Computer Proofs in Algebra, Combinatorics and Geometry

By Sara Billey
Professor of Mathematics
University of Washington

May 15, 2011

Outline

1. Example of human proof.
2. Example of computer proof.
3. History of first major computer proof.
4. Recent results

Definition of “Proof”

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

There exists an infinite number of prime numbers.

True or False?

Human Proof

Statement: There exists an infinite number of prime numbers.

Proof: Assume there exists only N distinct primes:

$$1<p_1 = 2 < p_2=3 < p_3 < \ldots < p_N.$$

Set $K= p_1\ p_2\ p_3 \ldots p_N + 1$.

K has a prime factorization say $K= q_1\ q_2\ q_3 \ldots q_M$

Proof: Assume there exists only N distinct primes:

$1<p_1 = 2 < p_2=3 < p_3 < \ldots< p_N$.

Set $K= p_1 \; p_2 \, p_3 \ldots p_N + 1$.

K has a prime factorization say $K= q_1 \, q_2 \, q_3 \ldots q_M$.

Subtracting

$$(*) \qquad q_1 \, q_2 \, q_3 \ldots q_M \; - \; p_1 \; p_2 \, p_3 \ldots p_N =1.$$

If $q_2 = p_j$ for some j then the left side of (*) is divisible by p_j with no remainder. But the right side of (*) is 1 so it is not divisible by $p_j >1$ with no remainder. Contradiction!

Proof: Assume there exists only N distinct primes:
$1<p_1 = 2 < p_2=3 < p_3 < \ldots < p_N$.
Set $K= p_1\ p_2\ p_3 \ldots p_N + 1$.
K has a prime factorization say $K= q_1\ q_2\ q_3 \ldots q_M$.

Subtracting

(*) $$q_1\ q_2\ q_3 \ldots q_M - p_1\ p_2\ p_3 \ldots p_N = 1.$$

If $q_1 = p_j$ for some j then the left side of (*) is divisible by p_j with no remainder. But the right side of (*) is 1 so it is not divisible by $p_j >1$ with no remainder. Contradiction!

Beautiful Proof !

Theorem: There exists an infinite number of prime numbers.

Proof: Assume there exists only N distinct primes:

$$1<p_1 = 2 < p_2=3 < p_3 < \ldots < p_N.$$

Set $K= p_1\ p_2\ p_3 \ldots p_N + 1$.

K has a prime factorization say $K= q_1\ q_2\ q_3 \ldots q_M$

Subtracting

$$(*) \qquad q_1\ q_2\ q_3 \ldots q_M\ -\ p_1\ p_2\ p_3 \ldots p_N = 1.$$

If $q_1 = p_j$ for some j then the left side of (*) is divisible by p_j with no remainder. But the right side of (*) is 1 so it is not divisible by $p_j > 1$ with no remainder. Contradiction!

Q.E.D.

Example of Computer Proof

Use symbolic algebra package like Maple or Mathematica.

Directions: Color the map below with as few colors as possible without choosing the same color for two adjacent states. Use letters like G for green or Y for yellow if you don't have colored pencils.

United States of America

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. "**

- True or False?

- Caveats: No two states touch at isolated points. Each state is connected.

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.** "

History:

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

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 and disproofs apear and get rejected. But much progress was made along the way.

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 and disproofs apear 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.

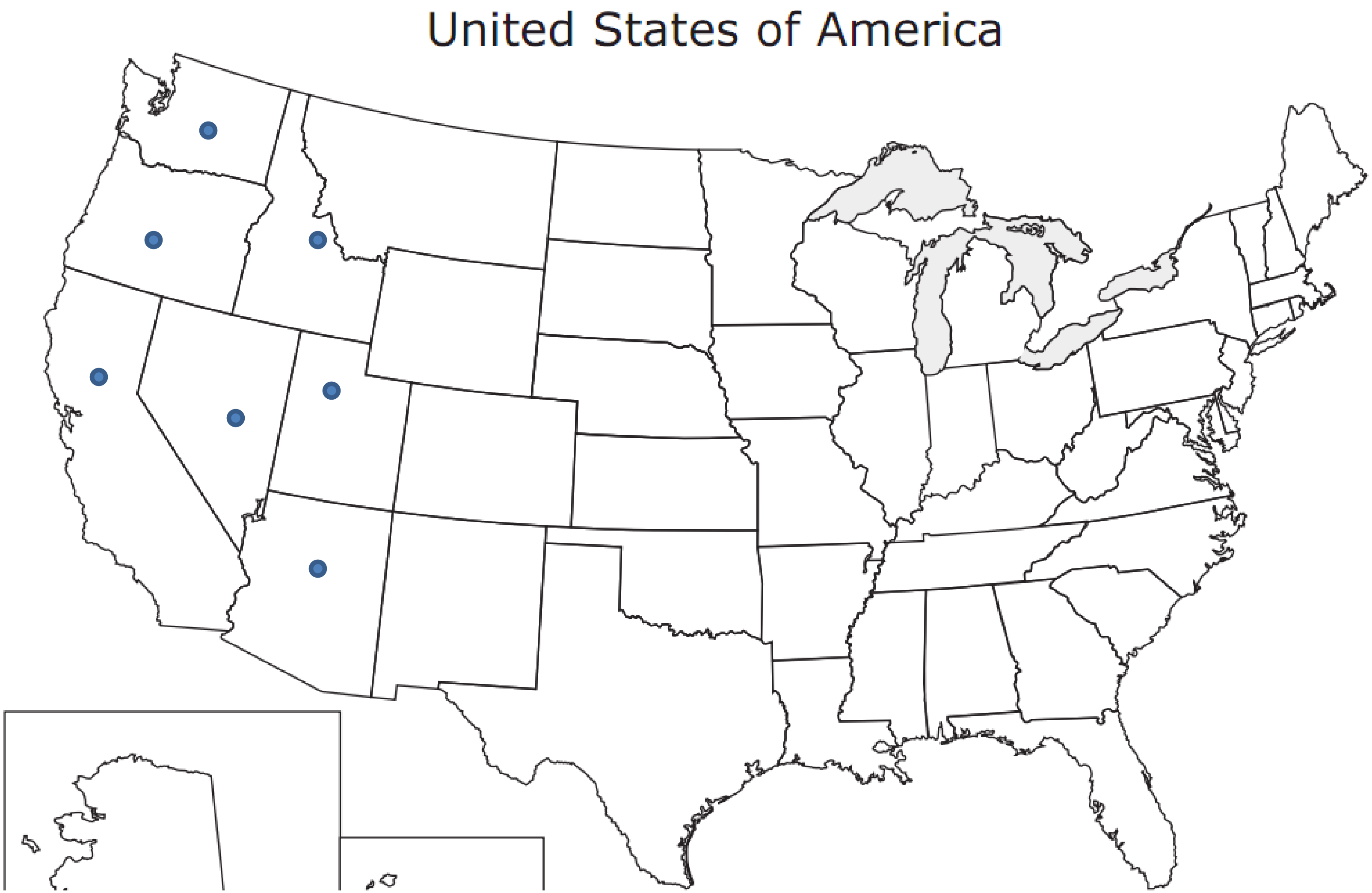
Reformulation

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

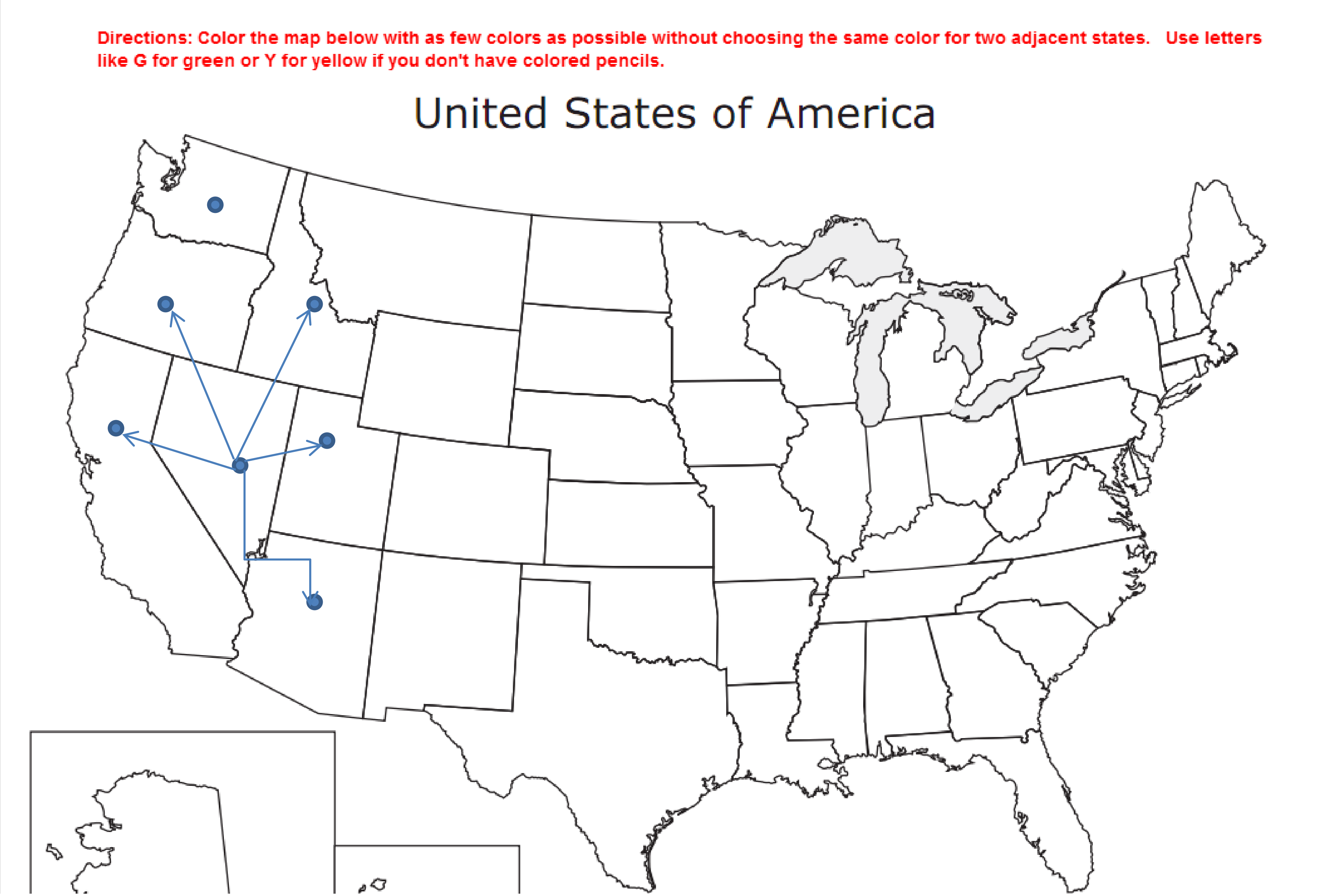
- Replace each state with a bold dot = vertex.
- Connect the dots representing two states if and only if they are adjacent on the map by path on the paper = edge.

Place a bold dot in each state.   Each dot is called a vertex of the graph.

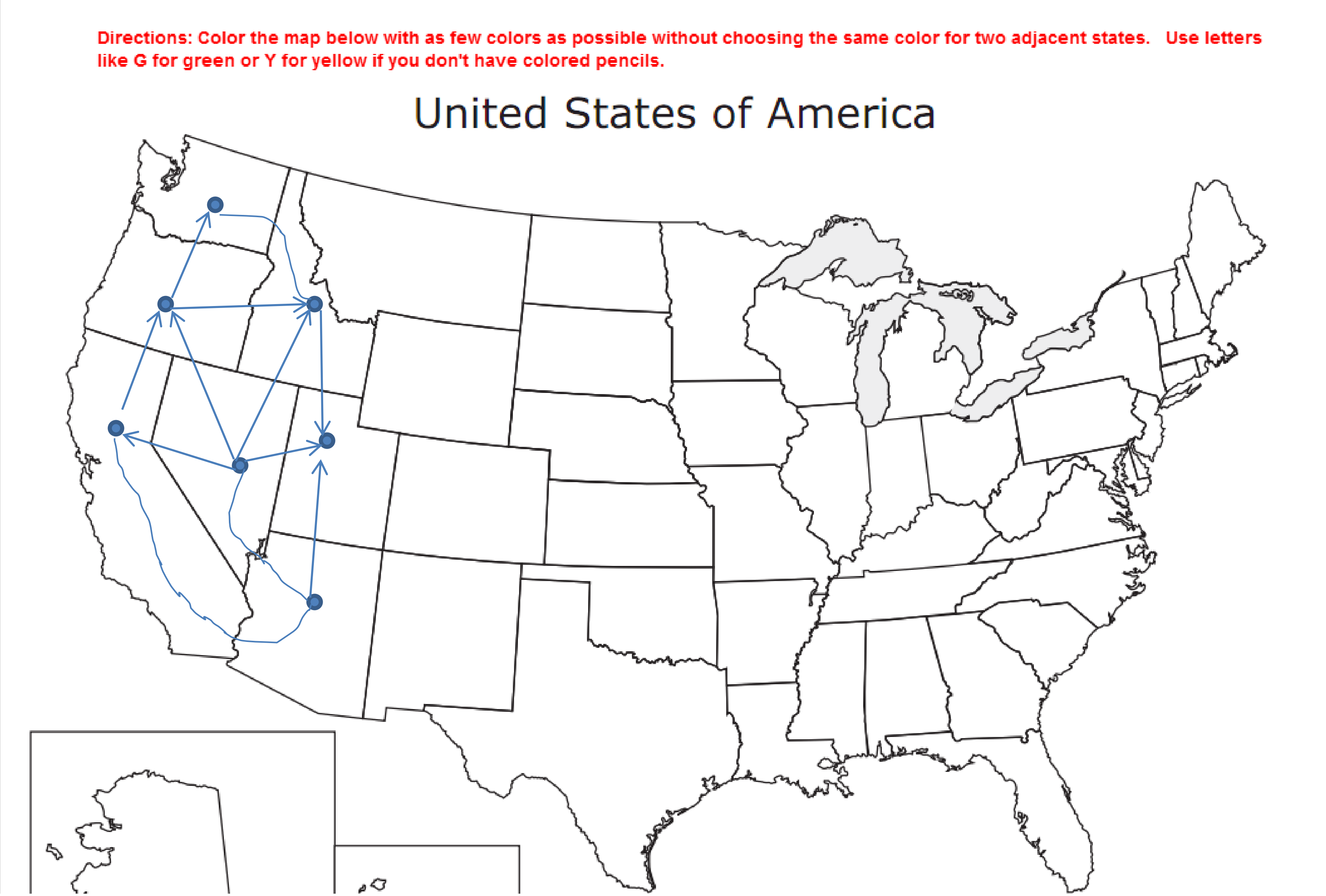
Directions: Color the map below with as few colors as possible without choosing the same color for two adjacent states.   Use letters like G for green or Y for yellow if you don't have colored pencils.



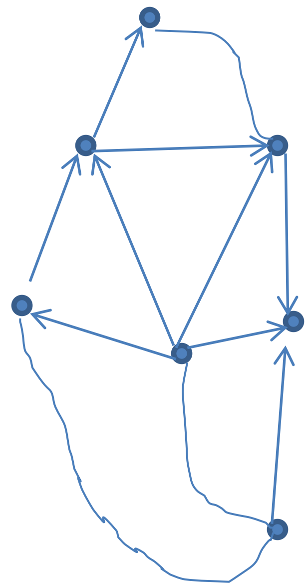
Draw a path between every pair vertices representing adjacent states which Only passes through those two states. Each path is called an edge of the graph.



Draw a path between every pair vertices representing adjacent states which Only passes through those two states. Each path is called 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.

Question: Can every map of states be represented by a planar graph?

Question: Is every graph planar?

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."

Controvercy over Computer Proof

- Imagine back to 1976… ..

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 and 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?

Good ideas in the Appel-Haken Proof

Outline of Proof:

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

- Reducibility (human only).
- Unavoidability (computer assisted).
- Algorithm for finding a coloring in G

Good ideas in the Appel-Haken Proof

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

- Reducibility: AH give a finite list of 1478 configurations in graphs. Each one of these cannot appear in G because if it did, they gave rules to replace G by a smaller graph that would still be planar and require more than 4 colors.

Good ideas in the Appel-Haken Proof

- Unavoidability: Every minimal counterexample to the 4CT must contain one of the configurations on the list.

A configuration is a small neighborhood in a graph. AH prove they only need to look at the second neighbors of each vertex and they bound the number of neighbors in each configuration. There are only a finite number of such graphs.

Good ideas in the Appel-Haken Proof

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

- Reducibility: AH give a finite list of 1478 configurations in graphs which cannot appear in G.
- Unavoidability: G must contain one of the configurations on the list.

Question: What can you conclude about G?

Good ideas in the Appel-Haken Proof

- Reducibility (human only).
- Unavoidability (computer assisted).

Together imply there always exists a 4 coloring of any planar graph. But how do we find one?

- Algorithm for finding a 4-coloring in G. Guaranteed to succeed if a 4-coloring exists.

History

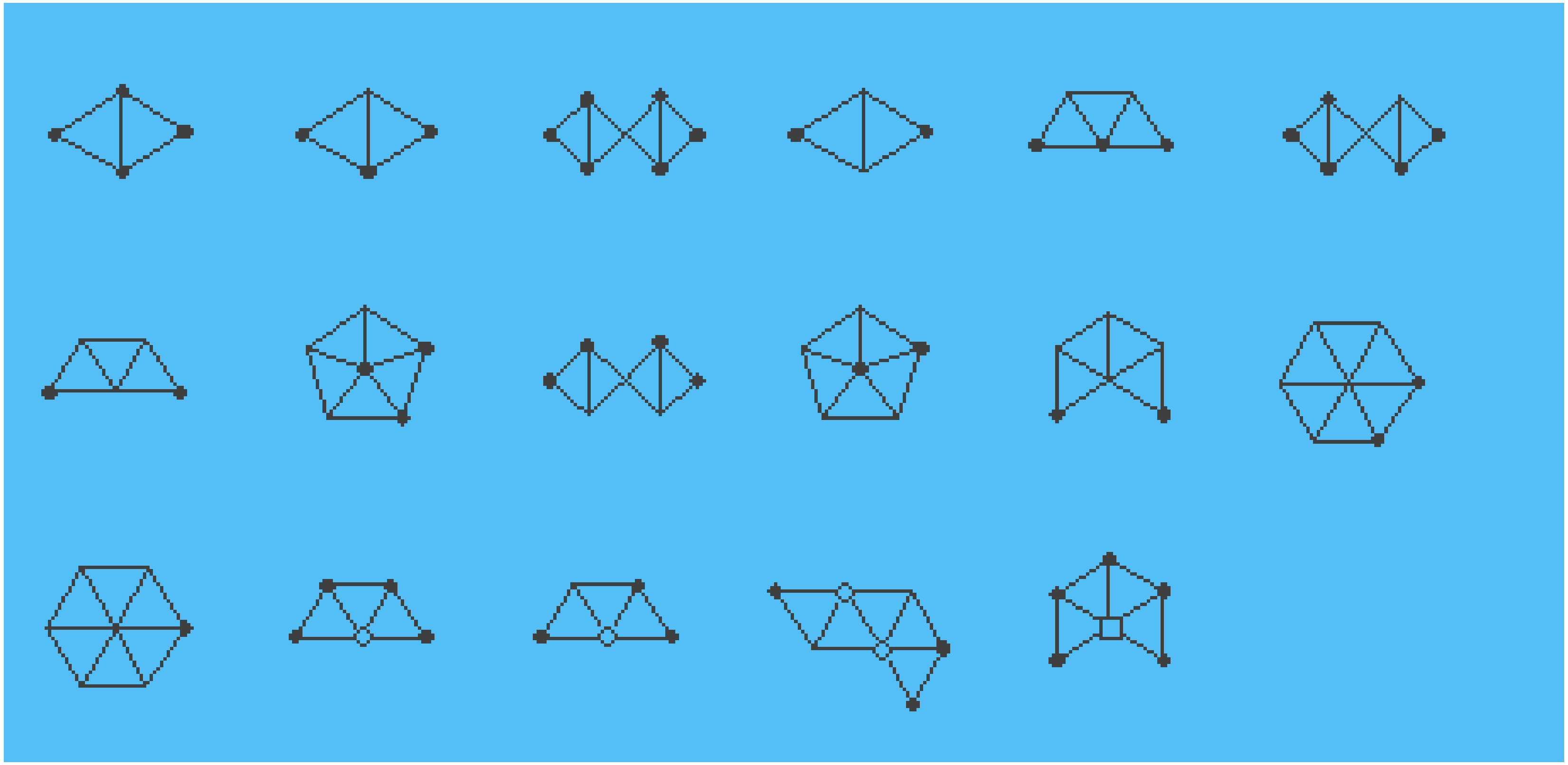
1996: “A New Proof of the Four Color Theorem”

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

- Human part of the proof is about 20 pages.
- Computer portion of the proof was originally written in C and several other people have independently programmed it.
- No graphs had to be coded 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.

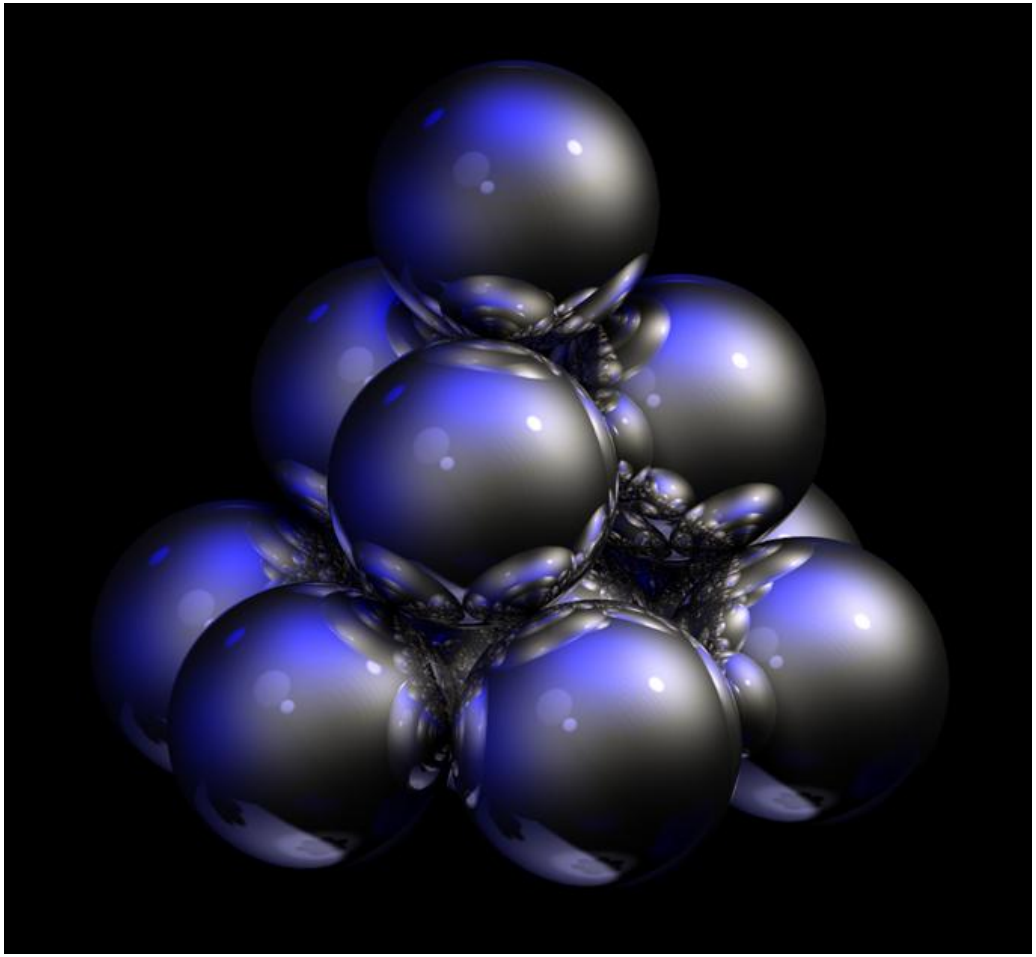
- Algorithm: RSST also give an algorithm to find a 4-coloring of a planar graph that takes about n^2 seconds on a graph with n vertices.

Kepler's Conjecture

Astronomers were wondering:

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

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

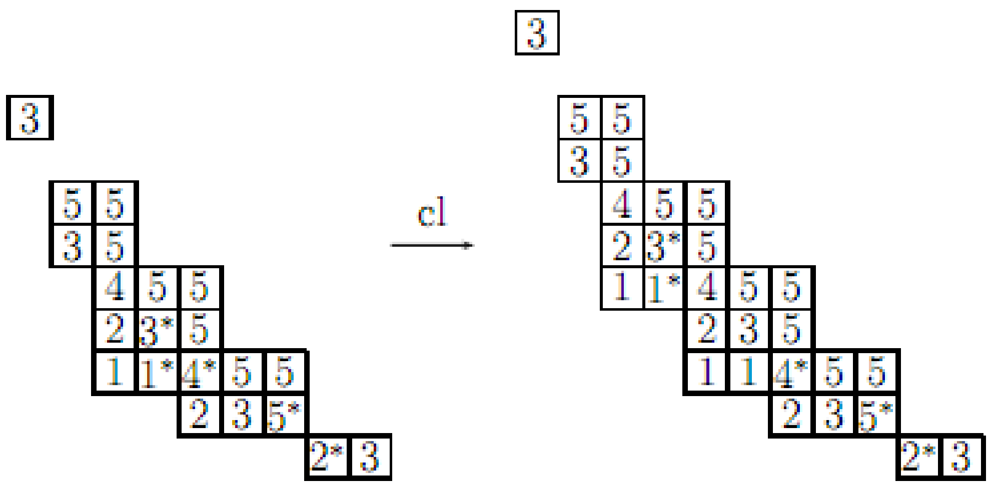
$$\frac{\pi}{\sqrt{18}} \approx 0.7404804898.$$

History of Hales Proof

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

A halting problem

Problem: Find all graph types corresponding with rank 5 starred strong tableaux under cloning.



Human part of the proof is 50 pages long. It is ready to publish.
Computer part has been running since January, but hasn't finished.

Questions: When should we submit it for publication?
Do you think it will be controversial?

Philosophical Question

What is the value of a computer proof?

- We get a new result which we can build on!
- We learn one more method of using computers to prove theorem.
- Every computer proof with no human proof contains a miracle which makes it computable!

Summary

Computers can be very helpful proving theorems about…

- Algebraic identities.
- Finite calculations.
- Halting problems

And what else?

Lots more

- Origami: Can you fold this? See "Geometric Folding Algorithms" by Demaine and O'Rourke.

- Automatic Theorem Checking: Is this human proof correct? See "How to Write a Proof" by Leslie Lamport in *American Mathematical Monthly* 102, 7 (August-September 1993) 600-608.

- Game Theory: Does this game have a winning strategy? See history of Connect Four in Wikipedia.