15-355

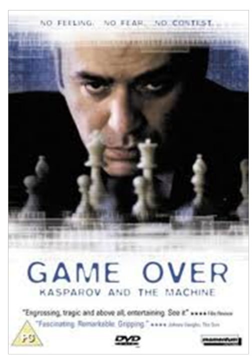
Modern Computer Algebra

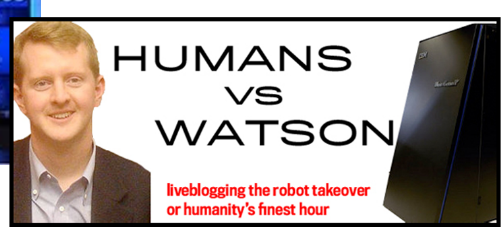
Victor Adamchik

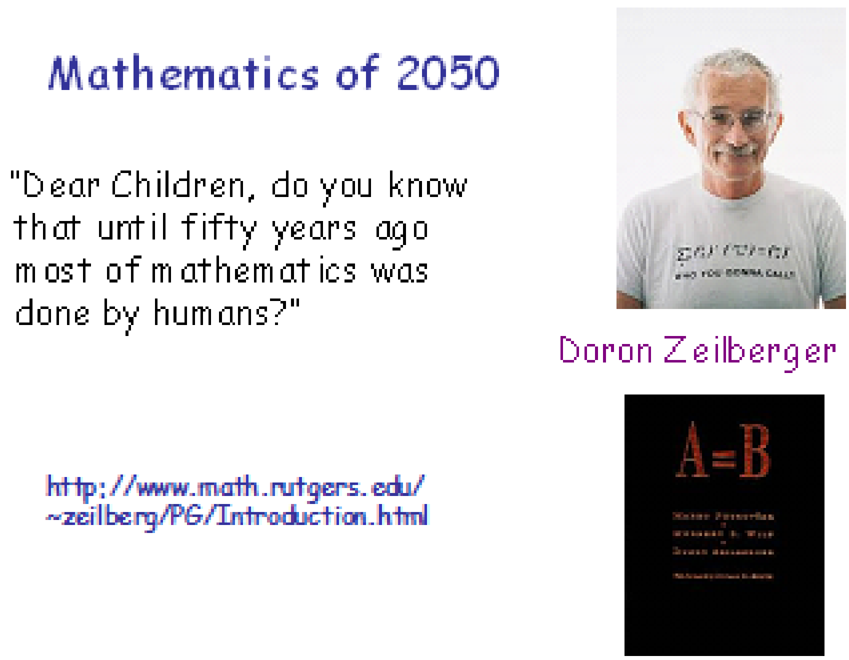
Carnegie Mellon University

Computer Assisted Proofs

In 1993 John Horgan, a writer for *Scientific American,* published an article called *The Death of Proof?* In this piece the author claimed that mathematical proof no longer had a valid role in modern thinking. Horgan's reasoning is that computers can do much more effectively what human beings have done traditionally - which is to *think*.







Computer assisted proofs are revolutionary mathematics!

Hales proof of the Kepler conjecture...

The latest proof of the 4 Color Theorem

Proof assistant languages such as Coq, Isabelle have successfully verified a number of important mathematical results..

Introduction to the course

What is algebra?

The goal of algebra is to find explicit solutions to algebraic problems. We are interested in *computational* solutions. Algebra has a strong influence on our thinking about algorithms. Thus, in this course we will investigate the relationship between computation and algebra.

Combinatorial Identities

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$$

$$\sum_{k=0}^{n} 2^k = 2^{n+1} - 1$$

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$$

$$\sum_{k=1}^{n} \frac{(-1)^k}{F_k F_{k+1}} = -\frac{F_n}{F_{n+1}}$$

$$\sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{\pi}{2}$$

The summation problem consists in finding and/or proving such identities.

$$\sum_{k=0}^{n} \frac{(-1)^k}{1+k} \binom{n}{k} = ?$$

Algebra assumes a greater amount of structure...

■ Gröbner Bases

Linear Equations: find x and y such that

$$\begin{cases} a x + b y = r \\ c x + d y = q \end{cases}$$

This problem is generalized in many ways...

Polynomial Equations: find x, y and z such that

$$\begin{cases} x^2 + y^2 + z^2 - 1 = 0 \\ x^2 + y^2 + z^2 - 2x = 0 \\ x - y + 2z = 0 \end{cases}$$

This leads to several the most fundamental problems in algebra: factorization, Gröbner bases, quantifier elimination.

Heron' s Formula. *Given a triangle. If s_1,s_2,s_3 are lengths of the sides and s is a half-perimeter $s = \frac{1}{2}(s_1 + s_2 + s_3)$ then Heron's formula states that the area is*

$$\Delta = \sqrt{s (s - s_1)(s - s_2)(s - s_3)}$$

Computational proof. Pick any three points in the plane

$$p_1 = \{x_1, y_1\}$$

$$p_2 = \{x_2, y_2\}$$
$$p_3 = \{x_3, y_3\}$$

Without loss of the generality, we assume that

$$x_1 = 0;\ y_1 = 0,\ \ y_2 = 0.$$

They form a triangle with the sides, the lengths of which can be expressed as

$$s_1 = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$$
$$s_2 = \sqrt{(x_1 - x_3)^2 + (y_1 - y_3)^2}$$
$$s_3 = \sqrt{(x_3 - x_2)^2 + (y_3 - y_2)^2}$$

The area is

$$A = \frac{1}{2} \left| \begin{array}{ccc} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{array} \right|$$

Now we put all these equations together to get a system of four polynomial equations.

$$s_1^2 = x_2^2$$
$$s_2^2 = x_3^2 + y_3^2$$
$$s_3^2 = (x_3 - x_2)^2 + y_3^2$$
$$2\,A = x_2\, y_3$$

Next, we use *Mathematica*'s GroebnerBasis

```
x₁ = 0; y₁ = 0; y₂ = 0;
GroebnerBasis[{
  s₁² - (x₁ - x₂)² - (y₁ - y₂)²,
  s₂² - (x₁ - x₃)² - (y₁ - y₃)²,
  s₃² - (x₃ - x₂)² - (y₃ - y₂)²,
  A - 1/2 Det[{{x₁, y₁, 1}, {x₂, y₂, 1}, {x₃, y₃, 1}}]},
 {A, s₁, s₂, s₃},   (* variables to keep *)
 {x₂, x₃, y₃},      (* variables to eliminate *)
 MonomialOrder → EliminationOrder]
```

$$\{16\,A^2 + s_1^4 - 2\,s_1^2\,s_2^2 + s_2^4 - 2\,s_1^2\,s_3^2 - 2\,s_2^2\,s_3^2 + s_3^4\}$$

Solving it in A yields the Heron formula:

$$16\,A^2+s_1^4+s_2^4+s_3^4-2\,s_1^2\,s_2^2\;-2\,s_1^2\,s_3^2\;-2\,s_2^2\,s_3^2=0$$

Complexity.

Given a system of m quadratic polynomials with n variables. Does it have a solution?

This is a NP-hard problem.

Hilbert Nullstellensatz problem: given a system of m polynomials in n variables over $\mathbb{C}$. Decide whether the system has a common zero.

Hilbert Nullstellensatz is a NP-complete problem.

Several algebraic models were proposed to study $P == NP$ problems. Leonare Blum and Steve Smale model...

■ Integration

What does it mean that a given function is integrable?

$$\int e^x\,dx=e^x$$

$$\int e^{-x^2}\,dx=\frac{\sqrt{\pi}}{2}\;\mathrm{erf}(x)$$

Clearly, e^{-x^2} is NOT integrable in terms of elementary functions, but integrable in terms of some special functions.

$$\int\frac{dx}{\sqrt{1-x^2}}=\sin^{-1}(x)$$

$$\int\frac{dx}{\sqrt{1-x^3}}=\text{Elliptic function}$$

$$\int\frac{1}{\sqrt{1+x+x^5}}\,dx=?$$