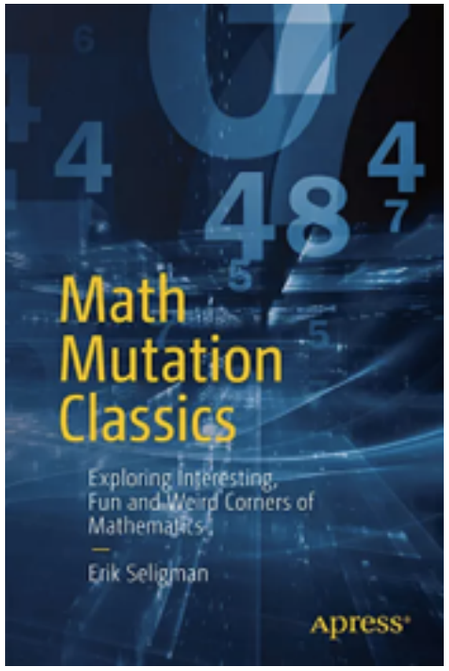
PARADOXES, MATHEMATICAL ODDITIES, AND FORMAL VERIFICATION

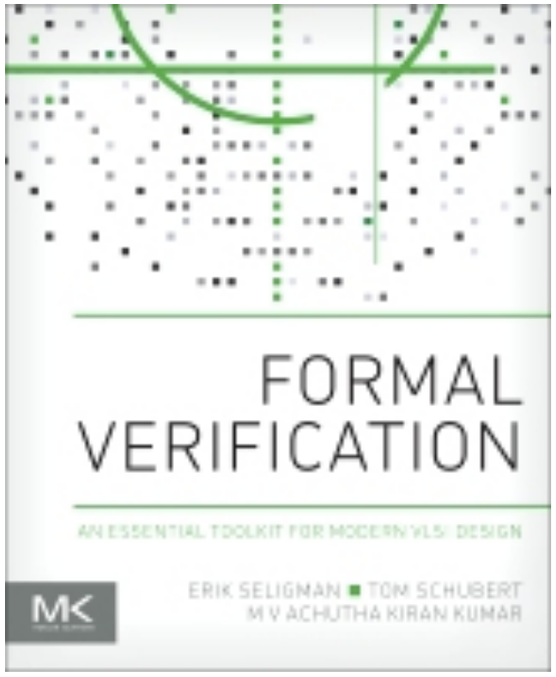
Erik Seligman

4/23/2019

DISCLAIMER

- Presentation is by Erik Seligman, author of

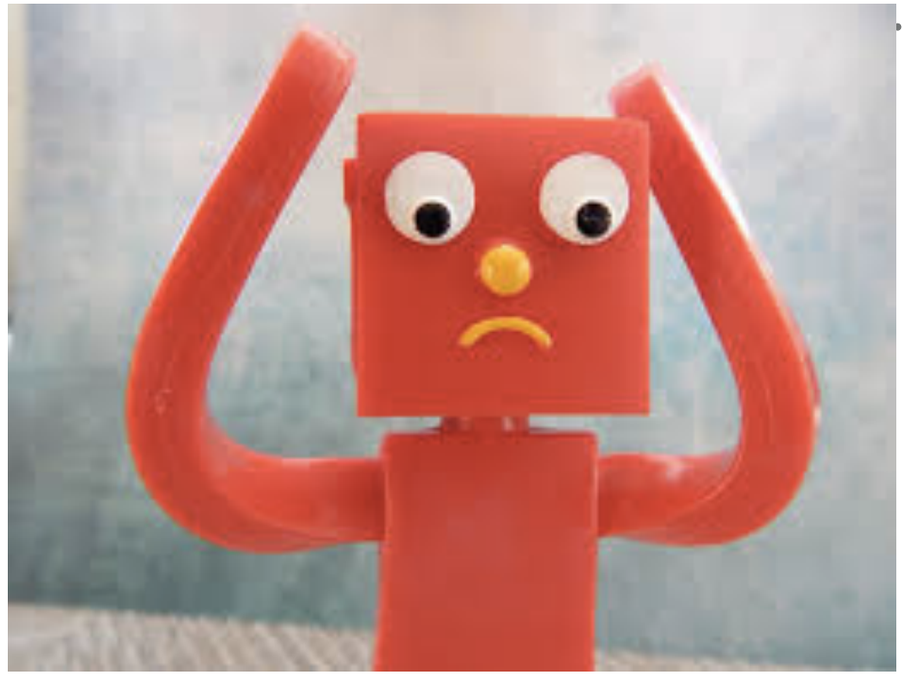




- and host of Math Mutation podcast…

- …NOT endorsed by any company in particular.

PARADOXES AND ODDITIES



- *Paradox*: Math statement that seems self-contradictory
- *Oddity*: Mathematical fact that might surprise you
  - Sometimes fuzzy boundary: *"This statement cannot be proven"*.
- Often resolvable in a line or two of algebra...
- .. but can provide qualitative insights into thought process

OUTLINE OF TALK

- Playing with Premises
- Amusing Assumptions
- Management Mania

OUTLINE OF TALK

- Playing with Premises
- Amusing Assumptions
- Management Mania

PLAYING WITH PREMISES

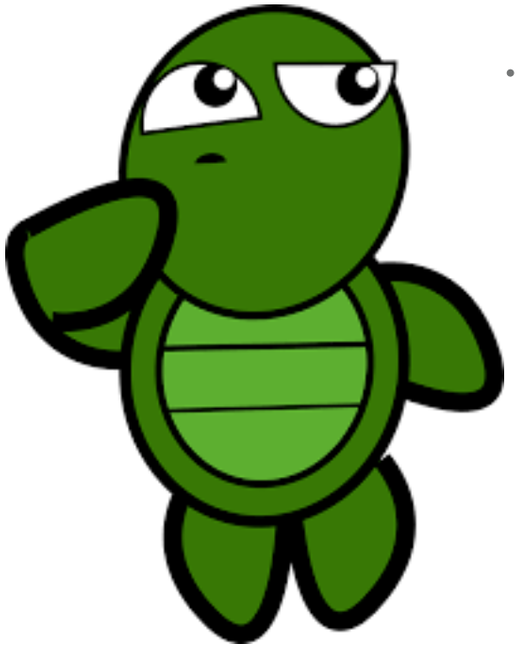
AN APOLOGY

- Speaker's Promise: I'll probably lie to you today.

AN APOLOGY: PROOF

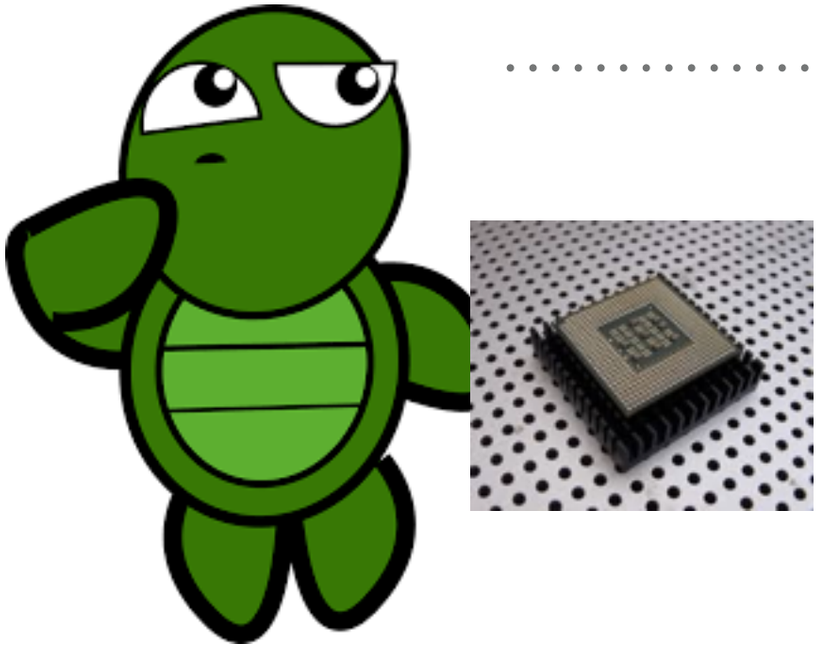
- Speakers Promise: I'll probably lie to you today.
- Assume I'm 97% accurate at any given minute
  - Talk 45 min ==> (.97^45) = .25
  - ==> *75% chance I'll say something wrong!*
  - David Makinson's "Preface Paradox"
- *Remember that even in a series of very accurate checks, small error chances accumulate!*

CARROLL'S STUBBORN TORTOISE



- Achilles: "P->Q, and P, therefore Q!"
    - Tortoise: You have another premise there…
    - ((P->Q) & P)) -> Q
- Achilles: "OK, you win. But with that, it's proven…"
    - Tortoise: Not so fast…
    - (((P->Q) & P)) -> Q) & (P->Q) & P -> Q
- (from dialogue by Lewis Carroll)

CARROLL'S STUBBORN VALIDATION ENGINEER



- When is a design "really" proven?
  - Did you enter correct specs into FPV tool?
  - Was FPV tool correctly implemented in C++?
  - Was C++ compiler formally verified?
  - Was it run on a formally verified OS?
- *"Full Proofs" always contain unproven assumptions!*

GRUE AND BLEEN

- Is this a blue house & a green house?

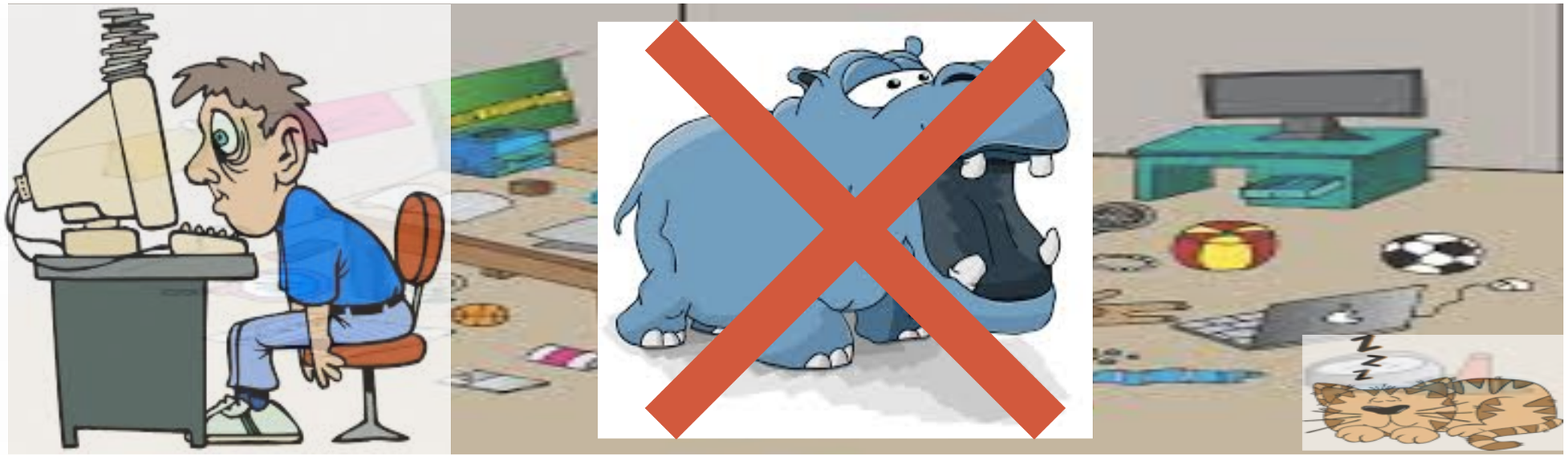
GRUE AND BLEEN

- Left house was GRUE: Green until 5 seconds ago, then blue
- Right house was BLEEN: similar definition
- How can you tell Grue & Bleen from Blue and Green?
  - Nelson Goodman's "new riddle of induction"

GRUE AND BLEEN AND PROOFS

- Left house was GRUE: Green until 5 seconds ago, then blue
- Right house was BLEEN: similar definition
- How can you tell Grue & Bleen from Blue and Green?
  - Nelson Goodman's "new riddle of induction"
- *Are you sure you've defined the right primitives?*
- *Be careful about bounded proofs, things can change!*

STUDYING HIPPOS IN MY BASEMENT

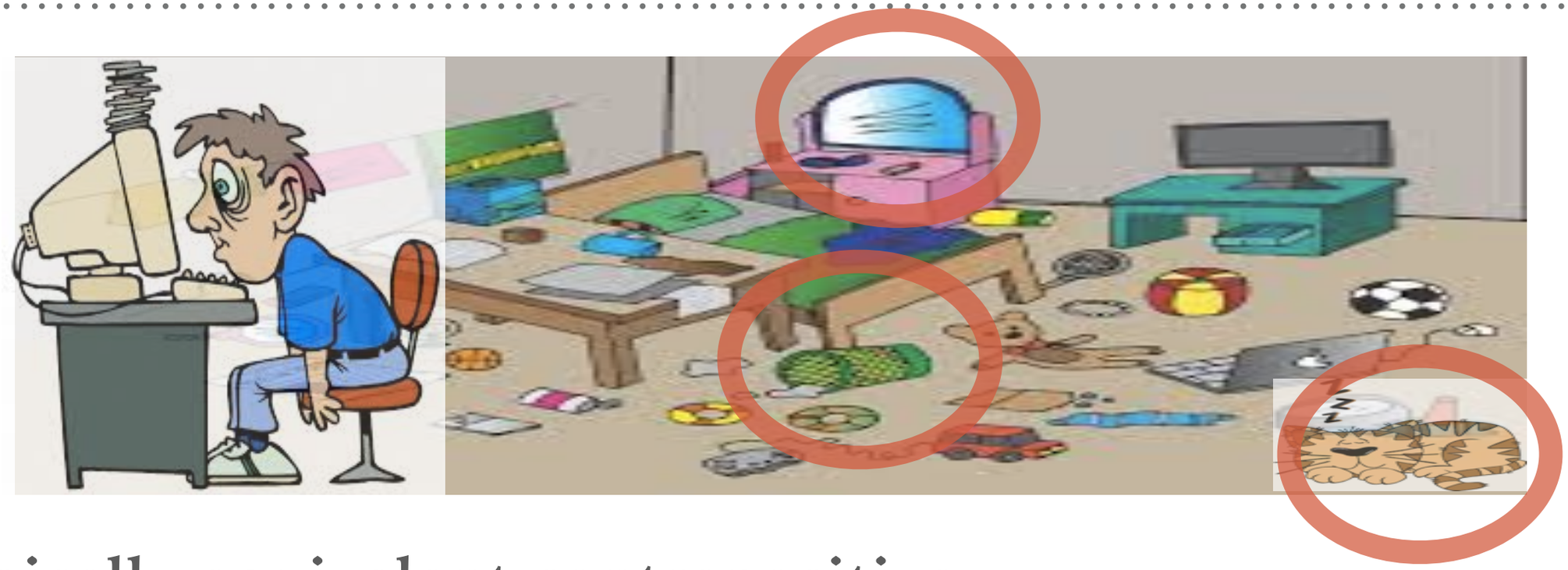


- I want to be a Hippologist… but too lazy to leave house
  - and wife won't let me get a pet hippo
- Can I gather evidence for *"X is Hippo ==> X has big nose"*?

STUDYING HIPPOS— USING CONTRAPOSITIVES

- I want to be a Hippologist… but too lazy to leave house
- Can I gather evidence for "*X is Hippo ==> X has big nose*"?
- Logically equivalent contrapositive (A->B == !B->!A)
  - *X doesn't have big nose ==> X is NOT hippo*
- Now it's easy to find confirming instances!

CONSIDER THE CONTRAPOSITIVE



- Logically equivalent contrapositive:
  - *A->B is equivalent to !B->!A*
- *Implication can go two ways— choose the most useful!*
  - *Which direction has the more meaningful trigger?*
  - *Which direction specifies the 'unusual' condition?*

OUTLINE OF TALK

- Playing with Premises
- Amusing Assumptions
- Management Mania

AMUSING ASSUMPTIONS

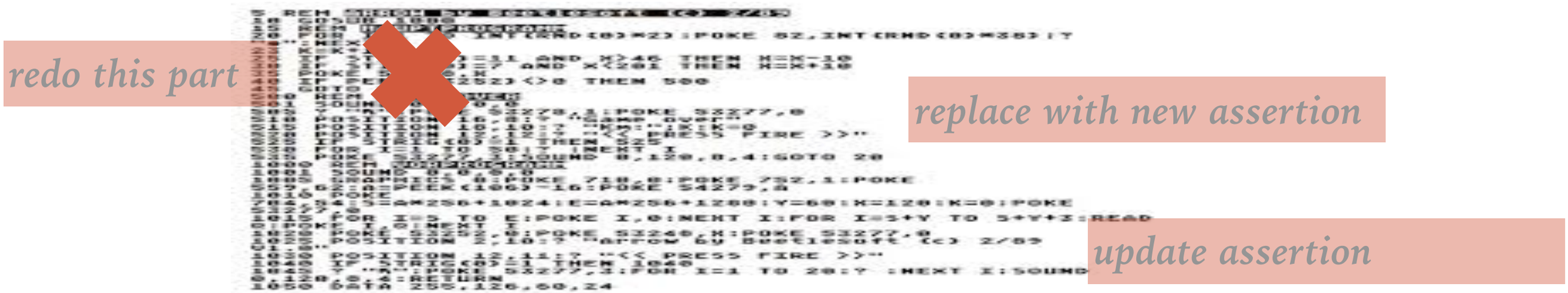
THE SHIP OF THESEUS

- Museum decides the Ship of Theseus needs renovation
  - Old plank thrown in junkyard
  - Plank replaced: is it the same ship?

THE SHIP OF THESEUS (II)

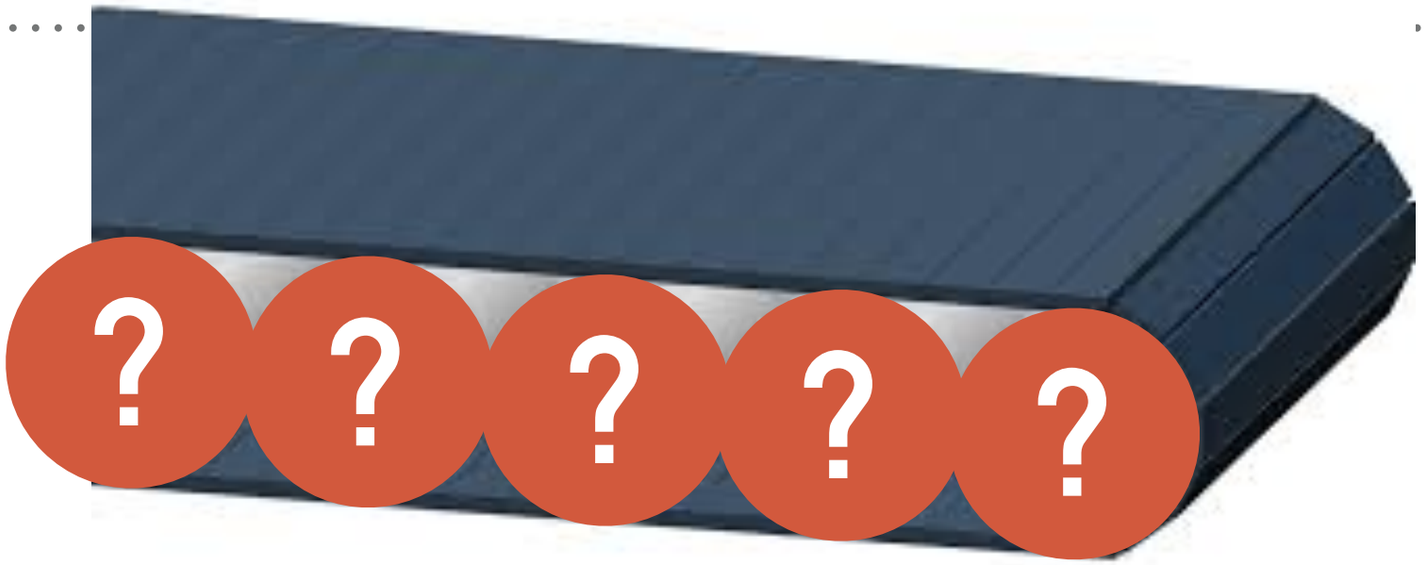
- A bum at the junkyard assembles discarded planks…
  - Which is the real ship?

THE VERIFICATION IP OF THESEUS



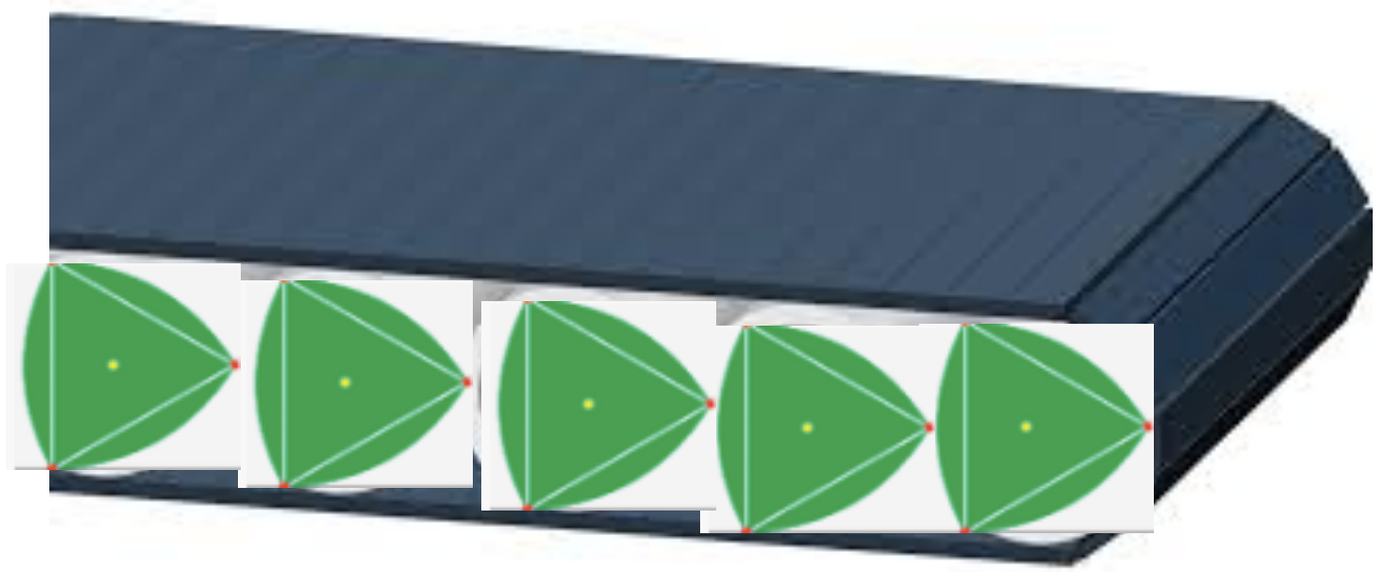
- *How about with Verification IP?*
  - *How much change makes it a new IP?*
  - *How much change requires re-verification vs spec?*

AN ALTERNATE SHAPE FOR WHEELS

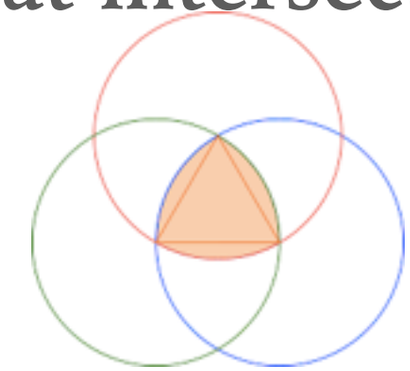


- Problem: smooth travel down assembly line.
- What are the assumptions for our rollers?

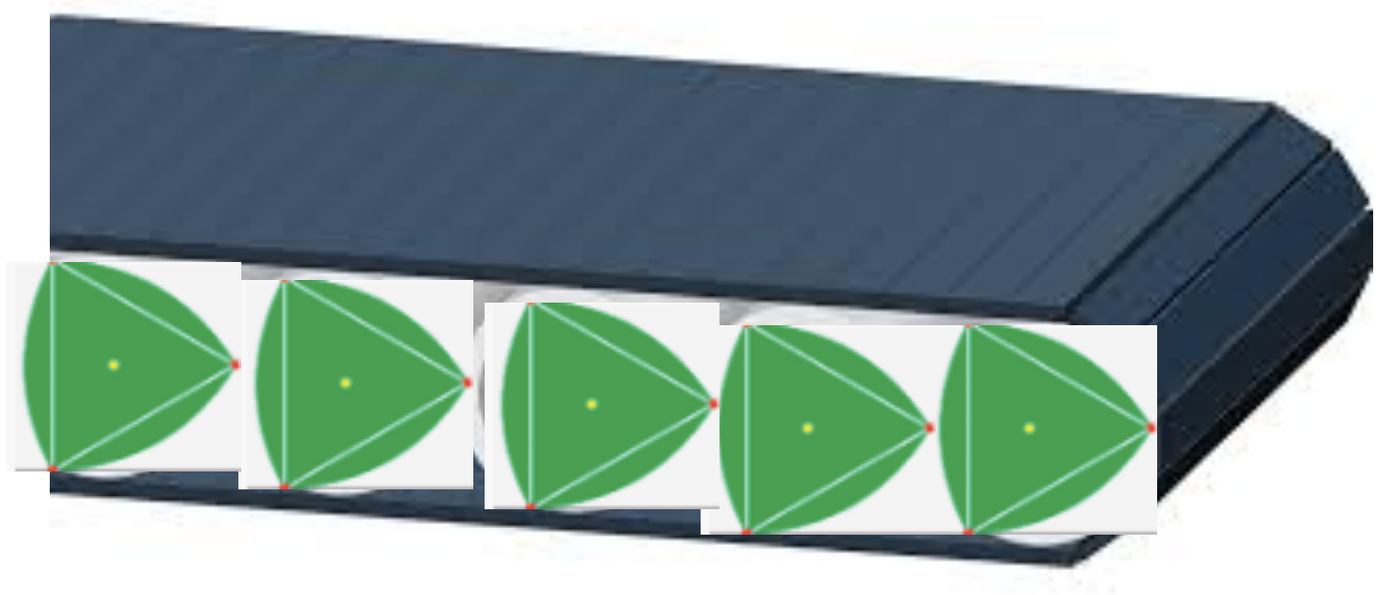
AN ALTERNATE SHAPE FOR WHEELS (II)



- Problem: smooth travel down assembly line.
- What are the assumptions for our rollers?
  - We need *curves of constant width— not necessarily circles!*
- Reuleaux Triangles- form at intersection of 3 circles



AN ALTERNATE SHAPE FOR WHEELS (III)

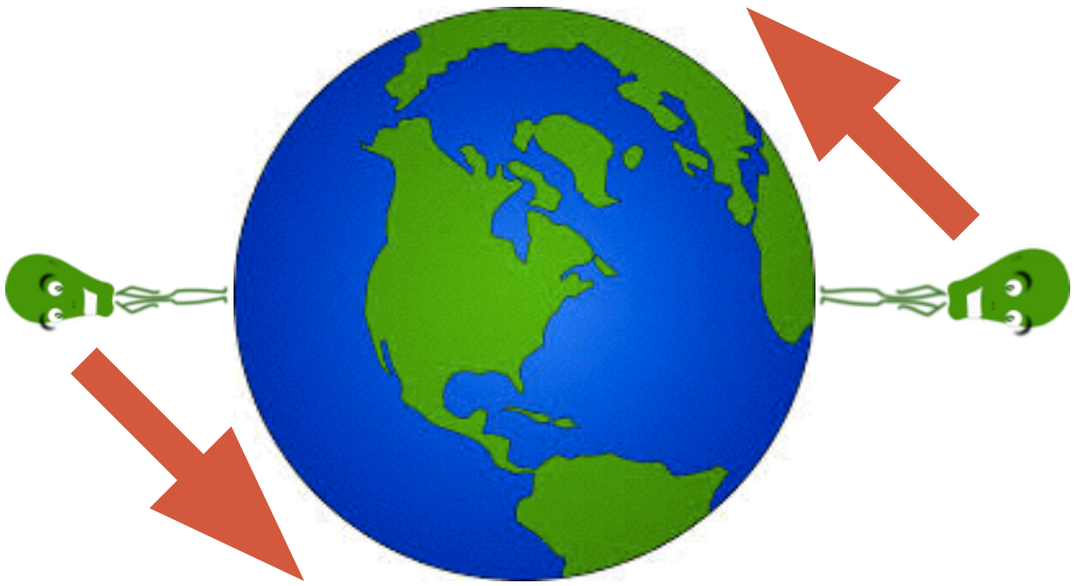


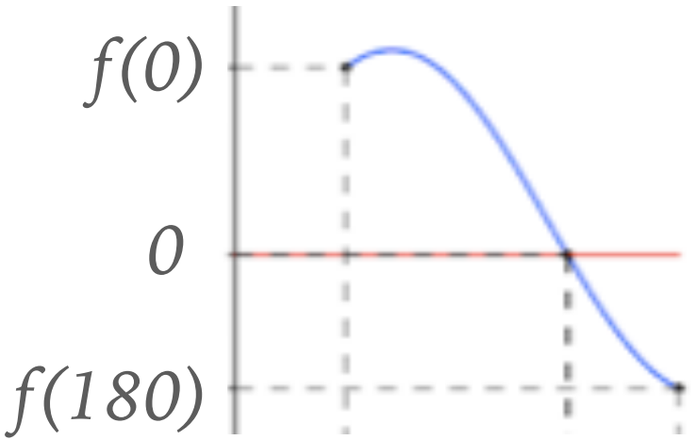
- Problem: smooth travel down assembly line.
- What are the assumptions for our rollers?
  - We need *curves of constant width— not necessarily circles!*
- *Enforce the spec, not a preconceived solution*

INTERMEDIATE VALUE PUZZLE

- Q: Are there 2 antipodal points on Earth that are the same temperature, right now?

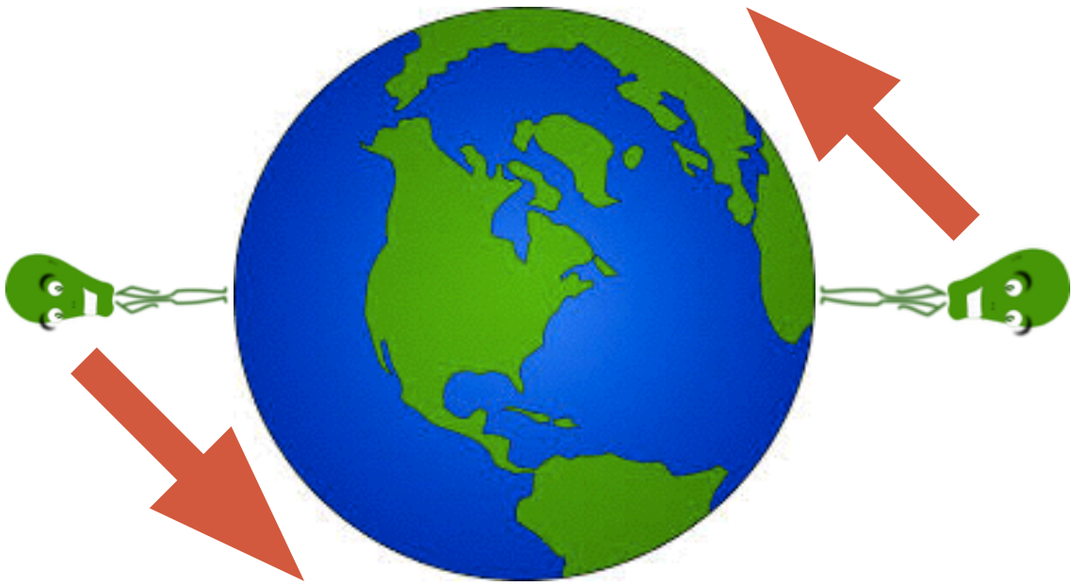
INTERMEDIATE VALUE PUZZLE (II)

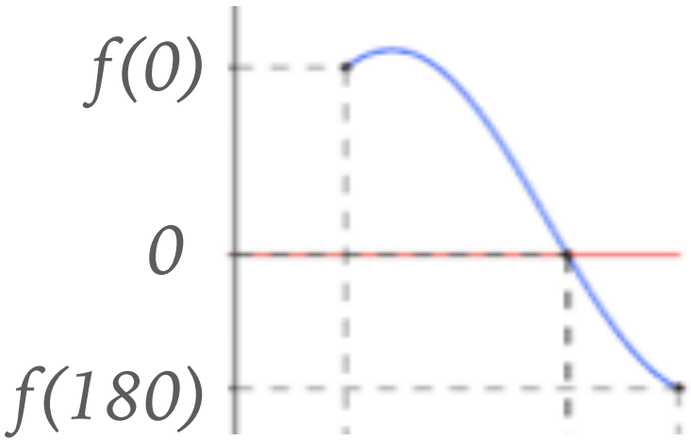




- Q: Are there 2 antipodal points on Earth that are the same temperature, right now?
- Use the *Intermediate Value Theorem:*
  - *If $f(a)>0$ and $f(b)<0$, and f is continuous*
    - *there is some point c between them where $f(c) = 0$.*
- Start at opposite points p and q
  - f(angle) = Temp(p) - Temp(q) = T at 0, -T at 180
  - ==> Somewhere between them, f(angle)= 0!

INTERMEDIATE VALUE PUZZLE (III)



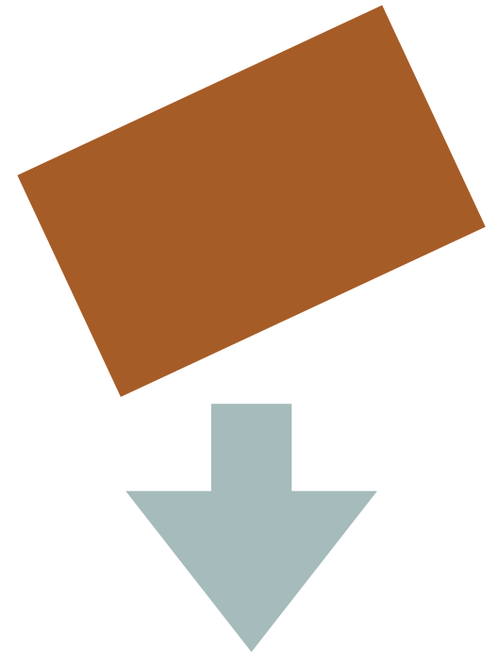


- Q: Are there 2 antipodal points on Earth that are the same temperature, right now?
- Provable using basic principles
  - Temperature is continuous
  - Intermediate Value Theorem
- *Be ready for far-reaching consequences of simple assumptions*

TERRELL ROTATION

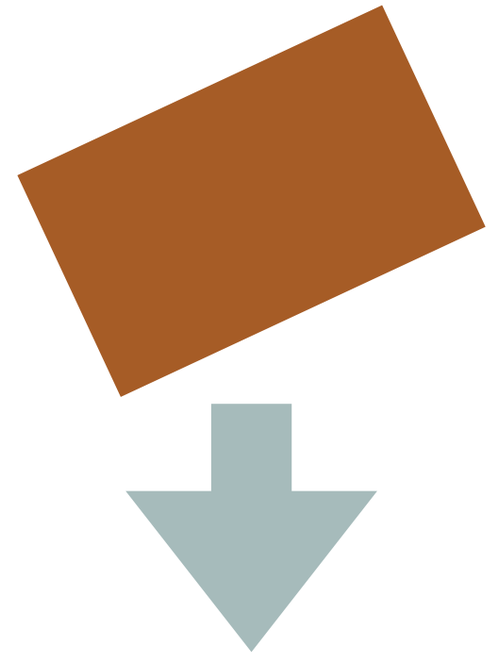
- We remember from relativity: if object is traveling close to speed of light, it shortens relative to observer
- If a square zooms past you… what do you see?

TERRELL ROTATION (II)



- We remember from relativity: if object is traveling close to speed of light, it shortens relative to observer
- If a square zooms past you… what do you see?
  - Actually, you see a *rotated* rectangle
  - Light from forward and rear edges arriving at slightly different times

TERRELL ROTATION (III)



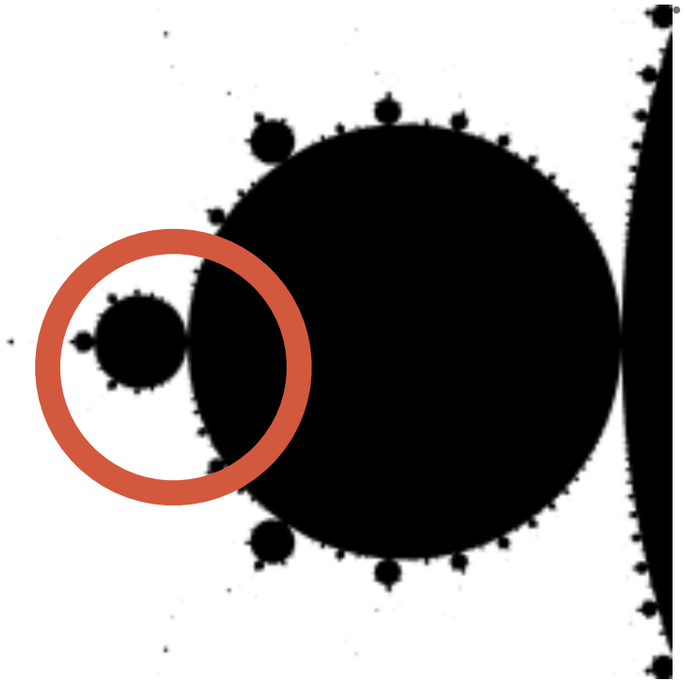
- For decades after Einstein, everyone got this wrong!
  - Common textbook illustrations omitted rotation
  - Famous physicists never thought it through
  - Terrell finally published real solution in 1959
- *All the smart people can miss something.*

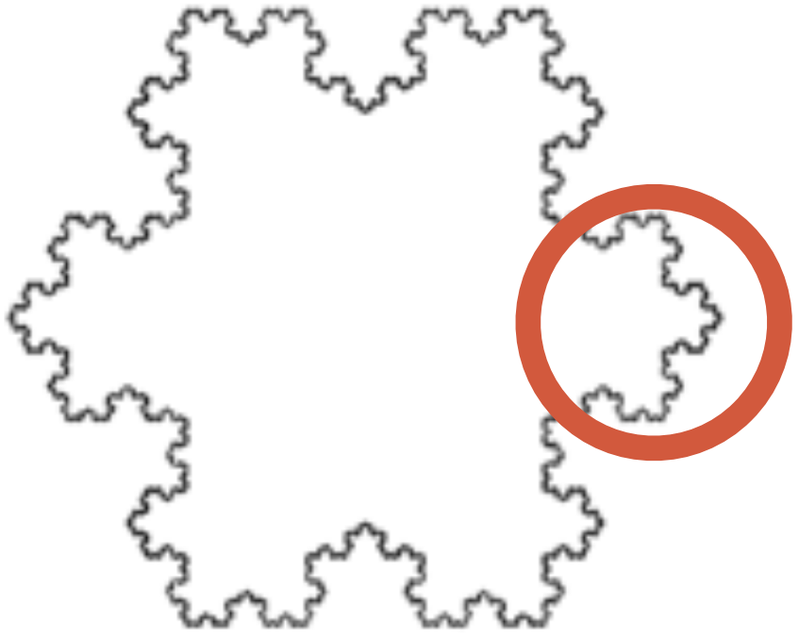
OUTLINE OF TALK

- Playing with Premises
- Amusing Assumptions
- Management Mania

MANAGEMENT MANIA

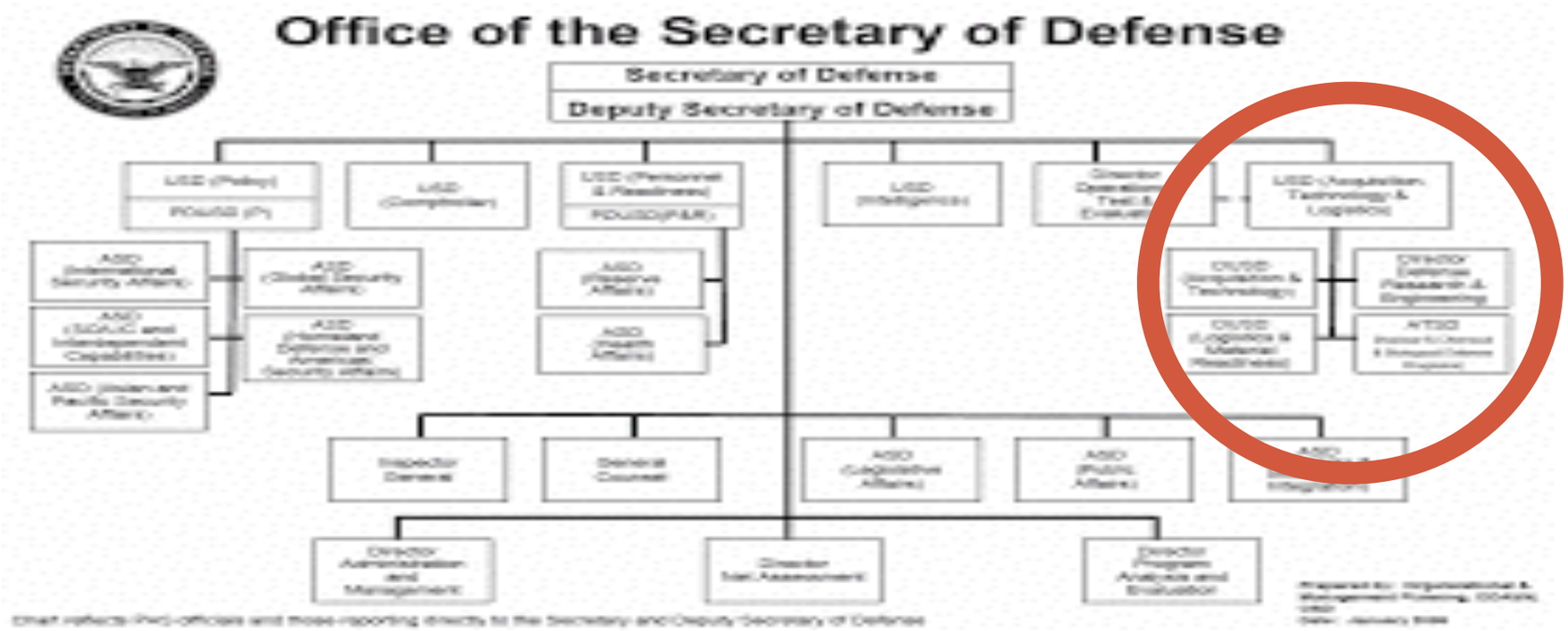
SELF-SIMILAR FRACTALS





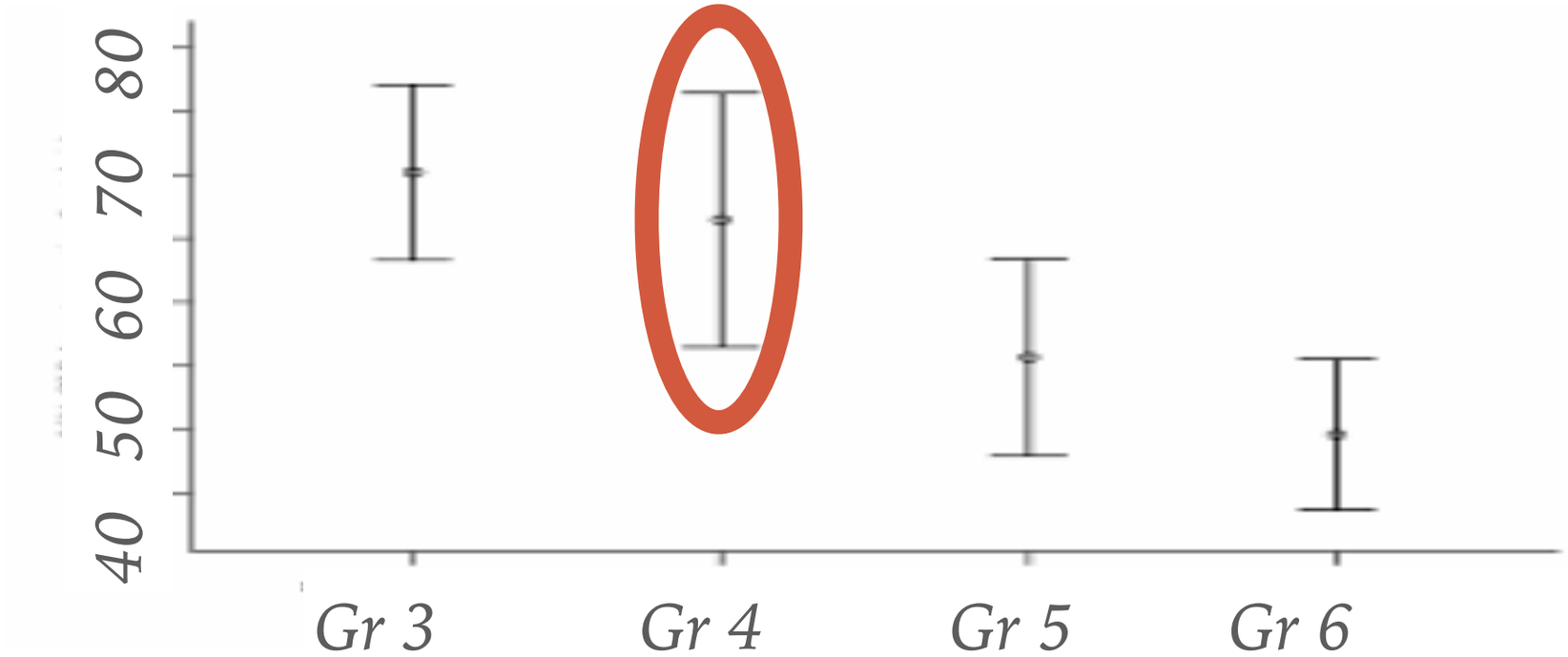
- Fractals: complex forms that are often self-similar

SELF-SIMILAR ORGANIZATIONS



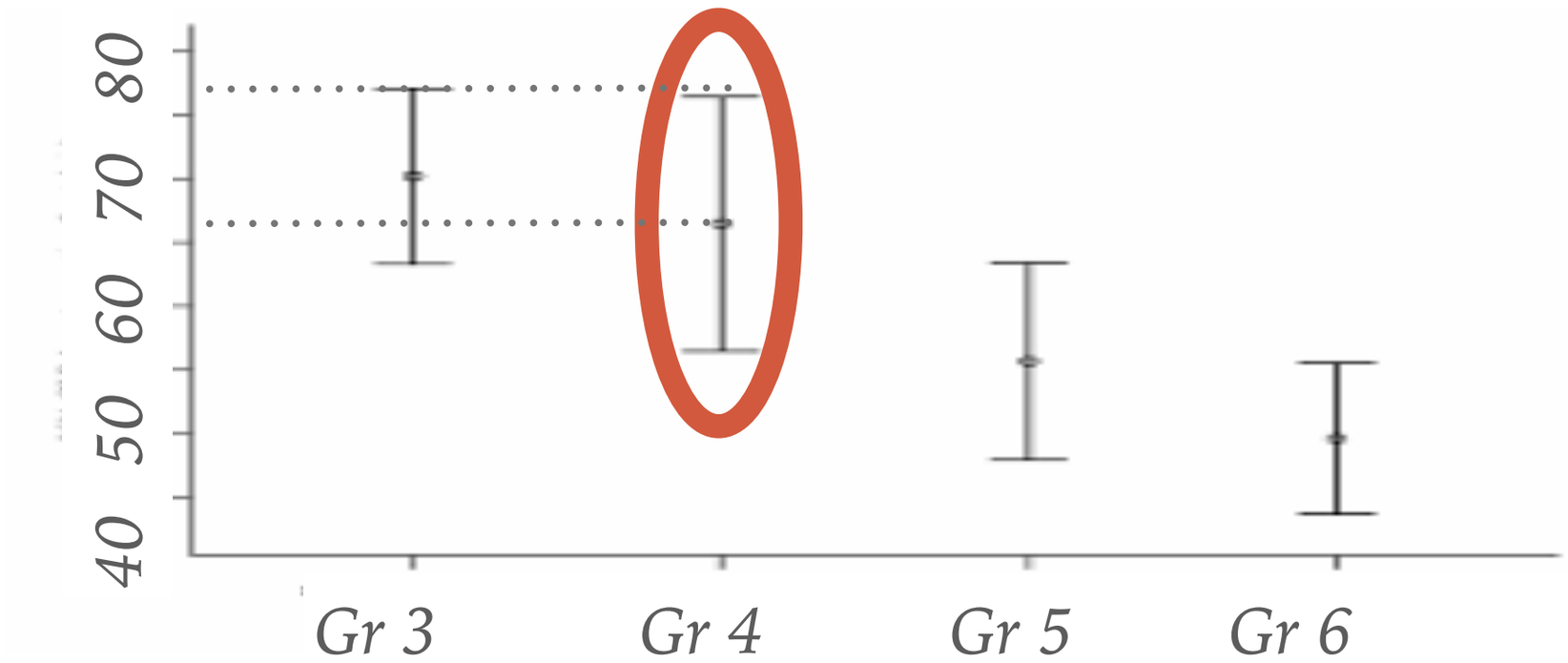
- How is an organization like a fractal?
  - *Parts of an org should reflect the same values as the top level*
  - (from Margaret Wheatley book)

ADJUSTED STATISTICS



- Graphs of results often come with error bars
- How to deal with uncertain results?
- Gr4 above == 66 +/- 11?

ADJUSTED STATISTICS IN GOVERNMENT



- "Adjusted Score" = value + error bar
  - Maximizes optimism for reporter
  - Gr 4 above has average of 66, but "adjusted score" of 77!
  - No comment on ethics…
- *If anyone claims to provide an "adjusted" measurement, investigate details of the adjustment*

ZENO'S PARADOX

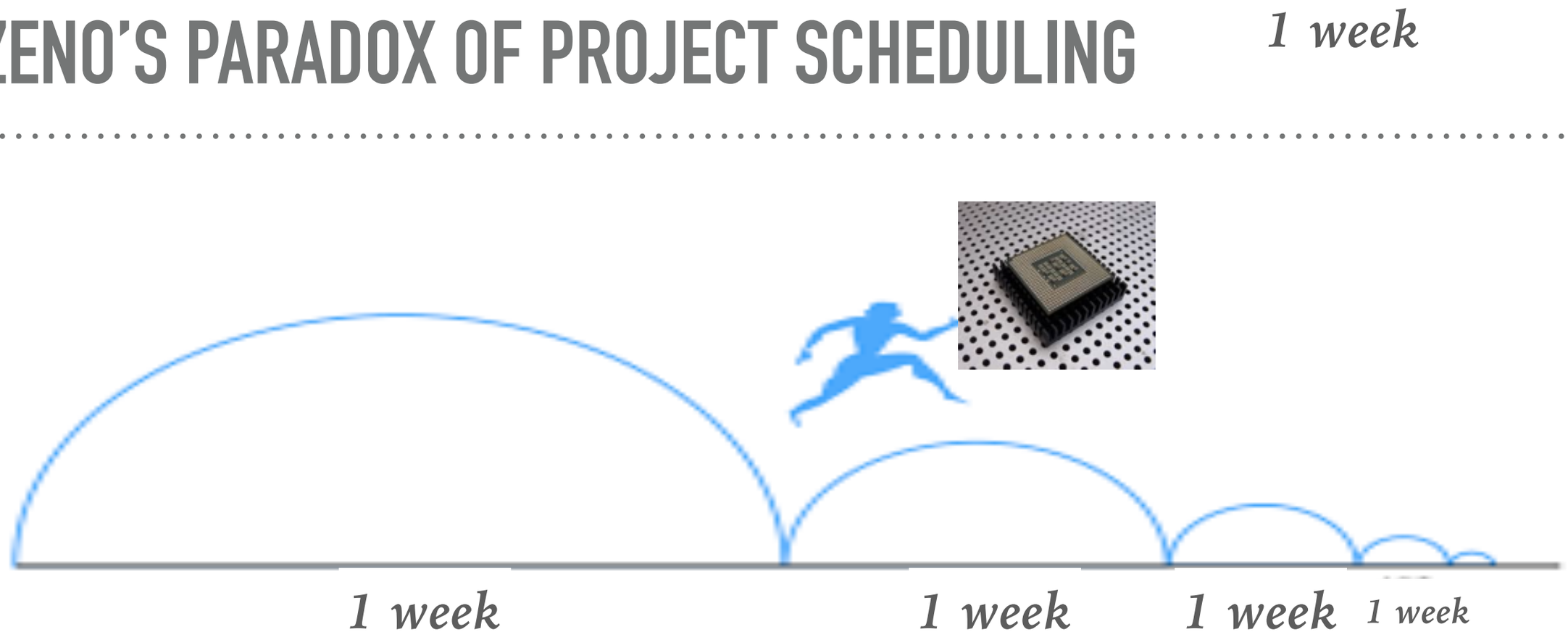
- An old classic, must be included in any paradox discussion!
  - Actually one of several similar paradoxes
- Can the Achilles cross the road?

ZENO'S PARADOX: SOLVED

- Can Achilles cross the road?
- *Solution: Infinite sum of infintesmals can be finite*

$$\sum 1/2^n = 1$$

ZENO'S PARADOX OF PROJECT SCHEDULING



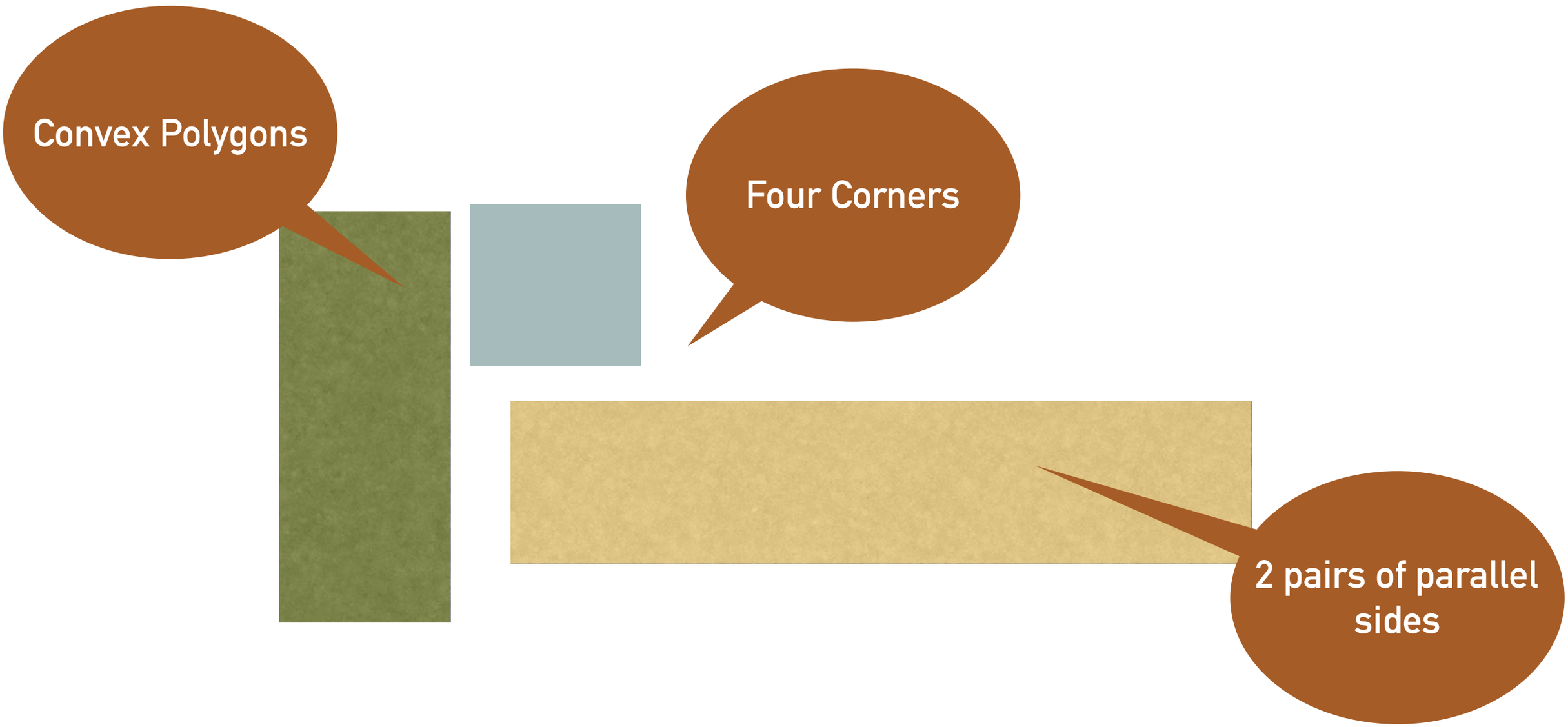
- Can Achilles ever finish FVing his design?
- *No longer a sum of infinitesimals*
- *As you tackle harder complexity issues, full proof efforts can stretch forever: create good bounded signoff criteria!*

ABUSING INDUCTION

- Q: What makes a rectangle a rectangle?
- To answer, observe a few…

ABUSING INDUCTION (II)

- Q: What makes a rectangle a rectangle?
- To answer, observe a few...



ABUSING INDUCTION (III)

- Q: What makes a rectangle a rectangle?
- Some common features:
  - Convex polygon
  - Four corners
  - Two pairs of parallel sides

Oops!

ABUSING INDUCTION (IV)- THE CONVERSE OF OUR INTENT

- Q: What makes a rectangle a rectangle?

Oops!

- What went wrong?
  - Only looking at *positive* examples gives us
    - (rectangle) ==> P
  - We also need to look at *negative* examples to infer
    - P ==> (rectangle)

ABUSING INDUCTION FOR CAREER ADVICE

- "I want to be a CEO"

Live in CA

Smart People

Interesting Hair

ABUSING INDUCTION FOR CAREER ADVICE

- "I want to be a CEO"
  - Need to contrast positive & negative examples

What's true about these people…

But not these?

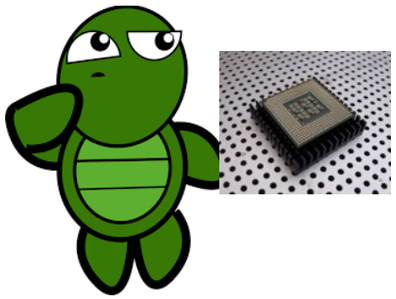
- *To gain wisdom through induction, always need to look at examples of both success and failure*
  - *Also applies to case study papers…*

SUMMARY

IMPORTANT LESSONS: PLAYING WITH PREMISES

- Preface Paradox in Validation

- Carroll's Stubborn FV-Implementing Tortoise



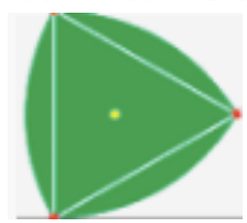
- Grue and Bleen and Primitives

- Contrapositive Hippos

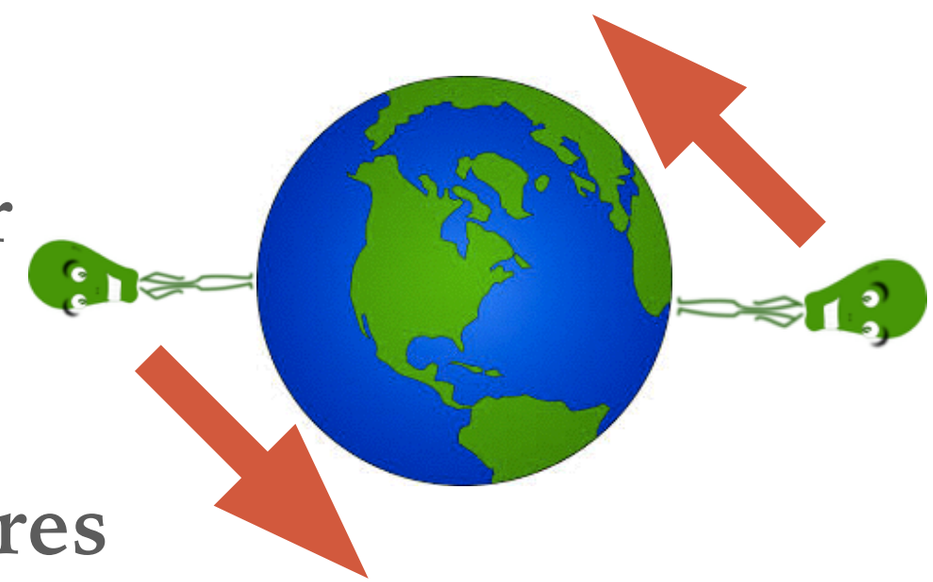
IMPORTANT LESSONS: AMUSING ASSUMPTIONS

- The Verification IP of Theseus

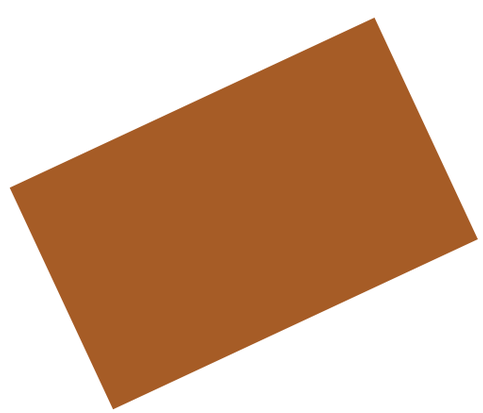
- Reuleaux's Non-Round Wheels



- Theorem-Controlled Weather



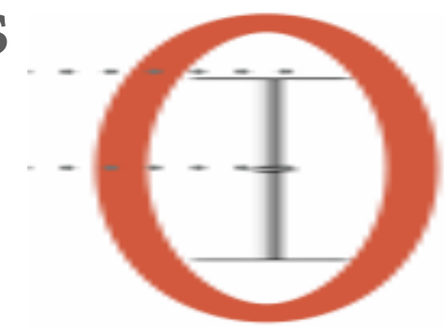
- Smart Physicists' Terell Failures



IMPORTANT LESSONS: MANAGEMENT MANIA

- The Fractal Organization

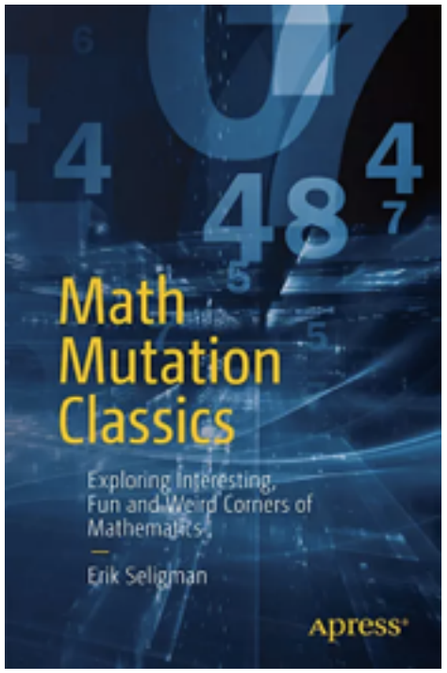
- The Truth about "Adjusted" Statistics

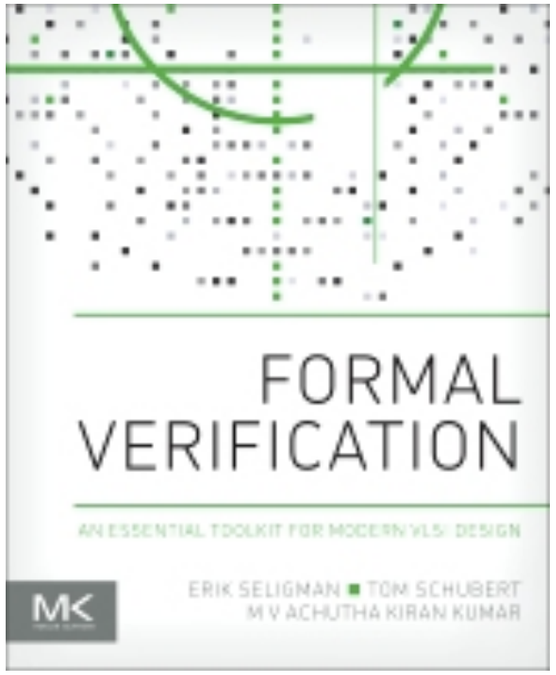


- Zeno's Paradox of Project Scheduling

- Abusing Induction for CEOs and Case Studies

FURTHER READING





- http://mathmutation.com
- http://formalverificationbook.com