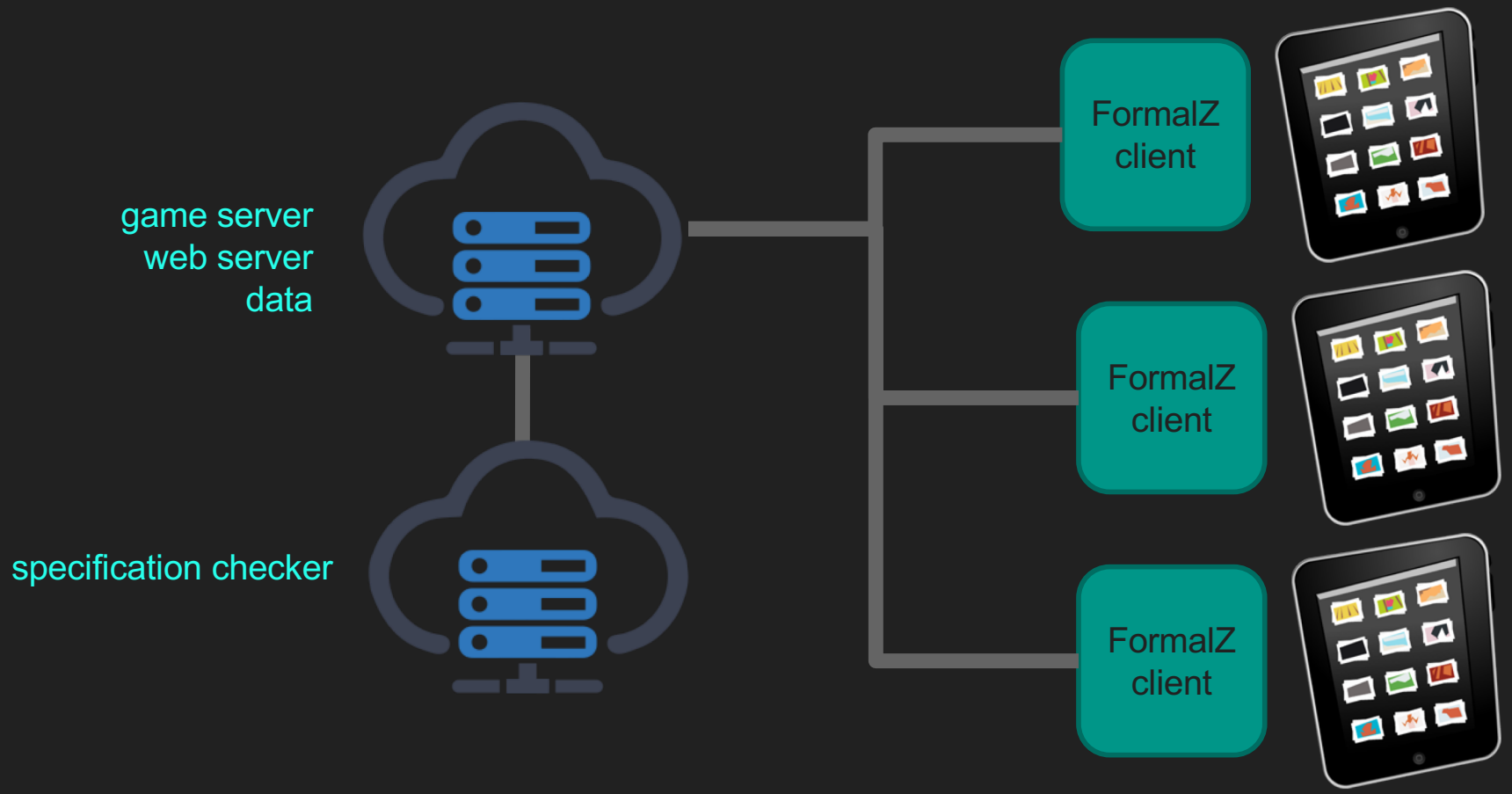
FormalZ : playfully formal



The game concept

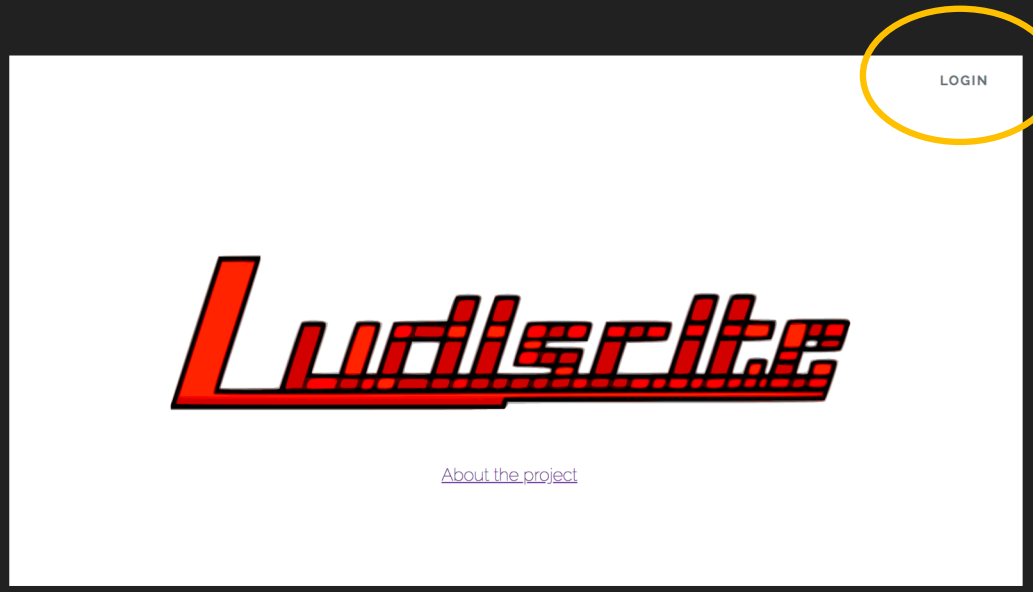
- It is an “educative game”, but not a trainer software.
- A cross-genre game of tower-defense and construction game
  - along the way, you also learn to formalize requirements.
- Deploy it in your course as a means to improve the students engagement.

FormalZ Architecture



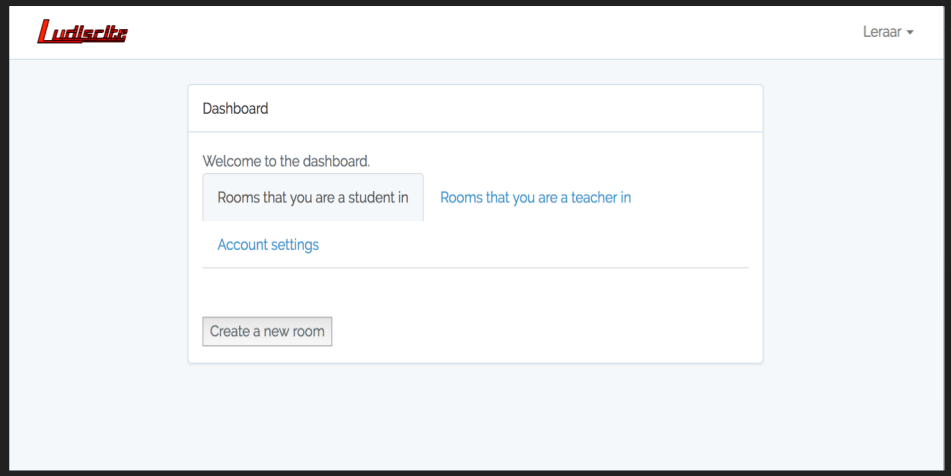
Tutorial FormalZ

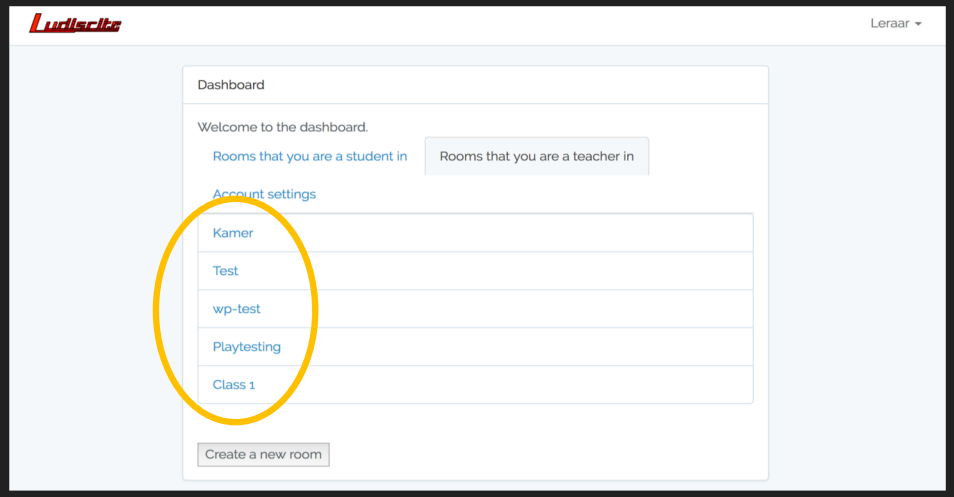
https://science-vs160.science.uu.nl/



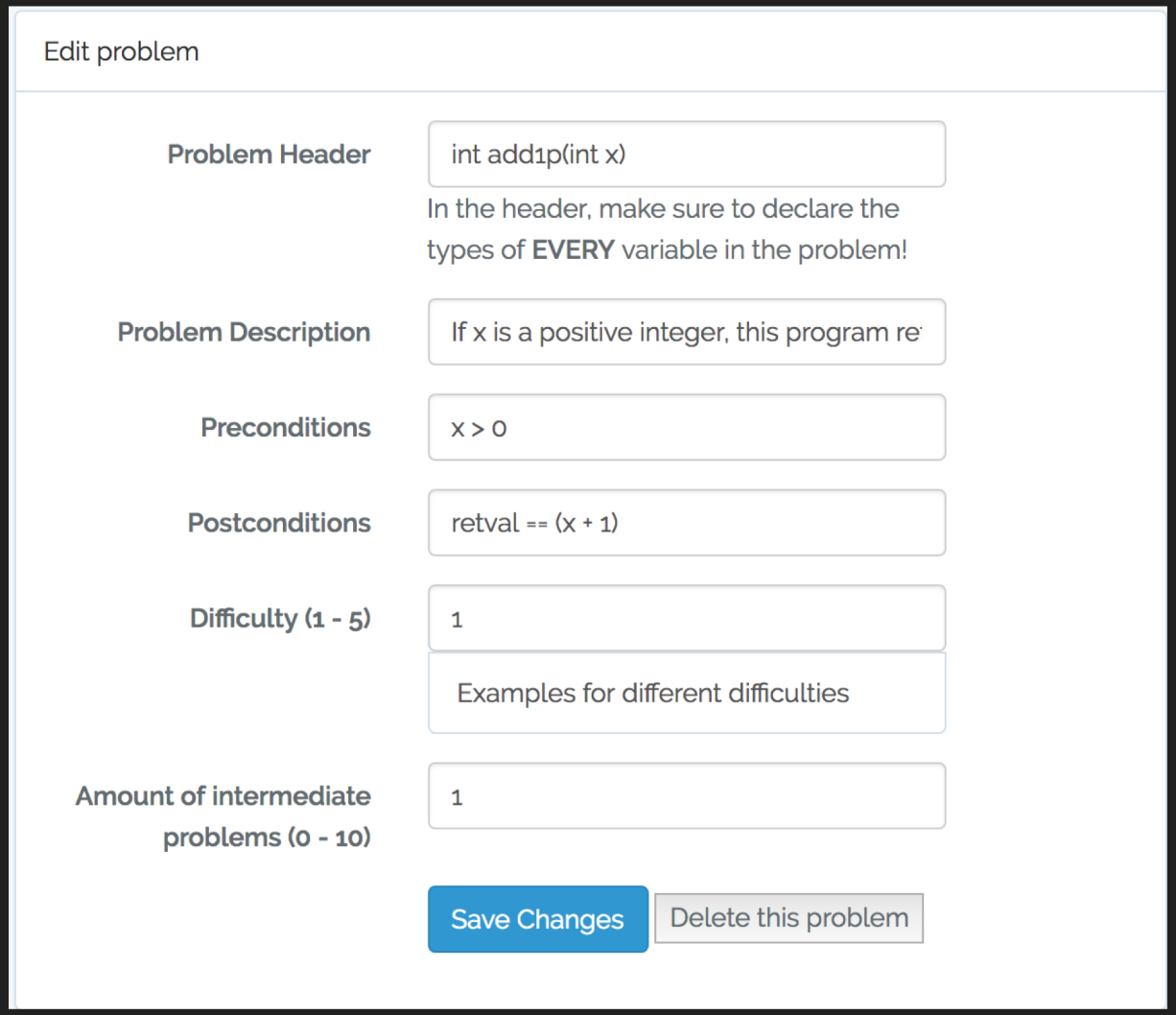
uname: funteacher
pwd: forall(h,a->h[a]<3)

Classroom management





Defining a “problem”



Few examples

- **int add1p(int x)**

  If x is a positive integer, this program returns x+1. Use "retval" to denote the return value.

  pre: x > 0

  post: retval == (x + 1)

Few examples

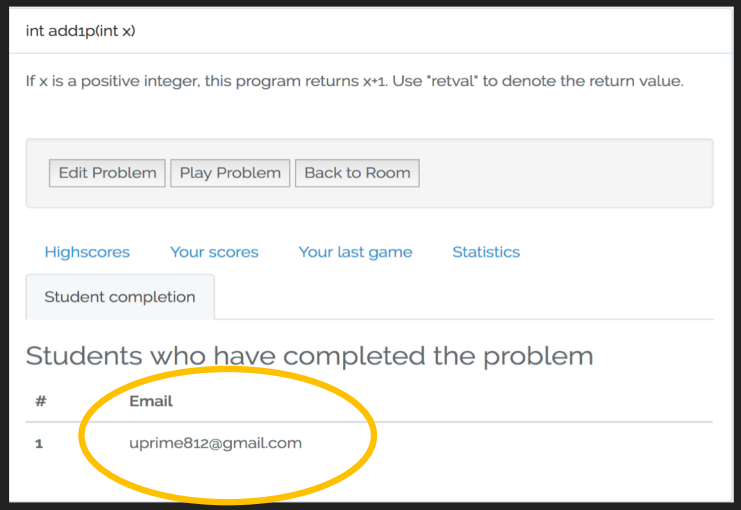
- **boolean allzero(int[] a, int i, boolean retval)**

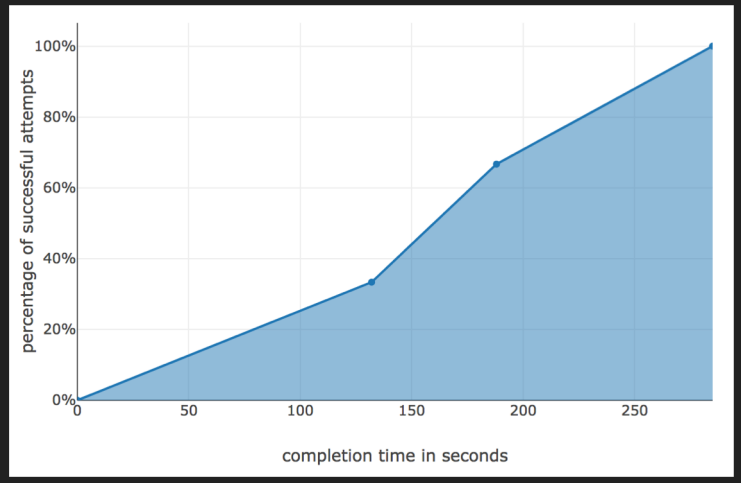
  Given a non-null array a, the program allzero checks if a consists of only 0's. The return value (represented by retval) will indicate this.

  pre: a != null

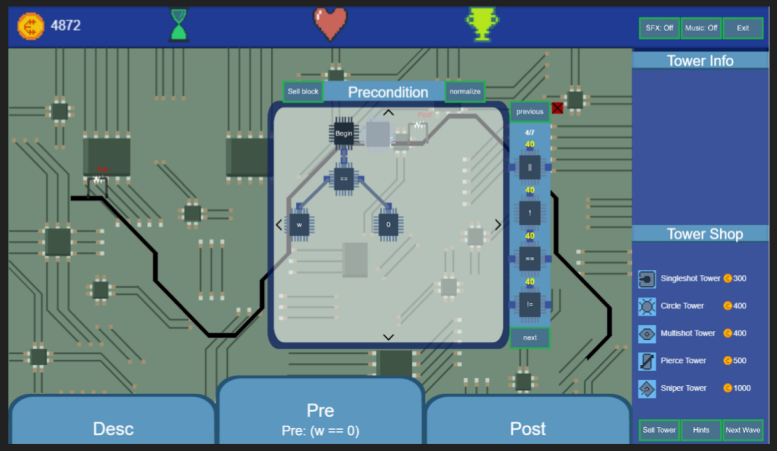
  post: retval == **forall**(a, i -> a[i] == 0)

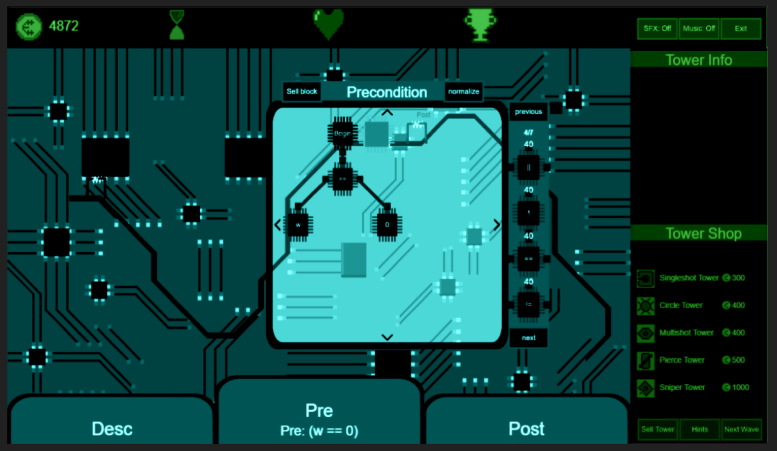
Classroom progress





Formalz future work





- Graphics.
- Analytics.
- Strengthening the gamification elements.
- Studying these innovations in actual class rooms.
- Public release.