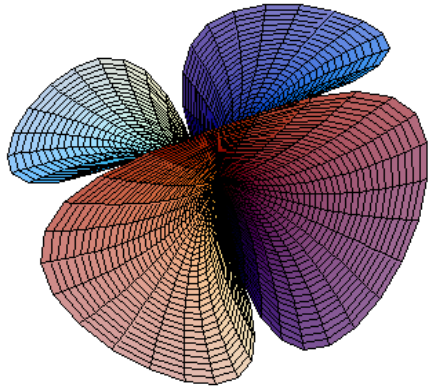
COMPUTER ASSISTED PROOFS:
COMING SOON TO A THEOREM NEAR YOU

By Sara Billey

University of Washington

March 23, 2015

Mathday 2015



http://en.wikipedia.org/wiki/Roman_surface

Outline

1. Human proofs vs computer-assisted proofs.
2. The first major computer proof: 4 Color Theorem
3. Hales' proof of Kepler's conjecture
4. Zeilberger's proof of Conway's Lost Cosmological Thm
5. Philosophical Questions

Definition of “Proof”

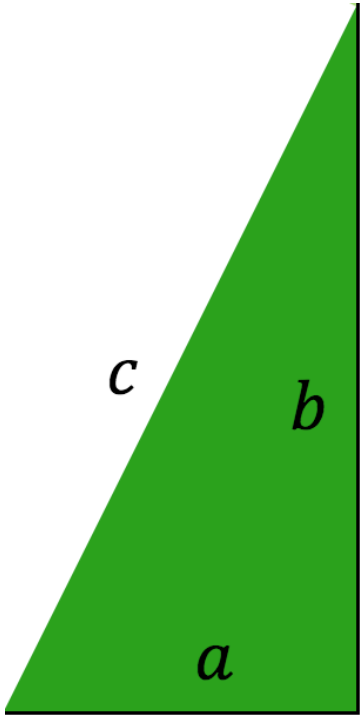
- Proof: An argument or evidence establishing the truth of a statement.

- From Bing:
- Definitions of **proof** (n)
- proof [proof]
- **conclusive evidence:** evidence or an argument that serves to establish a fact or the truth of something
- **test of something:** a test or trial of something to establish whether it is true
- **state of having been proved:** the quality or condition of having been proved
- **Synonyms:** resistant, resilient, impervious, immune

Statement

If a right triangle has sides lengths a,b,c, then $a^2 + b^2 = c^2$.

True or False?

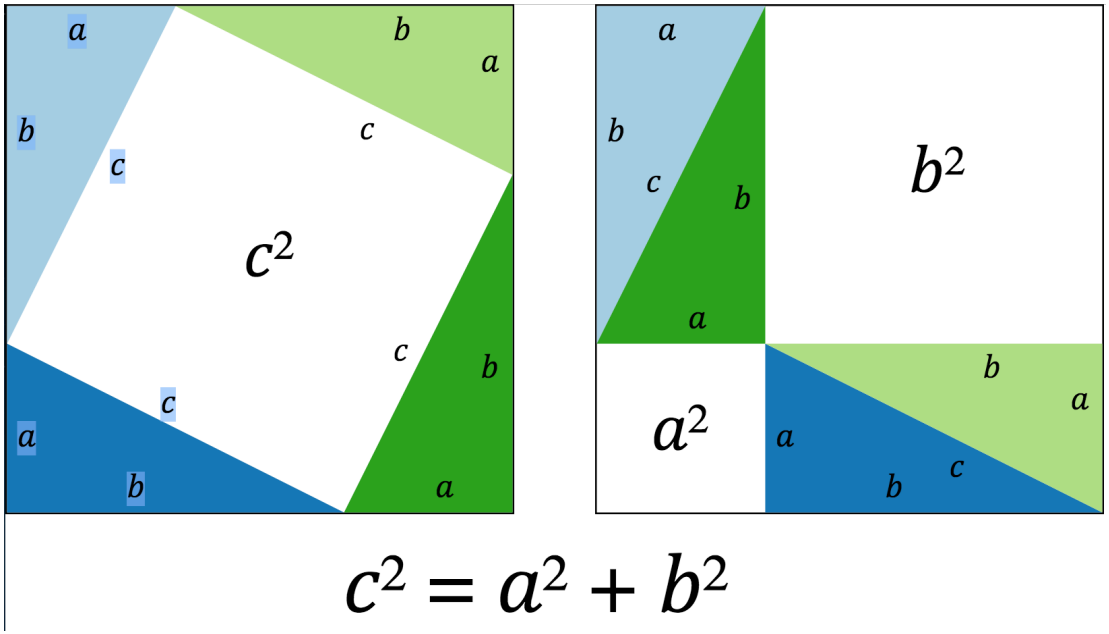


Classic Human Proof

Pythagorean Theorem (500BC):

If a right triangle has sides lengths a,b,c, then $a^2 + b^2 = c^2$.

Proof by picture:



$$c^2 = a^2 + b^2$$

http://upload.wikimedia.org/wikipedia/commons/9/9e/Pythagoras-proof-anim.svg

Q.E.D.

Examples of Computer Proof

Use symbolic algebra package like Maple, Mathematica or Sage.

- Simplify polynomials
- Trigonometric identities
- Integrals
- Finite sums

Go to Maple Demo.

Examples of Computer Proof

Next topic: The Four Color Theorem

Statement

- **“Every map of states/countries/counties etc can be colored using 4 colors such that no two adjacent states are given the same color.”**

- True or False?

- Caveats: No two states touch at isolated points. Each state is connected.
- Could you 4-color a big map like the United States?

A 4-coloring of the states

http://en.wikipedia.org/wiki/File:Map_of_USA_with_state_names.svg

Experiment

Try constructing a map for yourself which requires 5 colors.

Statement

"**Every map of states/countries/counties etc can be colored using 4 colors such that no two adjacent states are given the same color.**"

Colorful History:

- 1852: Conjectured to be true by Francis Guthrie (cartographer or botanist).
- Francis Guthrie -> Fredrick Guthrie -> Augustus De Morgan -> Arthur Cayley

Colorful History

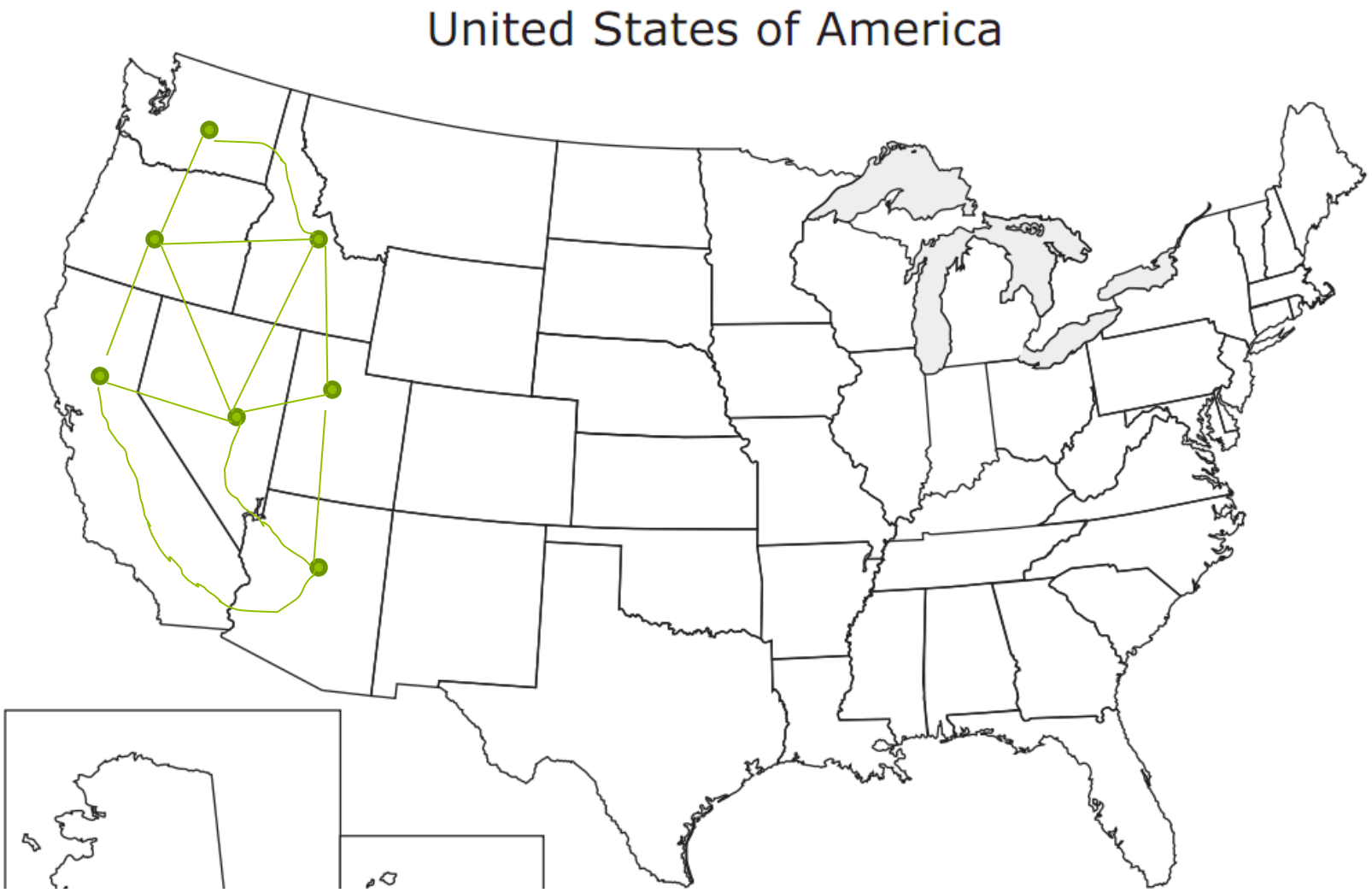
- 1852: Conjectured to be true by Francis Guthrie
- 1878: Cayley published Guthrie's conjecture.
- 1879: Kempe published a proof.
- 1880: Tait published a proof.
- 1890: Heawood pointed out a flaw with Kempe's proof!
- 1891: Petersen pointed out a flaw with Tait's proof!
- …. Many proofs appear and get rejected. But much progress was made along the way. The field of graph theory was born into mathematics.
- 1976 : Appel and Haken publish a highly controversial computer assisted proof. NY Times refuses to mention it.

Mathematical Reformulation

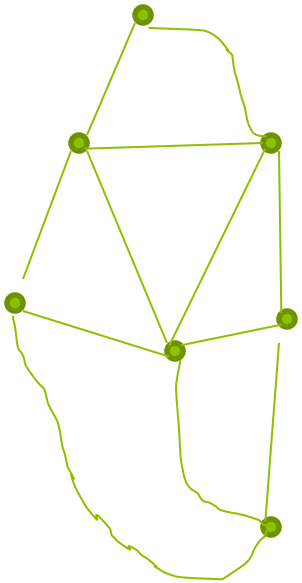
- Instead of coloring maps, the problem was generalized to coloring planar graphs.

- Place a bold dot on each state on the map.
- Connect the dots representing two states by a path if and only if they are adjacent on the map.
- Delete the map.

Each dot is a vertex of the graph. Each path is an edge of the graph.



Delete the map. What remains is a planar graph.



A graph G=(V,E) is a set of vertices V and a subset of all pairs of vertices E.

G is planar if all the edges can be drawn in the plane without crossing each other.

Four Color Theorem

“Every vertex in a planar graph can be assigned a color distinct from all of its adjacent neighbors using at most 4 colors.”

To date, there is no human only proof.

Four Color Theorem

“Every vertex in a planar graph can be assigned a color distinct from all of its neighbors using at most 4 colors.”

1976 : Appel and Haken publish a highly controversial computer assisted proof.

Good ideas in the Appel-Haken Proof

Outline: Assume G is a counterexample to the 4CT with a minimal number of vertices.

- Reducibility: There are 1478 configurations in graphs which cannot appear in a minimal counterexample.
- Unavoidability: Every minimal counterexample must contain one of the 1478 configurations on the list.

Question: What can you conclude about G?

Answer: G does not exist!

Controversy over Computer Proof

- Imagine back to 1976 when the 4 Color Theorem was first proved by Appel and Haken ..

PDP-8 Computer built around 1970

```
Assembly Language (from Wikipedia:  http://en.wikipedia.org/wiki/PDP-8)
********************************************************************************
This complete PDP-8 assembly language program outputs "Hello, world!" to the teleprinter.
  *10                / Set current assembly origin to address 10,
  STPTR,    STRNG-1     / An auto-increment register (one of eight at 10-17)

  *200               / Set current assembly origin to program text area
  HELLO,  CLA CLL       / Clear AC and Link again (needed when we loop back from tls)
        TAD I Z STPTR / Get next character, indirect via PRE-auto-increment address from the zero page
        SNA          / Skip if non-zero (not end of string)
        HLT          / Else halt on zero (end of string)
        TLS          / Output the character in the AC to the teleprinter
        TSF          / Skip if teleprinter ready for character
        JMP .-1       / Else jump back and try again
        JMP HELLO     / Jump back for the next character
  STRNG,  310          / H
        345          / e
        354          / l
        354          / l
        357          / o
        254          / ,
        240          / (space)
        367          / w
        357          / o
        362          / r
        354          / l
        344          / d
        241          / !
        0           / End of string
  $HELLO              /DEFAULT TERMINATOR
```

Controversy over Computer Proof

Appel and Haken Proof (1976).

- Human part of the proof is over 1000 pages long.
- No one else has ever been able to verify it.
- Many typos were found.
- Computer portion of the proof is written in assembly language and no one else has programmed it.
- 1478 graphs had to be coded by hand.

Question: Are you convinced they have a proof?

History

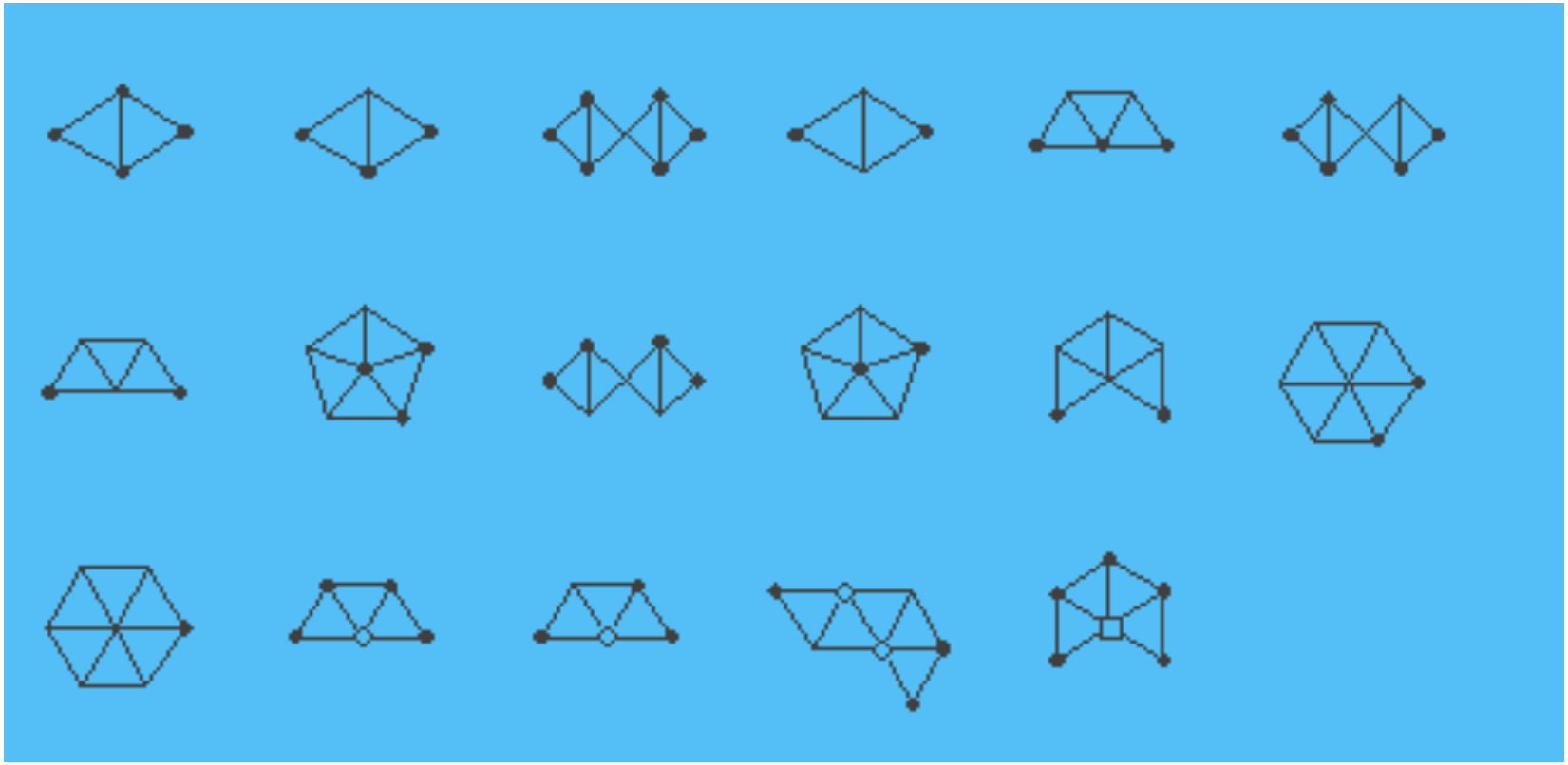
1996: “A New Proof of the Four Color Theorem”

published by Robertson, Sanders, Seymour, and Thomas based on the same outline.

- Human part of the proof is about 20 pages long.
- Computer portion of the proof was written in C.
- Several other people have independently programmed it.
- No graphs had to be input by hand.
- Only 633 configurations used.

Question: Are you convinced they have a proof?

Some of the 633 Configurations



History

1996: “A New Proof of the Four Color Theorem”

Published by Robertson, Sanders, Seymour, and Thomas based on the same outline.

- Algorithm: RSST also give an algorithm to find a 4-coloring of a planar graph that takes about n^2 seconds on a graph with n vertices.

- 2005: Georges Gonthier gave a formal proof verification of the 4CT. No human proof required!

Examples of Computer Proof

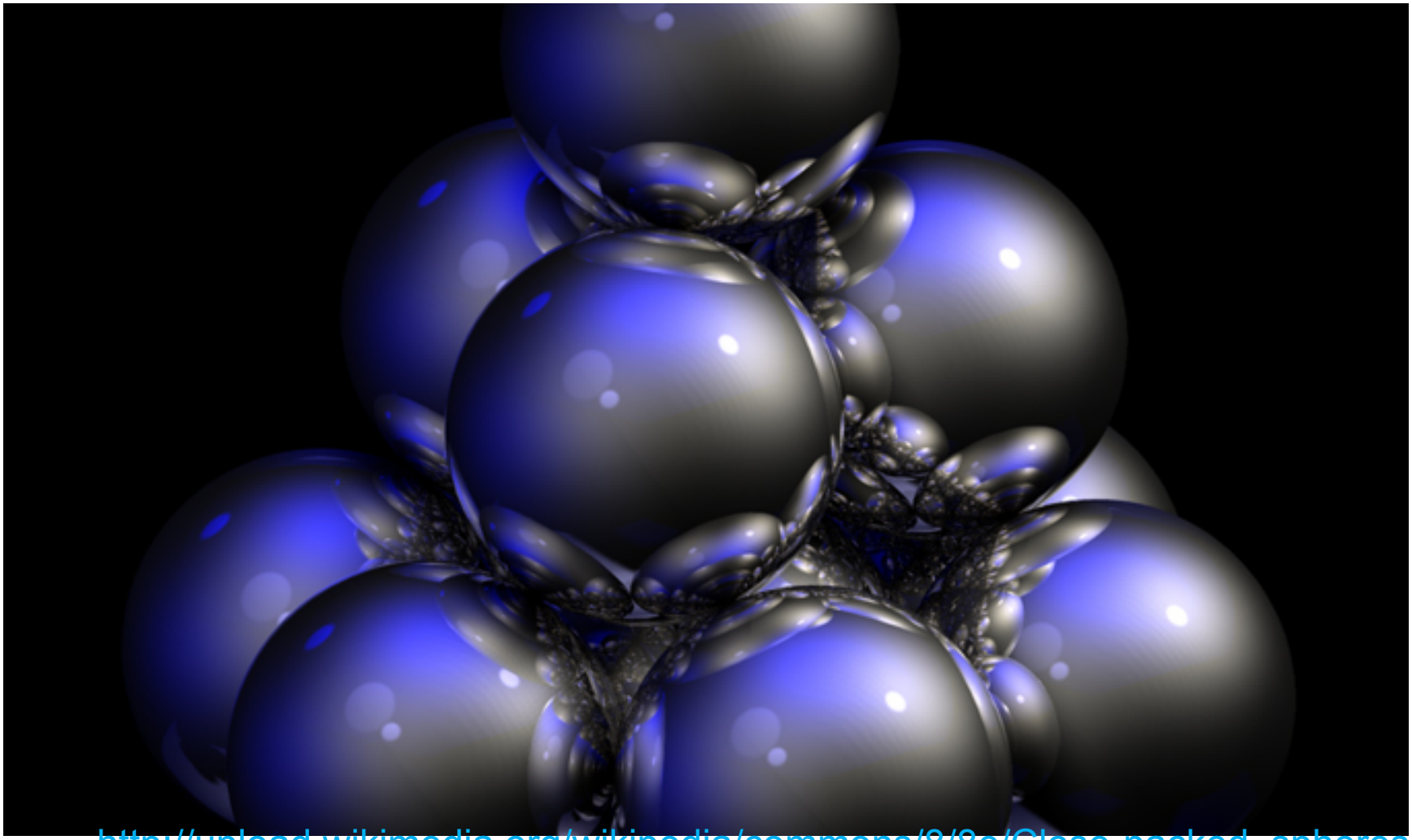
Next topic: Thomas Hales proof of Kepler's conjecture.

Harriot Investigation (ca 1600)

What is the best way to pack cannon balls in space so they are as densely packed as possible?

Thomas Harriot was the assistant to a ship captain. He corresponded with Johannes Kepler.

Hexagonal Close Packing



http://upload.wikimedia.org/wikipedia/commons/8/8e/Close-packed_spheres.jpg

Kepler's Conjecture

What is the best way to pack cannon balls in space so they are as close as possible?

Conjecture: The portion of space filled by cannonballs in the densest possible packing is given by the hexagonal close packing and has density

.

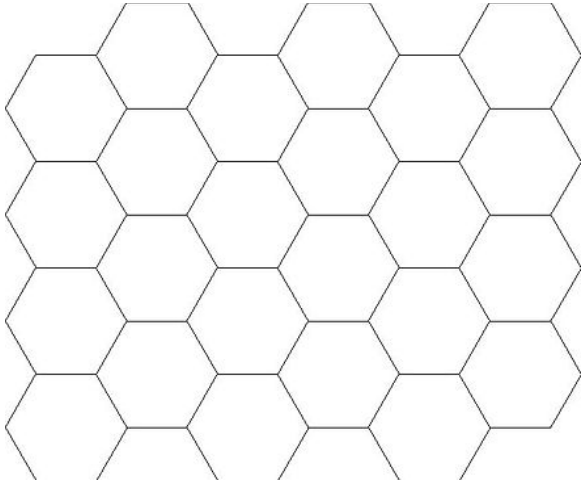
$$\frac{\pi}{\sqrt{18}} \approx 0.7404804898$$

Proof of Kepler Conjecture

- 1953: Toth showed that the problem could be reduced to a finite check of about 5000 cases.
- 1992: Thomas Hales began using linear programming to check these cases along with Samuel Ferguson.
- 1996 : Hales announced the proof was complete.
- 2005: Hales' paper was published in Annals of Math after being reviewed by a committee of 12 referees who said they were 99% certain it was correct.

Honeycomb Theorem

- **Honeycomb conjecture (Varro 36 BC)**: Any partition of the plane into equal area regions has perimeter at least that of the regular hexagonal honeycomb tiling.



- "Hexagons". Licensed under Public Domain via
- Wikimedia Commons –
- http://commons.wikimedia.org/wiki/File:Hexagons.jpg#/media/File:Hexagons.jpg

- THOMAS C. HALES, The honeycomb conjecture, Disc. Comp. Geom. 25 (2001) 1–22.

Lord Kelvin's Problem (1887)

- Unsolved Problem: How can we partition 3-dimensional space into equal volume regions with the least surface area?

Examples of Computer Proof

Zeilberger's proof of Conway's Lost Cosmological Thm:

Conway's "Look and Say" sequence:

1

11

21

1211

111221

Question: If L_n is the length of the sequence on the n^{th} step, what is L_{n+1}/L_n as n approaches infinity?

Examples of Computer Proof

Question: If L_n is the length of the sequence on the n^{th} step, what is L_{n+1}/L_n as n approaches infinity?

Answer: $L_{n+1}/L_n \rightarrow$ 1.30357726903… Conway's Constant

Somehow the proof was lost until ….

In 1997, Doron Zeilberger gave a computer assisted proof.

His proof relies on a halting problem: from each atomic word constructed so far, construct all ways of building further, until the empty set remains.

Philosophical Question

What is the value of a computer assisted proof?

- We get a new theorem which we can build on!
- We learn one more method of using computers to prove theorems.
- Every computer proof with no known human proof contains a miracle! Those miracles are important lemmas which inspire further research.

Difficult Questions

What if a computer program or hardware has a bug?

What evidence of computer verification is sufficient for a proof?

How can we ensure computer assisted proofs are “reproducible”?

Summary

Computers can be very helpful proving theorems about…

- Algebraic identities.
- Geometric density inequalities.
- Finite calculations.
- Halting problems.

And what else? Please join the conversation!

It is time to embrace computer proofs as a powerful technique and incorporate them in our math classes.

Lots more

- Origami: Can you fold this? See “Geometric Folding Algorithms” by Demaine and O’Rourke. (2007)
- Automatic Theorem Checking: Is this human proof correct? See “How to Write a Proof” by Leslie Lamport in *American Mathematical Monthly* 102, 7 (1993) . And the follow up “How to Write a 21st Century Proof” (2012).
- Game Theory: Does this game have a winning strategy? See history of Connect Four in Wikipedia.
- Computer verification of code: Amazon, Boeing …

Make every day a Mathday!

Search for Mathematical Knowledge Everywhere

Experiment with Mathematical Ideas

Create New Theorems

Dream Big: Science Fiction = Scientific Research Problems