

Program Correctness and its Limitations

David Sankel

Program Correctness and its Limitations

David Sankel | Principal Scientist

Software Technology Lab

Adobe

Image by Paula Garcia for Adobe Creative Residency



I don't know what program correctness is...

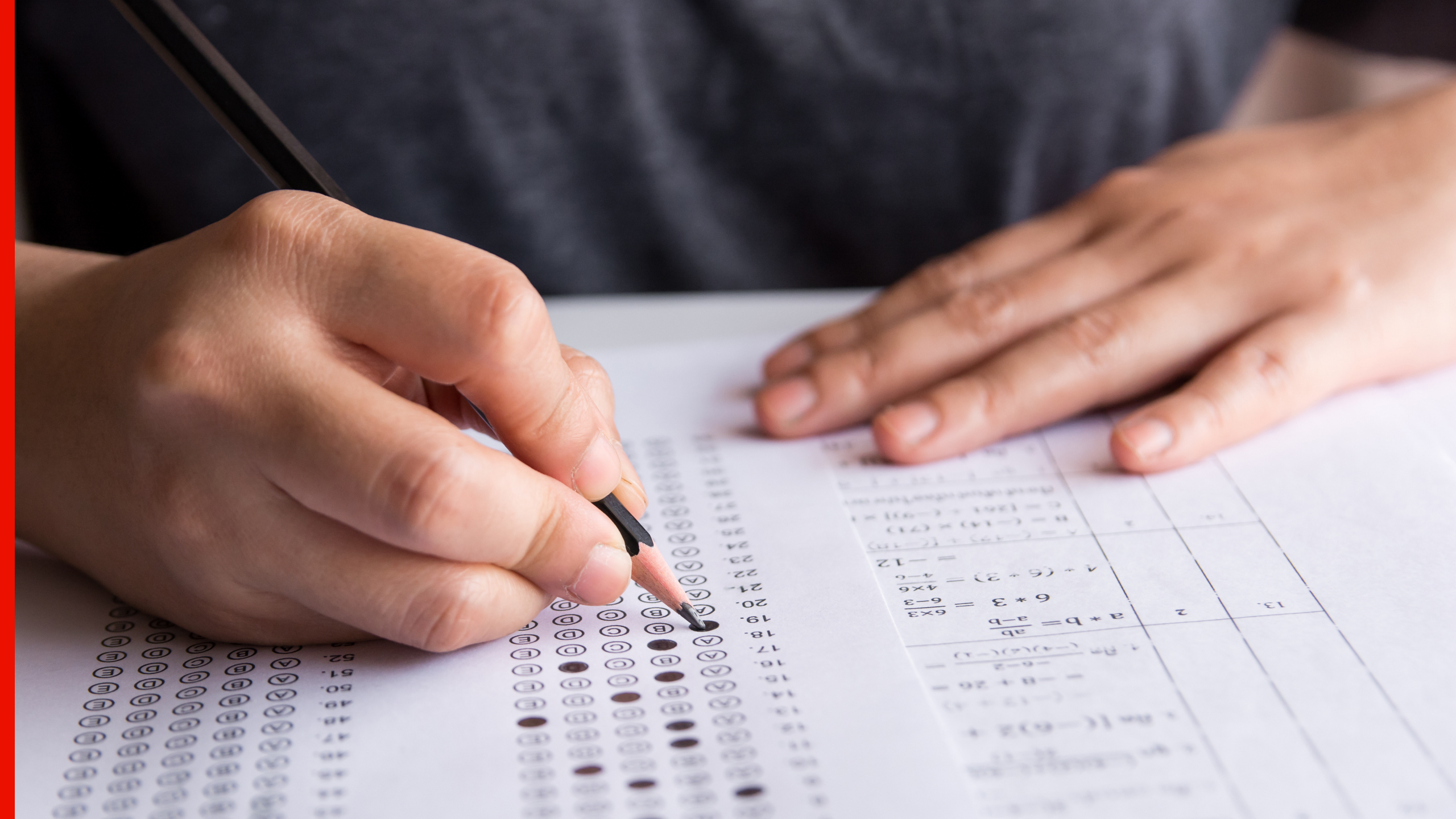
- We often speak of correctness in the context of programming, but I don't think we know what we're talking about
- I often see assumptions related to code correctness that don't hold up in practice
- I want a more rigorous foundation for correctness
- I want a better understanding of its limitations

This is supposed to be an interactive journey, please engage. I need your help

**Some people don't like this
kind of talk...**

G.F.Y.

What does correct mean?



Exam correctness

- Each response is said to either be “correct” or “incorrect”
- Correctness does not apply to the entirety of the filled out exam
- An assessment is made based on the proportion of correct responses.
(sometimes weighted)

(Print)

City State Zip Code

PHONE NO. : _____
(Print)

IMPORTANT: Please fill in these boxes exactly as shown on the back cover of your test book.

2. TEST FORM

3. TEST CODE

4. REGISTRATION NUMBER

6. DATE OF BIRTH

Month	Day	Year
☐ JAN		
☐ FEB		
☐ MAR	☐ 0	☐ 0
☐ APR	☐ 1	☐ 1
☐ MAY	☐ 2	☐ 2
☐ JUN	☐ 3	☐ 3
☐ JUL	☐ 4	☐ 4
☐ AUG	☐ 5	☐ 5
☐ SEP	☐ 6	☐ 6
☐ OCT	☐ 7	☐ 7
☐ NOV	☐ 8	☐ 8
☐ DEC	☐ 9	☐ 9

7. SEX

☐ MALE

☐ FEMALE

The Princeton Review

© TPR Education IP Holdings, LLC
FORM NO. 00001-PR

Section I Start with number 1 for each new section.
If a section has fewer questions than answer spaces, leave the extra answer spaces blank.

1. ☐ A ☒ B ☐ C ☐ D ☐ E

2. ☐ A ☐ B ☒ C ☐ D ☐ E

3. ☐ A ☐ B ☐ C ☒ D ☐ E

4. ☐ A ☐ B ☐ C ☒ D ☐ E

5. ☐ A ☐ B ☐ C ☐ D ☒ E

6. ☒ A ☐ B ☐ C ☐ D ☐ E

7. ☐ A ☐ B ☐ C ☐ D ☒ E

8. ☐ A ☐ B ☐ C ☒ D ☐ E

9. ☐ A ☐ B ☐ C ☐ D ☒ E

10. ☐ A ☒ B ☐ C ☐ D ☐ E

11. ☐ A ☐ B ☒ C ☐ D ☐ E

12. ☐ A ☐ B ☐ C ☒ D ☐ E

13. ☐ A ☐ B ☐ C ☒ D ☐ E

14. ☐ A ☐ B ☒ C ☐ D ☐ E

15. ☐ A ☐ B ☐ C ☐ D ☒ E

16. ☒ A ☐ B ☐ C ☐ D ☐ E

17. ☐ A ☐ B ☐ C ☐ D ☒ E

18. ☐ A ☐ B ☐ C ☒ D ☐ E

19. ☐ A ☒ B ☐ C ☐ D ☐ E

20. ☐ A ☒ B ☐ C ☐ D ☐ E

21. ☐ A ☐ B ☐ C ☒ D ☐ E

22. ☐ A ☐ B ☐ C ☐ D ☒ E

23. ☐ A ☒ B ☐ C ☐ D ☐ E

24. ☐ A ☐ B ☐ C ☒ D ☐ E

25. ☒ A ☐ B ☐ C ☐ D ☐ E

26. ☐ A ☐ B ☒ C ☐ D ☐ E

27. ☐ A ☐ B ☐ C ☐ D ☒ E

28. ☒ A ☐ B ☐ C ☐ D ☐ E

29. ☐ A ☐ B ☐ C ☐ D ☒ E

30. ☐ A ☐ B ☐ C ☒ D ☐ E

31. ☒ A ☐ B ☐ C ☐ D ☐ E

32. ☐ A ☒ B ☐ C ☐ D ☐ E

33. ☐ A ☐ B ☐ C ☐ D ☒ E

34. ☐ A ☐ B ☐ C ☐ D ☒ E

35. ☐ A ☐ B ☒ C ☐ D ☐ E

36. ☐ A ☒ B ☐ C ☐ D ☐ E

37. ☐ A ☐ B ☐ C ☐ D ☒ E

38. ☐ A ☐ B ☒ C ☐ D ☐ E

39. ☐ A ☐ B ☒ C ☐ D ☐ E

40. ☐ A ☐ B ☐ C ☒ D ☐ E

41. ☐ A ☐ B ☐ C ☐ D ☒ E

42. ☐ A ☐ B ☒ C ☐ D ☐ E

43. ☐ A ☐ B ☐ C ☐ D ☒ E

44. ☐ A ☐ B ☒ C ☐ D ☐ E

45. ☐ A ☐ B ☐ C ☐ D ☒ E

33/45

**What makes one answer
correct and the others
incorrect?**





16. (a) I wouldn't mind the *drudgery* of the work if they paid higher wages. (b) Would you clear away all this *drudgery* so that I'll have some room in which to work? (c) He agreed that the housework was pure *drudgery*. (d) He escaped the *drudgery* of his father's farm by running away.

How is correctness determined?

It isn't determined by "the answer key".

There's got to be something more to it

What?

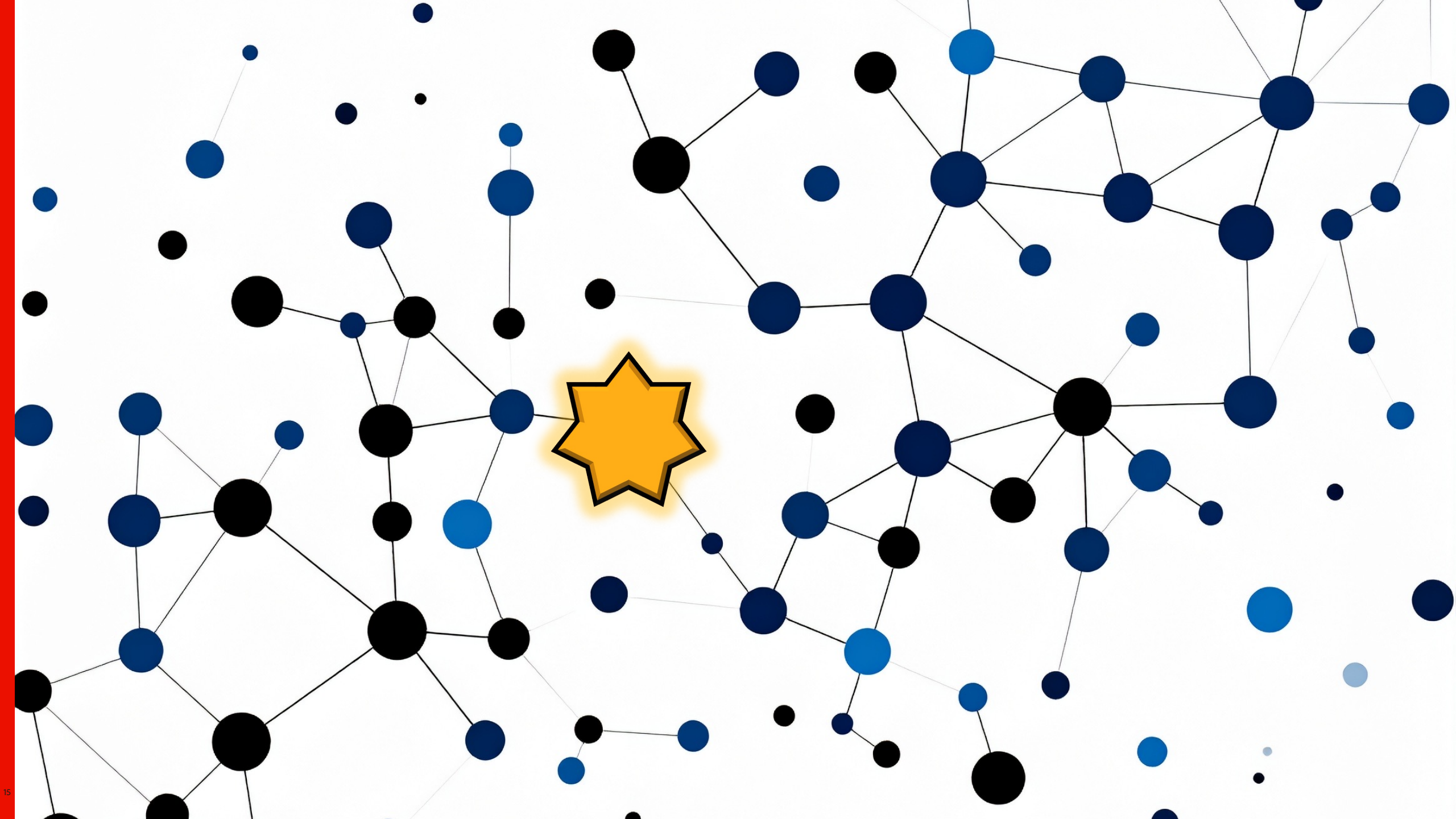


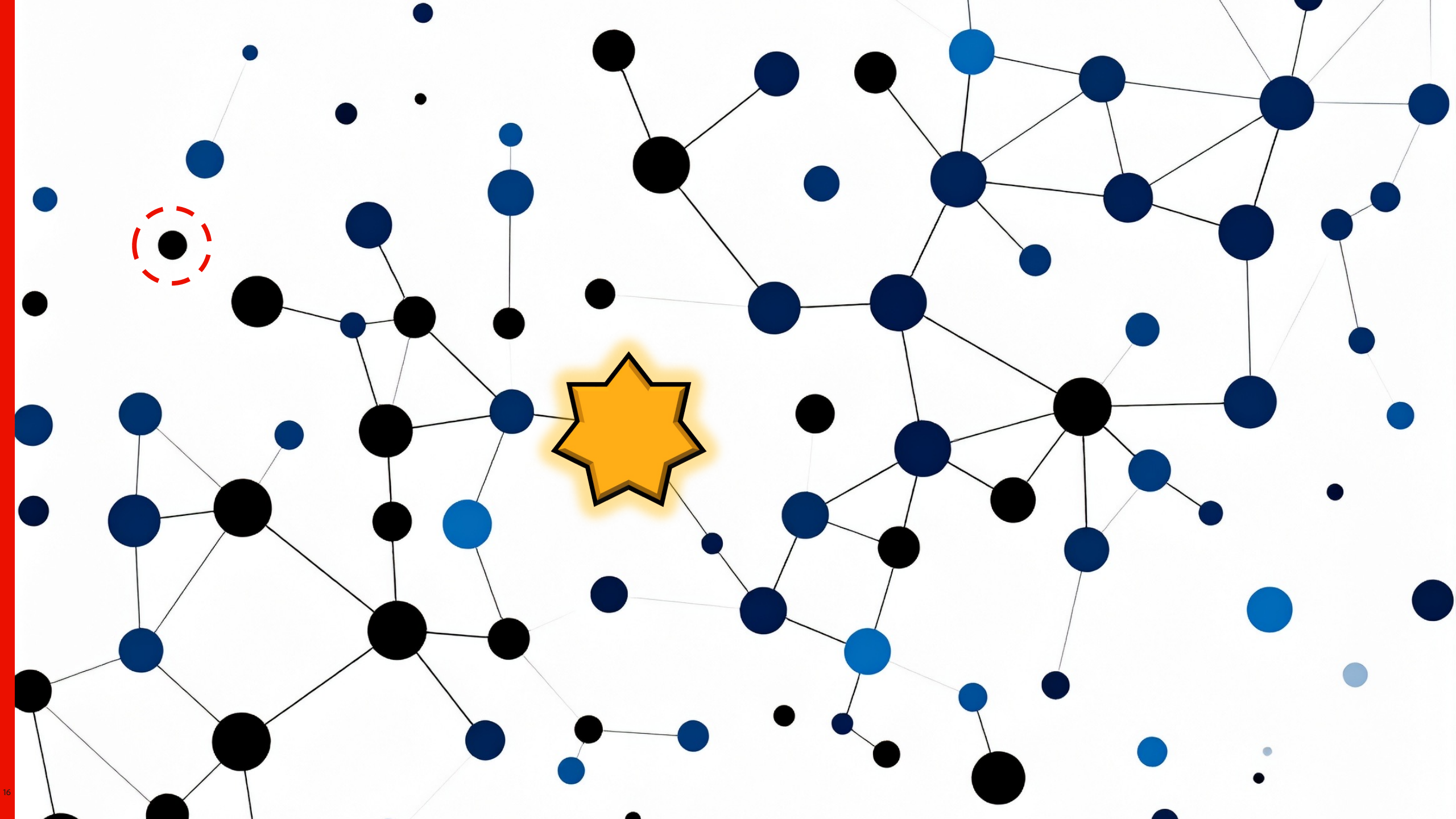
Correctness

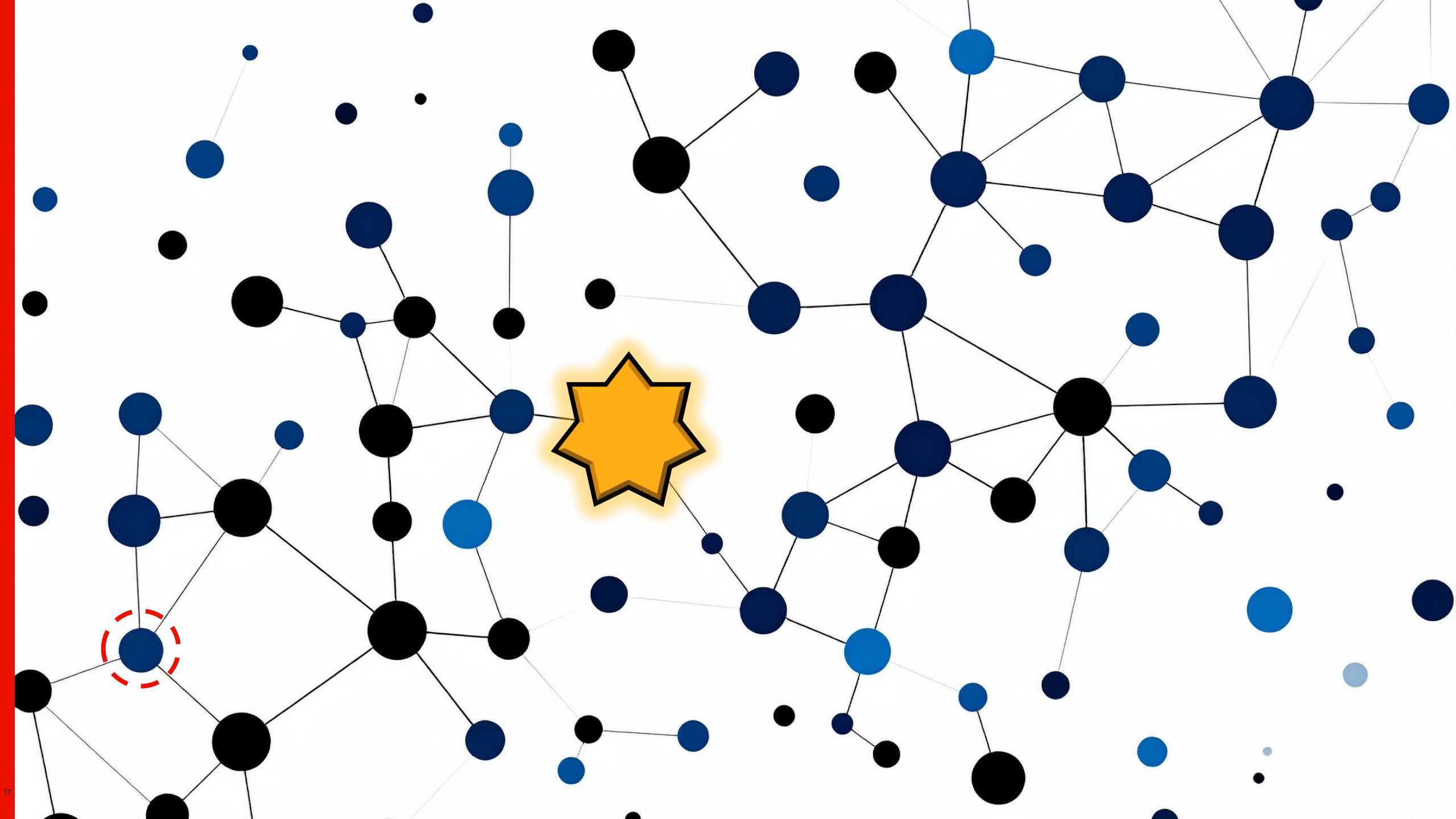
For correctness to be well-defined, it seems like

1. There needs to be an agreed-upon “basis of truth”.
 1. Usually self-evident, but sometimes hypothetical
2. There’s usually some way to take claims beyond the basis of truth and demonstrate that the truth supports those claims or contradicts them.

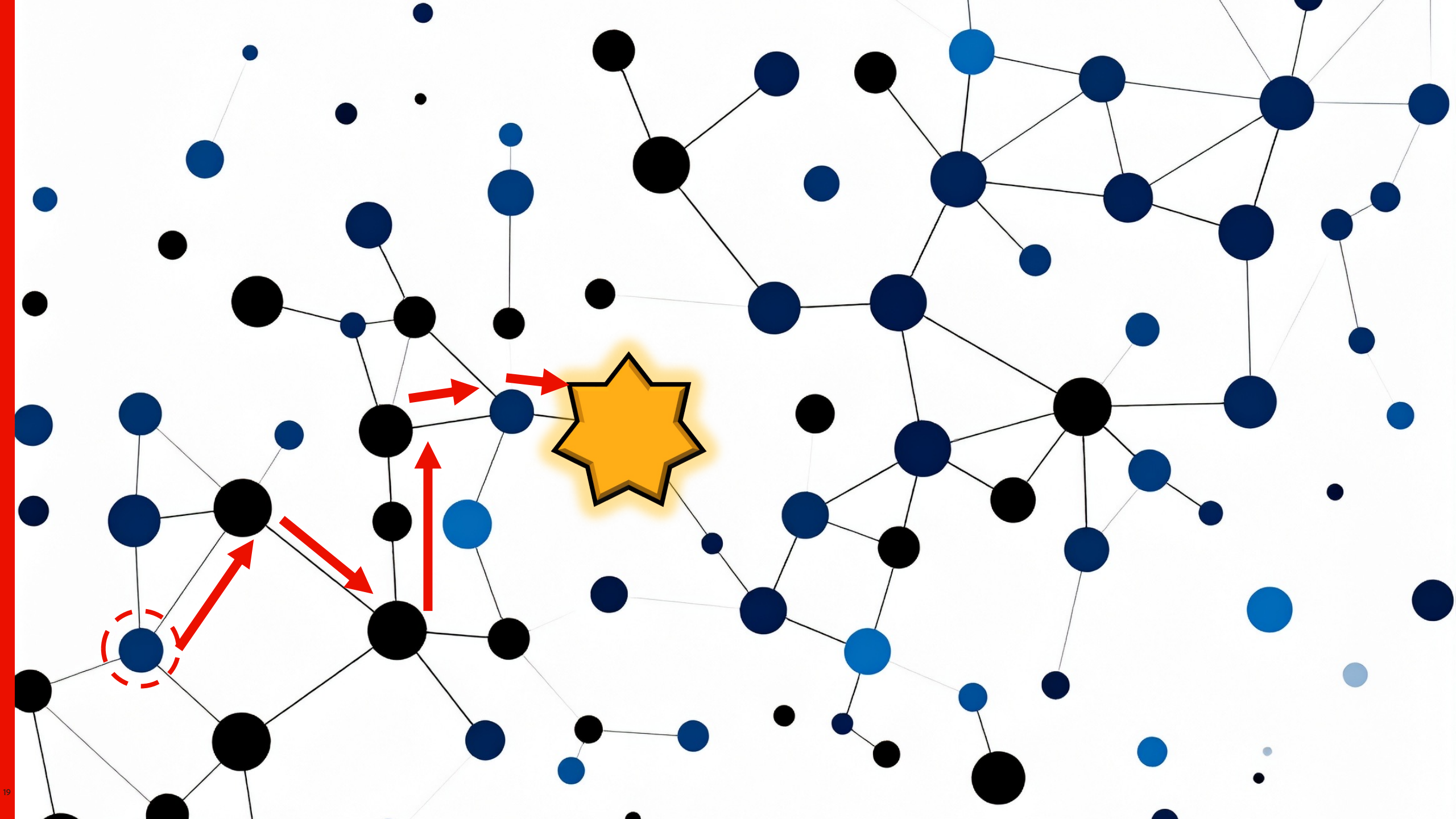












What is truth?

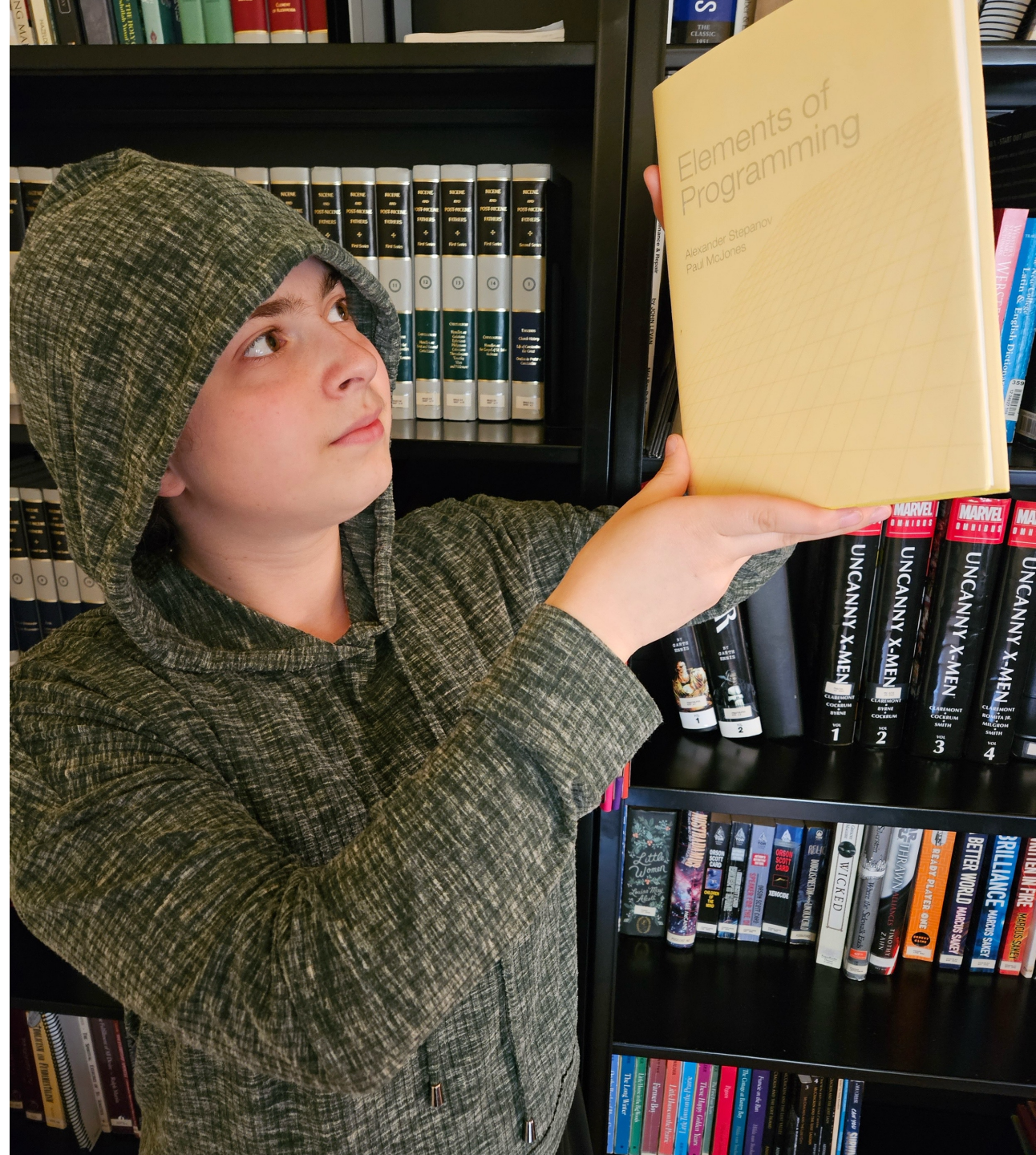
Use an inspired person

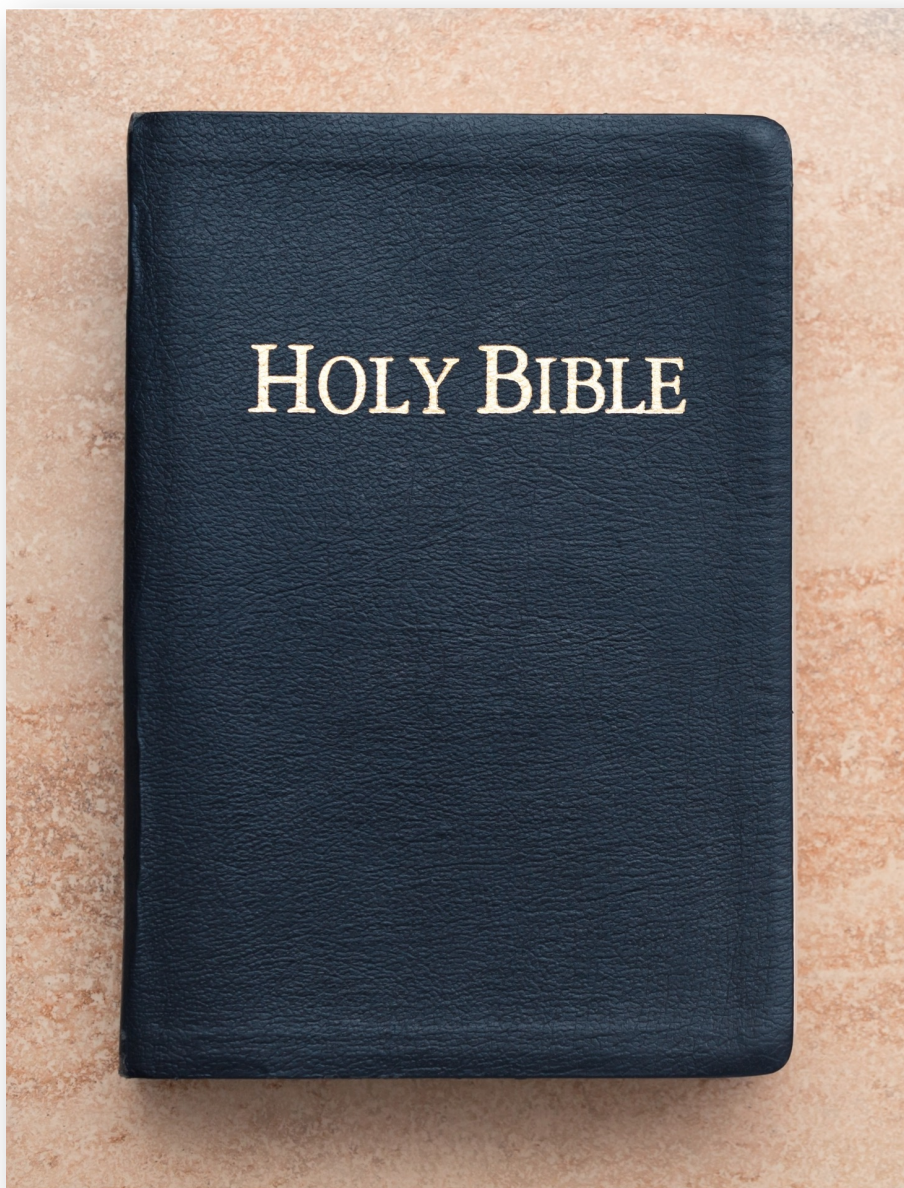
- “basis of truth” defined by a particular person’s authority
- Requires very low mental energy



Use an inspired book

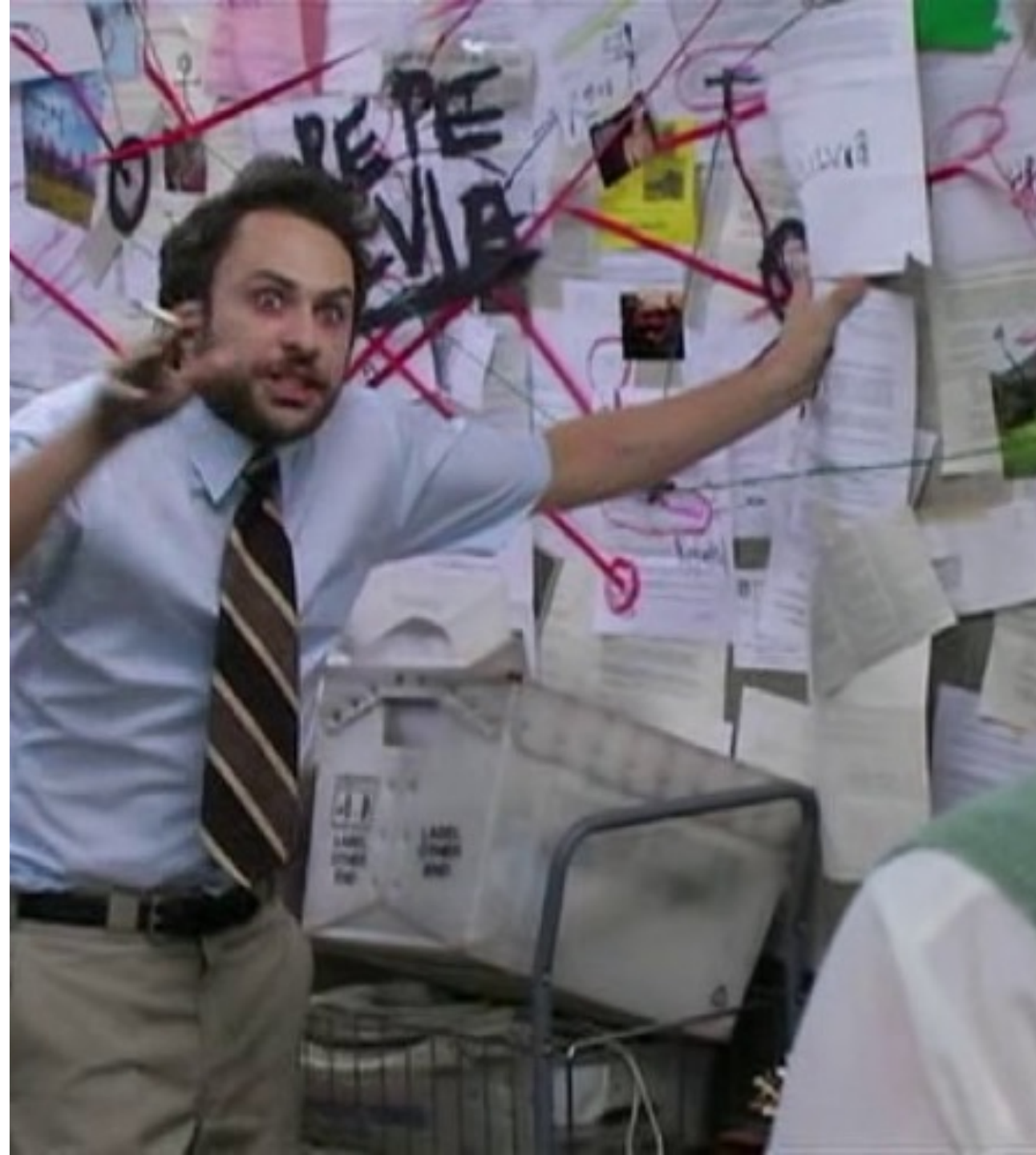
- Most questions can be answered
- Requires derivation work
- Subject to unresolvable contradictions





Role your own

- Requires a lot of mental energy
- Constant vigilance is required to avoid contradictions
- Frequently coincides with madness



Your basis of truth?

Is this program correct?

```
int main() {  
    return 0;  
}
```


Is this program correct?

```
int main(_) {  
    return 0;  
}
```

Is this program correct?

```
#include <climits>

int main() {
    int i = INT_MAX;
    i++;
    return 0;
}
```


Is this program correct?

```
#include <cstdlib>
```

```
int main() {  
    std::abort();  
}
```

Is this program correct?

```
#include <cstdlib>
```

```
int main() {  
    std::exit(0);  
}
```


**What about function
correctness?**

Is f correct?

```
void f(int &i) {  
    i++;  
}
```

Is inc2 correct?

```
void f(int &i) {  
    i++;  
}
```

```
// Sets x to x+2  
void inc2(int &x) {  
    f(x);  
    f(x);  
}
```


Is inc2 correct?

```
void f(int &i) {  
    i++;  
}
```

```
// Sets x to x+2  
// - precondition: x < INT_MAX-2  
void inc2(int &x) {  
    f(x);  
    f(x);  
}
```

Is inc3 correct?

```
// Sets x to x+2
// - precondition: x < INT_MAX-2
void inc3(int &x) {
    ++x;
    ++x;
}
```

Is inc4 correct?

```
// Sets x to x+2
// - precondition: x < INT_MAX-2
void inc3(int &x) {
    ++x;
    ++x;
}
```

```
// Sets x to x+4
// - precondition: x < INT_MAX-4
void inc4(int &x) {
    inc3(x);
    inc3(x);
}
```


Is qfe correct?

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

```
// Returns an x such that ax^2+bx+c=0 holds  
float qfe(float a, float b, float c) {  
    return -b + sqrt(b*b - 4*a*c)/2*a;  
}
```

What can make qfe correct?

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

- a. // Returns an x such that $ax^2+bx+c=0$ holds
- b. // Returns an x such that $ax^2+bx+c=0$ holds or NaN
- c. // Returns an x such that $ax^2+bx+c=0$ holds or NaN
// if it's outside the range that this function can compute.
- d. // Returns an x such that $ax^2+bx+c=0$ holds and none of the
// operations in $'-b + \sqrt{b*b - 4*a*c}/2*a'$ overflow and
// $b^2 > 4ac$

```
float qfe(float a, float b, float c) {  
    return -b + sqrt(b*b - 4*a*c)/2*a;  
}
```

Rigor

Does program correctness have a mathematical basis?

Say a function specification is a predicate P over C++ functions f_x .

$P(f_x)$ holds if f_x adheres to the specification.

- Are these predicates allowed to bifurcate based on non-lexical whitespace?
- What if the predicates consisted of pairs of the world state before the call and the world state after the call?
- Or maybe they consist of relations between before/after world states?
- How would you deal with randomness?

Complexity in contracts

```
// Returns an index to the first element of 'v' not ordered before 'i', or -1 if no such element is found.  
// Runs in  $O(\log(n))$  time.  
// - precondition: v is sorted  
size_t lower_bound(int i, std::span<int> v);
```

- Runtime is not expressible if predicates are relations between before/after world states.
- What about using the C++ abstract machine?
- The as-if rule allows compilers to change complexity. What to do?

Favorite talk of the week: Computing Correctness



Nick Waddoups

Computing Correctness

What can formal verification do for us?

Beginner

Intermediate

Math/Analysis



Do the words "*formal verification*" send shivers of concern down your spine? This talk will introduce the concept of automated formal verification, and explore how learning about automated formal verification provides a foundation for writing clean code that can be reasoned about. While formally verifying an entire code base is not needed for many projects, the principles behind formal verification apply to all projects and can improve your code. This talk specifically explores model checking and deductive reasoning techniques, demonstrates how we can reason "like a computer", and aims to enable better software design.

The Dafny example

```
method bin_search(arr: seq<int32>, target: int32) returns (index: int32)
  requires is_sorted(arr)
  ensures
    || ((exists i :: 0 ≤ i < |arr| && arr[i] = target)
        ⇒ (0 < index < |arr| as int32 && arr[index] = target))
    || (!exists i :: 0 ≤ i < |arr| && arr[i] = target) ⇒ (index = |arr| as int32)
  {
    var low: int32 := 0;
    var high: int32 := |arr| as int32;

    while (low < high)
      invariant 0 ≤ low ≤ high ≤ |arr| as int32
      {
         $\exists i : 0 \leq i < \text{arr.size}() \wedge \text{arr}[i] = \text{target} \implies \text{bin\_search}(\text{arr}, \text{target}) = i$ 
         $\vee \neg \exists i : 0 \leq i < \text{arr.size}() \wedge \text{arr}[i] = \text{target} \implies \text{bin\_search}(\text{arr}, \text{target}) = \text{arr.size}()$ 
        } else {
          high := mid;
        }
      }

    index := low;
  }
```


Does correctness have a solid mathematical foundation?

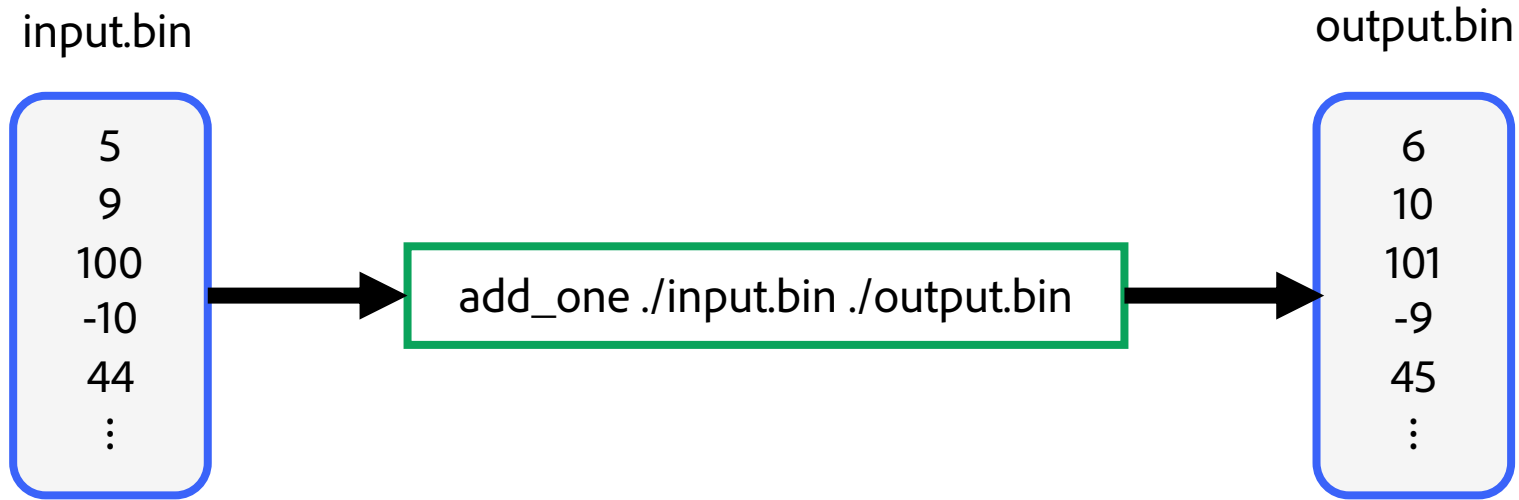
Does correctness have a *satisfying* mathematical foundation?

Does correctness have a *satisfying* mathematical foundation?

Not that I have seen.

- Correctness cannot be separated from human communication
 - Varying degrees of specificity and alignment.
 - All communication counts: including function names.
 - Basis of truth, assumptions, is an essential element
- Correctness and requirements are closely related
 - It is nonsensical to proclaim a solution correct that does not meet agreed-upon requirements
 - “Performance optimized” can be a more useful as a contract than a complexity specification
- Basis of truth must be shared between human participants
 - Using whatever is common will result in more opportunities for discourse

add_one

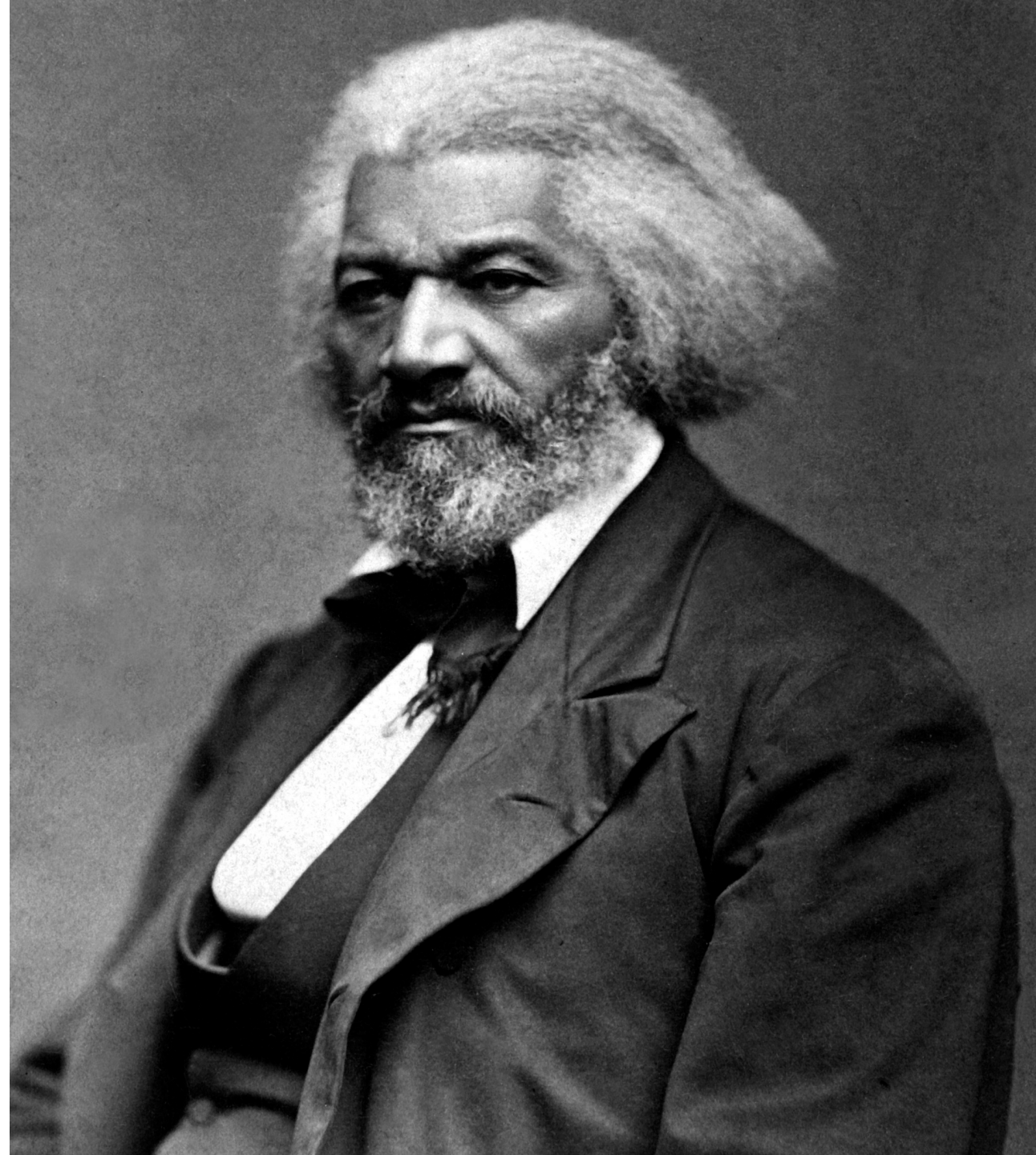


- Files are on an ultra-high performance drive so IO speed is negligible.
- This is being run on a highly specialized embedded processor that isn't superscalar.
- This is a "never enough performance" use-case.
- The input.bin files will never have ints nearing INT_MAX

Is it sometimes better to write incorrect code?

Frederick Douglass

- 1889-1891
- Former slave
- Famous speechwriter and abolitionist



What to the Slave Is the Fourth of July?

FREDERICK DOUGLASS'S "FOURTH OF JULY" SPEECH (1852)

July 5, 1852

Mr. President, Friends and Fellow Citizens:

He who could address this audience without a quailing sensation, has stronger nerves than I have. I do not remember ever to have appeared as a speaker before any assembly more shrinkingly, nor with greater distrust of my ability, than I do this day. A feeling has crept over me, quite unfavorable to the exercise of my limited powers of speech. The task before me is one which requires much previous thought and study for its proper performance. I know that apologies of this sort are generally considered flat and unmeaning. I trust, however, that mine will not be so considered. Should I seem at ease, my appearance would much misrepresent me. The little experience I have had in addressing public meetings, in country school houses, avails me nothing on the present occasion.

The papers and placards say, that I am to deliver a 4th July oration. This certainly, sounds large, and out of the common way, for me. It is true that I have often had the privilege to speak in this beautiful Hall, and to address many who now honor me with their presence. But neither their familiar faces, nor the perfect gage I think I have of Corinthian Hall, seems to free me from embarrassment.

The fact is, ladies and gentlemen, the distance between this platform and the slave plantation, from which I escaped, is considerable—and the difficulties to be overcome in getting from the latter to the former, are by no means slight. That I am here today, is, to me, a matter of astonishment as well as of gratitude. You will not, therefore, be surprised, if in what I have to say, I evince no elaborate preparation, nor grace my speech with any high sounding exordium. With little experience and with less learning, I have been able to throw my thoughts hastily and imperfectly together; and trusting to your patient and generous indulgence, I will proceed to lay them before you.

This, for the purpose of this celebration, is the 4th of July. It is the birthday of your National Independence, and of your political freedom. This, to you, is what the Passover was to the emancipated people of God. It carries your minds back to the day, and to the act of your great deliverance; and to the signs, and to the wonders, associated with that act that day. This celebration also marks the beginning of another year of your national life; and reminds you that the Republic of America is now 76 years old. I am glad, fellow-citizens, that your nation is so young. Seventy-six years, though a good old age for a man, is but a mere speck in the life of a nation. Three score years and ten is the allotted time for individual men; but nations number their years by thousands. According to this fact, you are, even now only in the beginning of your national career, still lingering in the period of childhood. I repeat, I am glad this is so. There is hope in the thought, and hope is much needed, under the dark clouds which lower above the horizon. The eye of the reformer is met with angry flashes, portending disastrous times; but his heart may well beat lighter at the thought that America is young, and that she is still in the impressible stage of her existence. May he not hope that high lessons of wisdom, of justice and of truth, will yet give direction to her destiny? Were the nation older, the patriot's heart might be sadder, and the reformer's brow heavier. Its future might be shrouded in gloom, and the hope of its prophets go out in sorrow. There is consolation in the thought, that America is young. Great streams are not easily turned from channels, worn deep in the course of ages. They may sometimes rise in quiet and stately majesty, and inundate the land, refreshing and fertilizing the earth with their mysterious properties. They may also rise in wrath and fury, and bear away, on their angry waves, the accumulated wealth of years of toil and hardship. They, however, gradually flow back to the same old channel, and flow on as serenely as ever. But, while the river may not be turned aside, it may dry up, and leave nothing behind but the withered branch, and the unsightly rock, to howl in the abyss-sweeping wind, the sad tale of departed glory. As with rivers so with nations.

Editor

Editor Score

76%

Formal writing

Corrections

Spelling

18

Grammar

135

How does correctness relate to quality?

- *What* is incorrect makes a difference.
 - Did they take 1 point of or 10 points off?
- There's frequently a curve
 - How did the rest of the class do?
- Sometimes correctness is a very small component
 - Essay question vs. multiple choice
 - Interface design

Are we writing correct programs?

Say we write 30-line functions correctly 99.9% of the time.

Consider a 1-million-line program. How likely is it that it is correct?

$$(0.999)^{33333} \approx 2.195 \times 10^{-15}$$

Or 0.00000000000002195% of the time

We've made the decision to write incorrect code.

We've made the decision to write incorrect code.

- I'm not sure we could if we wanted to
- Sometimes we talk as if
 - Writing correct code is our goal
 - Correct code trumps other quality considerations

Let's be real

- Admit the tradeoffs we're making between correctness and other quality factors (e.g. cost, time to market, staffing limitations)
- There's a difference between consequential bugs and non-consequential bugs
- We need to share and learn more about the other, frequently more important, aspects of software quality

Conclusion



Click to add text



Adobe