¿Pueden los ordenadores ayudarnos en la demostración de teoremas?

Jónathan Heras

School of Computing, University of Dundee, UK
http://www.computing.dundee.ac.uk/staff/jheras/

Curso de Actualización en Matemáticas
20 de marzo de 2013

Índice

1. Motivación
2. Demostración automatizada
3. Demostración asistida por ordenador

Índice

1 Motivación

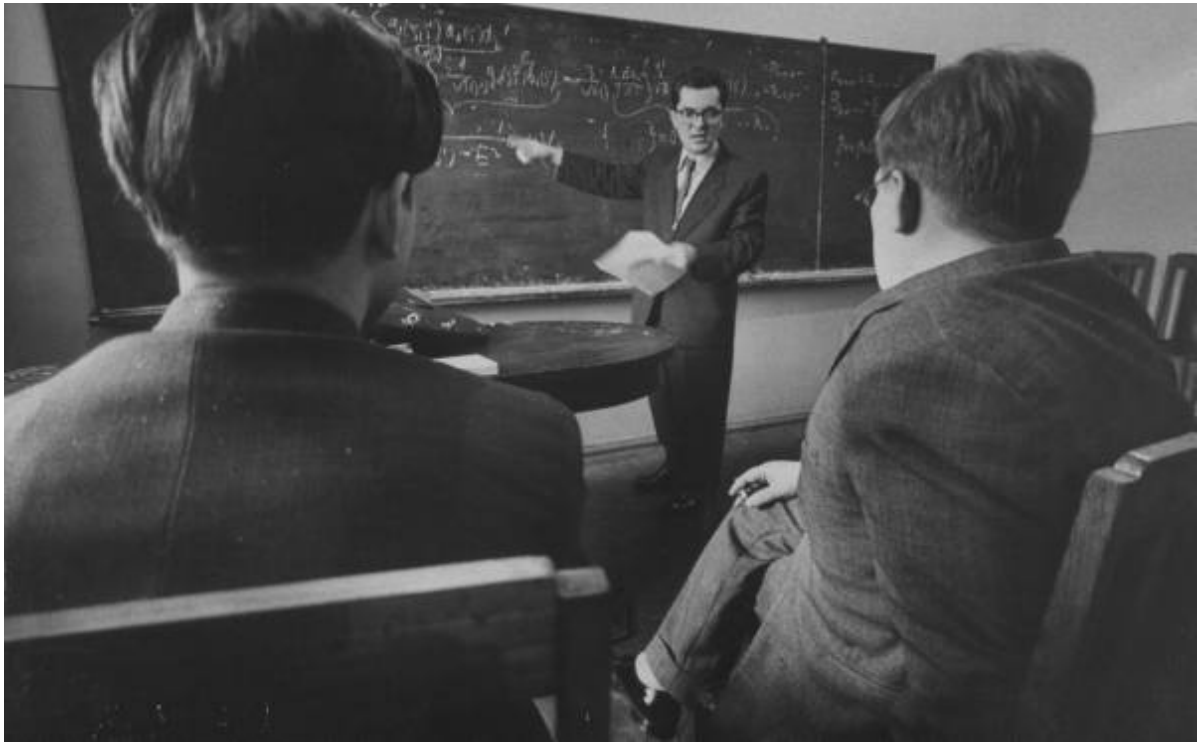
2 Demostración automatizada

3 Demostración asistida por ordenador

La ubicuidad de los ordenadores en Matemáticas

La ubicuidad de los ordenadores en Matemáticas

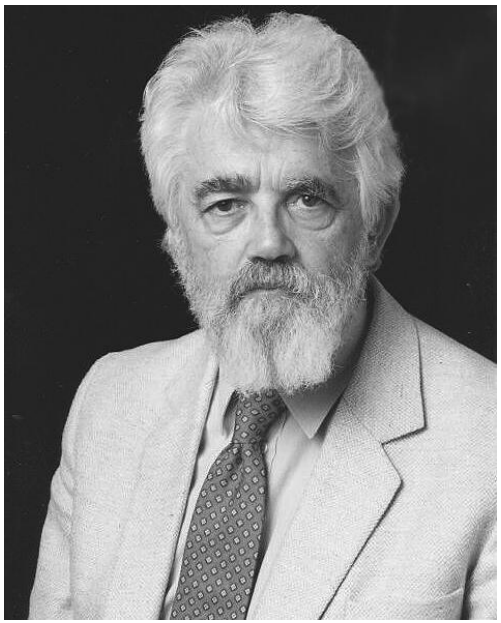
pero . . . ¿nos pueden ayudar a demostrar teoremas?



Del sueño de Leibniz (1646–1716) . . .

Leibniz soñaba con diseñar una “lingua characteristica” (un lenguaje en el que todo el conocimiento pudiera ser expresado formalmente) y un “calculus ratiocinator” (cálculo del razonamiento) tal que cuando los filósofos discreparan pudieran decir “calculemus”, formulando el problema en la lingua characteristica y resolverlo usando el calculus ratiocinator.

. . . al de McCarthy (1927–2011)



"Proof-checking by computer may be as important as proof generation. It is part of the definition of formal system that proofs be machine checkable.

. . .

For example, instead of trying out computer programs on test cases until they are debugged, one should prove that they have the desired properties."[John McCarthy]

¿Por qué?

- Incrementar la fiabilidad de los resultados matemáticos:
  - A. B. Kempe, On the geographical problem of four-colors;
  - A. Wiles, Modular elliptic curves and Fermat's Last Theorem;
  - E. Gallardo & C. Cowen, Rota's Universal Operators and Invariant Subspaces in Hilbert Spaces;
  - R. Mikhailov & J. Wu, On homotopy groups of the suspended classifying spaces;
  - M. Lecat, Erreurs de Mathématiciens des origines à nos jours.

¿Por qué?

- Incrementar la fiabilidad de los resultados matemáticos:
  - A. B. Kempe, On the geographical problem of four-colors;
  - A. Wiles, Modular elliptic curves and Fermat's Last Theorem;
  - E. Gallardo & C. Cowen, Rota's Universal Operators and Invariant Subspaces in Hilbert Spaces;
  - R. Mikhailov & J. Wu, On homotopy groups of the suspended classifying spaces;
  - M. Lecat, Erreurs de Mathématiciens des origines à nos jours.
- Corrección de demostraciones que usan ordenadores para realizar cálculos:
  - K. Appel & W. Haken, Every map is four colourable;
  - T. C. Hales, A proof of the Kepler conjecture;
  - A. Romero & J. Rubio, Homotopy groups of suspended classifying spaces: an experimental approach.

¿Por qué?

- Incrementar la fiabilidad de los resultados matemáticos:
  - A. B. Kempe, On the geographical problem of four-colors;
  - A. Wiles, Modular elliptic curves and Fermat's Last Theorem;
  - E. Gallardo & C. Cowen, Rota's Universal Operators and Invariant Subspaces in Hilbert Spaces;
  - R. Mikhailov & J. Wu, On homotopy groups of the suspended classifying spaces;
  - M. Lecat, Erreurs de Mathématiciens des origines à nos jours.
- Corrección de demostraciones que usan ordenadores para realizar cálculos:
  - K. Appel & W. Haken, Every map is four colourable;
  - T. C. Hales, A proof of the Kepler conjecture;
  - A. Romero & J. Rubio, Homotopy groups of suspended classifying spaces: an experimental approach.
- Problema con el tamaño y complejidad de ciertas demostraciones:
  - A. Wiles, Modular elliptic curves and Fermat's Last Theorem (98 pags);
  - N. Robertson & P. Seymour, Graph Minors ($\sim$ 500 pags, 1983–2004);
  - Clasificación de grupos simples ($\sim$ 500 artículos, $\sim$ 100 autores).

Haciendo matemáticas en el ordenador

- Cálculo:
- Demostración:

Haciendo matemáticas en el ordenador

- Cálculo:
  - numérico: grandes cálculos, visualización, simulación, ...
  - simbólico: manipulación de fórmulas.
- Demostración:

Haciendo matemáticas en el ordenador

- Cálculo:
  - numérico: grandes cálculos, visualización, simulación, ...
  - simbólico: manipulación de fórmulas.
- Demostración:
  - automátizada;
  - asistida.

Haciendo matemáticas en el ordenador

- Cálculo:
  - numérico: grandes cálculos, visualización, simulación, ...
  - simbólico: manipulación de fórmulas.
- Demostración:
  - automátizada;
  - asistida.

Índice

1 Motivación

2 Demostración automatizada

3 Demostración asistida por ordenador

Demostración automatizada de teoremas

"In ten years, a computer would discover and prove an important new mathematical theorem."[Herbert A. Simon,1957]

Demostración automatizada de teoremas

"In ten years, a computer would discover and prove an important new mathematical theorem."[Herbert A. Simon,1957]

Demostración automatizada de teoremas

"In ten years, a computer would discover and prove an important new mathematical theorem."[Herbert A. Simon,1957]

En los sistemas de demostración automatizada se suministra como dato de entrada el enunciado de un teorema y ellos son capaces de encontrar automáticamente una demostración del mismo.

Demostración automatizada de teoremas

"In ten years, a computer would discover and prove an important new mathematical theorem."[Herbert A. Simon,1957]

En los sistemas de demostración automatizada se suministra como dato de entrada el enunciado de un teorema y ellos son capaces de encontrar automáticamente una demostración del mismo.

- SAT solvers,
- SMT solvers,
- Demostradores de teoremas basados en el principio de resolución.

SAT solvers

Problema

Dada una expresión booleana con variables y sin cuantificadores (e.g. $(x_1 \vee \neg x_2 \vee x_3) \wedge (\neg x_2 \vee \neg x_3 \vee x_4)$), determinar si tiene asociada una asignación de valores para sus variables que hace que la expresión sea verdadera.

SAT solvers

Problema

Dada una expresión booleana con variables y sin cuantificadores (e.g. $(x_1 \vee \neg x_2 \vee x_3) \wedge (\neg x_2 \vee \neg x_3 \vee x_4)$), determinar si tiene asociada una asignación de valores para sus variables que hace que la expresión sea verdadera.

SAT solvers:

- Diferentes sistemas: glucose, glueminisat, 3S, plingeling, ...
- Aplicaciones: criptoanálisis, verificación de modelos, planificación, teoría de códigos, scheduling, ...
- Fue el primer problema NP-completo conocido.

SMT solvers

Un SMT (satisfiability modulo theory) solver es una herramienta que decide la satisfabilidad de una fórmula en una teoría de primer orden.

SMT solvers

Un SMT (satisfiability modulo theory) solver es una herramienta que decide la satisfabilidad de una fórmula en una teoría de primer orden.

- Teorías de primer orden: teoría de los enteros, de los racionales, de vectores, ...
- Generalización de SAT solvers.
- Una fórmula SMT puede verse como una fórmula SAT donde las variables se reemplazan por formulas en las teorías de primer orden (e.g. $x + y \leq 0 \wedge (x = z \implies z + y = -1) \wedge z > 3t$).

SMT solvers

Un SMT (satisfiability modulo theory) solver es una herramienta que decide la satisfabilidad de una fórmula en una teoría de primer orden.

- Teorías de primer orden: teoría de los enteros, de los racionales, de vectores, ...
- Generalización de SAT solvers.
- Una fórmula SMT puede verse como una fórmula SAT donde las variables se reemplazan por formulas en las teorías de primer orden (e.g. $x + y \leq 0 \wedge (x = z \implies z + y = -1) \wedge z > 3t$).
- Diferentes sistemas: Simplify, Alt-Ergo, Yices, Z3, CVC3, ...
- Aplicaciones: verificación de programas, planificación, scheduling, generación de casos de prueba, ...

Resolution Theorem Provers

Demostradores de teoremas basados en el principio de resolución:

- se niega el enunciado que se quiere probar y se añade a una lista de axiomas que se conoce como cierta;
- se usa el principio de resolución para llegar a una contradicción; y
- como el enunciado negado es inconsistente con los axiomas dados, se tiene que el enunciado original debe ser consistente.

Resolution Theorem Provers

Demostradores de teoremas basados en el principio de resolución:

- se niega el enunciado que se quiere probar y se añade a una lista de axiomas que se conoce como cierta;
- se usa el principio de resolución para llegar a una contradicción; y
- como el enunciado negado es inconsistente con los axiomas dados, se tiene que el enunciado original debe ser consistente.

Sistemas más exitosos en el campo de razonamiento automatizado:

- La librería TPTP (Thousands of Problems for Theorem Provers): problemas de álgebra, topología, análisis, ...
- Distintos sistemas: EQP, Prover9, E, SPASS, Vampire, ...

Resolution Theorem Provers

Demostradores de teoremas basados en el principio de resolución:

- se niega el enunciado que se quiere probar y se añade a una lista de axiomas que se conoce como cierta;
- se usa el principio de resolución para llegar a una contradicción; y
- como el enunciado negado es inconsistente con los axiomas dados, se tiene que el enunciado original debe ser consistente.

Sistemas más exitosos en el campo de razonamiento automatizado:

- La librería TPTP (Thousands of Problems for Theorem Provers): problemas de álgebra, topología, análisis, ...
- Distintos sistemas: EQP, Prover9, E, SPASS, Vampire, ...

Teorema (Demo en Prover9)

Sea G un grupo, y e su elemento neutro. Si, para todo x de G, $x^2 = e$, entonces G es conmutativo.

El mayor éxito: la conjetura de Robbins

Definición

Un álgebra booleana es un conjunto junto con:

- *una operación binaria $+$, que es asociativa y conmutativa; y*
- *una operación unaria n, tal que $n(nx + y) + n(nx + ny) = x$.*

Definición

Un álgebra de Robbin es un conjunto junto con:

- *una operación binaria $+$, que es asociativa y conmutativa; y*
- *una operación unaria n, tal que $n(n(x + y) + n(x + ny)) = x$.*

El mayor éxito: la conjetura de Robbins

Definición

Un álgebra booleana es un conjunto junto con:

- *una operación binaria $+$, que es asociativa y conmutativa; y*
- *una operación unaria n, tal que $n(nx + y) + n(nx + ny) = x$.*

Definición

Un álgebra de Robbin es un conjunto junto con:

- *una operación binaria $+$, que es asociativa y conmutativa; y*
- *una operación unaria n, tal que $n(n(x + y) + n(x + ny)) = x$.*

Teorema

Las álgebras de Robbins son álgebras booleanas.

El mayor éxito: la conjetura de Robbins

Definición

Un álgebra booleana es un conjunto junto con:

- *una operación binaria $+$, que es asociativa y conmutativa; y*
- *una operación unaria n, tal que $n(nx + y) + n(nx + ny) = x$.*

Definición

Un álgebra de Robbin es un conjunto junto con:

- *una operación binaria $+$, que es asociativa y conmutativa; y*
- *una operación unaria n, tal que $n(n(x + y) + n(x + ny)) = x$.*

Teorema

Las álgebras de Robbins son álgebras booleanas.

S. Winker demostró que es suficiente que en un álgebra de Robbins existan elementos c y d tales que $c + d = c$ para que sea un álgebra booleana.

La conjetura de Robbins

- conjetura estuvo abierta por más de 60 años,
- demostrada finalmente por el demostrador EQP,
- 8 días de cálculo y 30 megabytes de memoria.

La conjetura de Robbins

- conjetura estuvo abierta por más de 60 años,
- demostrada finalmente por el demostrador EQP,
- 8 días de cálculo y 30 megabytes de memoria.

7	$n(n(n(x)+y)+n(x+y))=y$	[Robbins equation]
10	$n(n(n(x+y)+n(x)+y)+y)=n(x+y)$	$[7 \to 7]$
11	$n(n(n(n(x)+y)+x+y)+y)=n(n(x)+y)$	$[7 \to 7]$
29	$n(n(n(n(x)+y)+x+2y)+n(n(x)+y))=y$	$[11 \to 7]$
54	$n(n(n(n(n(x)+y)+x+2y)+n(n(x)+y)+z)+n(y+z))=z$	$[29 \to 7]$
217	$n(n(n(n(n(x)+y)+x+2y)+n(n(x)+y)+n(y+z)+z)+z)=n(y+z)$	$[54 \to 7]$
674	$n(n(n(n(n(n(x)+y)+x+2y)+n(n(x)+y)+n(y+z)+z)+z+u)+n(n(y+z)+u))=u$	$[217 \to 7]$
6736	$n(n(n(n(3x)+x)+n(3x))+n(n(n(3x)+x)+5x))=n(n(3x)+x)$	$[10 \to 674]$
8855	$n(n(n(3x)+x)+5x)=n(3x)$	$[6736 \to 7,\text{simp:}54,\text{flip}]$
8865	$n(n(n(n(3x)+x)+n(3x)+2x)+n(3x))=n(n(3x)+x)+2x$	$[8855 \to 7]$
8866	$(n(n(3x)+x)+n(3x))=x$	$[8855 \to 7,\text{simp:}11]$
8870	$n(n(n(n(3x)+x)+n(3x)+y)+n(x+y))=y$	$[8866 \to 7]$
8871	$n(n(3x)+x)+2x=2x$	$[8865,\text{simp:}8870,\text{flip}]$

La conjetura de Robbins

- conjetura estuvo abierta por más de 60 años,
- demostrada finalmente por el demostrador EQP,
- 8 días de cálculo y 30 megabytes de memoria.

7	$n(n(n(x)+y)+n(x+y))=y$	[Robbins equation]
10	$n(n(n(x+y)+n(x)+y)+y)=n(x+y)$	$[7 \to 7]$
11	$n(n(n(n(x)+y)+x+y)+y)=n(n(x)+y)$	$[7 \to 7]$
29	$n(n(n(n(x)+y)+x+2y)+n(n(x)+y))=y$	$[11 \to 7]$
54	$n(n(n(n(n(x)+y)+x+2y)+n(n(x)+y)+z)+n(y+z))=z$	$[29 \to 7]$
217	$n(n(n(n(n(x)+y)+x+2y)+n(n(x)+y)+n(y+z)+z)+z)=n(y+z)$	$[54 \to 7]$
674	$n(n(n(n(n(n(x)+y)+x+2y)+n(n(x)+y)+n(y+z)+z)+z+u)+n(n(y+z)+u))=u$	$[217 \to 7]$
6736	$n(n(n(n(3x)+x)+n(3x))+n(n(n(3x)+x)+5x))=n(n(3x)+x)$	$[10 \to 674]$
8855	$n(n(n(3x)+x)+5x)=n(3x)$	$[6736 \to 7,\text{simp:}54,\text{flip}]$
8865	$n(n(n(n(3x)+x)+n(3x)+2x)+n(3x))=n(n(3x)+x)+2x$	$[8855 \to 7]$
8866	$(n(n(3x)+x)+n(3x))=x$	$[8855 \to 7,\text{simp:}11]$
8870	$n(n(n(n(3x)+x)+n(3x)+y)+n(x+y))=y$	$[8866 \to 7]$
8871	$n(n(3x)+x)+2x=2x$	$[8865,\text{simp:}8870,\text{flip}]$

Problema de decisión en un sistema álgebraico abstracto – hecho casi a medida para la búsqueda por ordenador.

Otros ejemplos

Algoritmos adhoc para resolver clases de problemas:

- el algoritmo WZ da pruebas automatizadas de sumas hipergeométricas,
- métodos basados en bases de Gröbner resuelven problemas de pertenencia a ideales,
- el algoritmo geométrico de Wu prueba teoremas como el teorema de Pascal en la elipse,
- el algoritmo de Tarski resuelve problemas formulados en el lenguaje de primer orden de los reales,
- ...

Limitaciones

La lógica de primer orden no es lo suficientemente expresiva para expresar algunos resultados matemáticos.

Limitaciones

La lógica de primer orden no es lo suficientemente expresiva para expresar algunos resultados matemáticos.

Entscheidungsproblem, El problema de decisión [Hilbert 1928]

Dado un enunciado en lógica de primer orden, ¿exite un algoritmo capaz de determinar si dicho enunciado es un teorema?

Limitaciones

La lógica de primer orden no es lo suficientemente expresiva para expresar algunos resultados matemáticos.

Entscheidungsproblem, El problema de decisión [Hilbert 1928]

Dado un enunciado en lógica de primer orden, ¿exite un algoritmo capaz de determinar si dicho enunciado es un teorema?

Kurt Gödel

Alonzo Church

Alan Turing

¿Pueden descubrir teoremas?

"In ten years, a computer would discover and prove an important new mathematical theorem."[Herbert A. Simon,1957]

¿Pueden descubrir teoremas?

"In ten years, a computer would discover and prove an important new mathematical theorem."[Herbert A. Simon,1957]

- The Automated Mathematician: "descubrió" los números naturales, los números primos, ternas Pitagóricas, el teorema fundamental de la aritmética.
- Eurisko, sucesor de The Automated Mathematician.
- El proyecto Theorymine.

Índice

1 Motivación

2 Demostración automatizada

3 Demostración asistida por ordenador

¿Qué son los asistentes para la demostración?

Programas que permiten el desarrollo de pruebas formales gracias a la colaboración hombre-máquina.

¿Qué son los asistentes para la demostración?

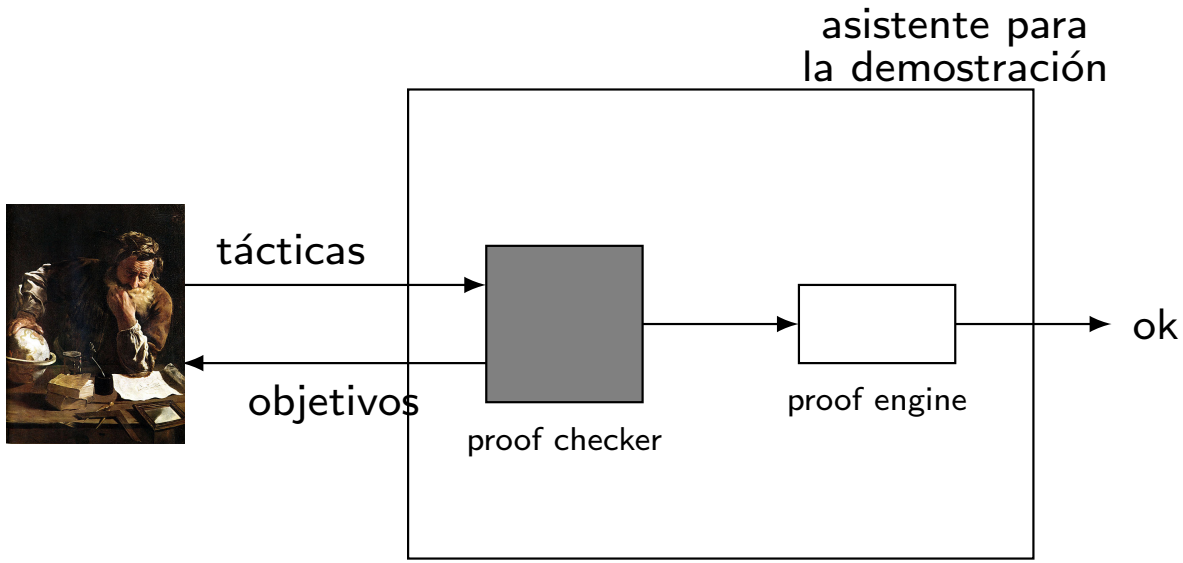
Programas que permiten el desarrollo de pruebas formales gracias a la colaboración hombre-máquina.

- El usuario indica los pasos que debe seguir la demostración.
- El ordenador se encarga de comprobar que todos los pasos dados por el usuario, así como la prueba generada son correctos.

¿Qué son los asistentes para la demostración?

Programas que permiten el desarrollo de pruebas formales gracias a la colaboración hombre-máquina.

- El usuario indica los pasos que debe seguir la demostración.
- El ordenador se encarga de comprobar que todos los pasos dados por el usuario, así como la prueba generada son correctos.



Las distintas fases de una demostración

1. Encontrar una demostración:

   Hacer experimentos, imaginar, simplificar, ...
   No se conservará, pero es una parte fundamental.

Las distintas fases de una demostración

1. Encontrar una demostración:

   Hacer experimentos, imaginar, simplificar, ...
   No se conservará, pero es una parte fundamental.

2. Dar una demostración:

   Prueba detallada que explica porque el teorema se satisface, la estrategia de la prueba y pequeños pasos que permiten verificar el teorema.

Las distintas fases de una demostración

1. Encontrar una demostración:

   Hacer experimentos, imaginar, simplificar, ...
   No se conservará, pero es una parte fundamental.

2. Dar una demostración:

   Prueba detallada que explica porque el teorema se satisface, la estrategia de la prueba y pequeños pasos que permiten verificar el teorema.

3. Presentar una demostración:

   explicarla a otras personas, mejorarla, simplificarla, generalizarla, ...

Las distintas fases de una demostración

1. Encontrar una demostración:

   Hacer experimentos, imaginar, simplificar, ...
   No se conservará, pero es una parte fundamental.

2. Dar una demostración:

   Prueba detallada que explica porque el teorema se satisface, la estrategia de la prueba y pequeños pasos que permiten verificar el teorema.

3. Presentar una demostración:

   explicarla a otras personas, mejorarla, simplificarla, generalizarla, ...

Los asistentes para la demostración ayudan en los pasos 2 y 3.

Los sistemas más usados

- Mizar (teoría de conjuntos).
- Isabelle (lógica de orden superior).
- HOL4 (lógica de orden superior).
- HOL-light (lógica de orden superior).
- Coq (teoría de tipos constructiva).
- ACL2 (lógica de primer orden).
- ...

Dos estilos

Procedural:

Declarativo:

Dos estilos

Procedural:

Indica que es lo que hay que hacer: baja del tren, ve a la derecha, sube las escaleras, sal a la calle, ve hacia la izquierda, ...

Teorema (Demo en Coq)

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

Declarativo:

Dos estilos

Procedural:
Indica que es lo que hay que hacer: baja del tren, ve a la derecha, sube las escaleras, sal a la calle, ve hacia la izquierda, ...

Teorema (Demo en Coq)

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

Declarativo: (más parecido a las demostraciones en matemáticas).
Indica a donde ir: ve a la calle Luís de Ulloa, ve al Edificio Vives, ve a la segunda planta, ...

Teorema (Demo en Isabelle)

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

Formalizando el "top 100"

Formalización del "top 100" de los teoremas matemáticos:

- lista creada por Freek Wiedijk:
  - irracionalidad de $\sqrt{2}$,
  - infinitud de los números primos,
  - imposibilidad de la trisección de un ángulo,
  - divergencia de la serie armónica,
  - teorema fundamental del álgebra
  - teorema fundamental del cálculo integral,
  - transcendencia del número e,
  - primer teorema de incompletitud de Gödel,
  - ...
- Actualmente al 88 %

El teorema de los cuatro colores

Teorema

Dado cualquier mapa geográfico con regiones continuas, éste puede ser coloreado con cuatro colores diferentes, de forma que no queden regiones adyacentes con el mismo color.

El teorema de los cuatro colores: Historia

- 1852: Francis Guthrie conjetura el resultado.

El teorema de los cuatro colores: Historia

- 1852: Francis Guthrie conjetura el resultado.
- 1879: Alfred Kempe da una "prueba" de la conjetura de los cuatro colores.

El teorema de los cuatro colores: Historia

- 1852: Francis Guthrie conjetura el resultado.
- 1879: Alfred Kempe da una "prueba" de la conjetura de los cuatro colores.
- 1890: Percy Heawood demuestra que la prueba de Kempe era incorrecta y prueba el teorema de los cinco colores.

El teorema de los cuatro colores: Historia

- 1852: Francis Guthrie conjetura el resultado.
- 1879: Alfred Kempe da una "prueba" de la conjetura de los cuatro colores.
- 1890: Percy Heawood demuestra que la prueba de Kempe era incorrecta y prueba el teorema de los cinco colores.
- 1976: Kenneth Appel y Wolfgang Haken desarrollan una prueba con la ayuda de un ordenador:

El teorema de los cuatro colores: Historia

- 1852: Francis Guthrie conjetura el resultado.
- 1879: Alfred Kempe da una "prueba" de la conjetura de los cuatro colores.
- 1890: Percy Heawood demuestra que la prueba de Kempe era incorrecta y prueba el teorema de los cinco colores.
- 1976: Kenneth Appel y Wolfgang Haken desarrollan una prueba con la ayuda de un ordenador:
  - si la conjetura fuera falsa $\Longrightarrow$ $\exists$ un mapa con el menor número de regiones que necesita al menos cinco colores,

El teorema de los cuatro colores: Historia

- 1852: Francis Guthrie conjetura el resultado.
- 1879: Alfred Kempe da una "prueba" de la conjetura de los cuatro colores.
- 1890: Percy Heawood demuestra que la prueba de Kempe era incorrecta y prueba el teorema de los cinco colores.
- 1976: Kenneth Appel y Wolfgang Haken desarrollan una prueba con la ayuda de un ordenador:
  - si la conjetura fuera falsa $\Longrightarrow \exists$ un mapa con el menor número de regiones que necesita al menos cinco colores,
  - pero dicho contraejemlo no existe:

El teorema de los cuatro colores: Historia

- 1852: Francis Guthrie conjetura el resultado.
- 1879: Alfred Kempe da una "prueba" de la conjetura de los cuatro colores.
- 1890: Percy Heawood demuestra que la prueba de Kempe era incorrecta y prueba el teorema de los cinco colores.
- 1976: Kenneth Appel y Wolfgang Haken desarrollan una prueba con la ayuda de un ordenador:
  - si la conjetura fuera falsa $\Longrightarrow$ $\exists$ un mapa con el menor número de regiones que necesita al menos cinco colores,
  - pero dicho contraejemlo no existe:
    1. identificar una colección de mapas de modo que todo mapa debe contener una porción que se parezca a uno de ellos (1936 casos),
    2. calcularon que cada uno de estos mapas no puede formar parte de dicho contraejemplo más pequeño.

El teorema de los cuatro colores: formalización en Coq

- 1997: N. Robertson, D. Sanders, P. Seymour y R. Thomas dan una nueva prueba: más sencilla pero usando un ordenador.
- 2000: Georges Gonthier formaliza la parte computacional de dicha prueba en Coq.
- 2005: Georges Gonthier formaliza completamente la prueba en Coq.

El teorema de los cuatro colores: formalización en Coq

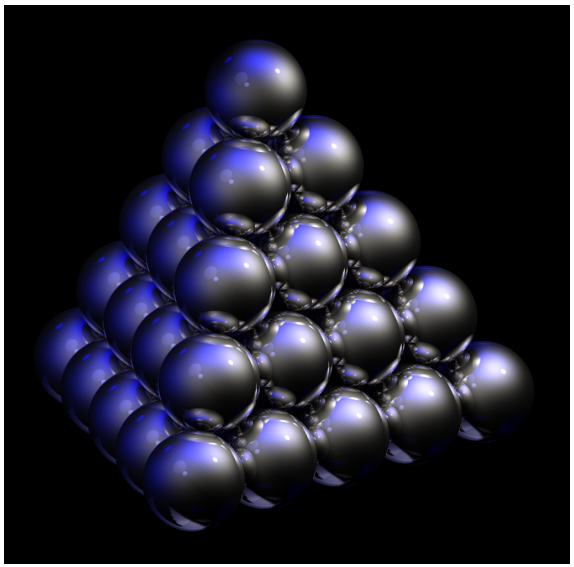
- 1997: N. Robertson, D. Sanders, P. Seymour y R. Thomas dan una nueva prueba: más sencilla pero usando un ordenador.
- 2000: Georges Gonthier formaliza la parte computacional de dicha prueba en Coq.
- 2005: Georges Gonthier formaliza completamente la prueba en Coq.

"formal proof is not merely a method to make absolutely sure we have not made a mistake in a proof, but also a tool that shows us and compels us to understand why a proof works."[G. Gonthier]

La conjetura de Kepler (1611)

Teorema

La manera más compacta de apilar esferas del mismo tamaño es una piramide.



La conjetura de Kepler: la demostración de Thomas Hales

1998 : Thomas Hales anuncia una prueba de la conjetura de Kepler:

- 300 páginas manuscritas:
  - reducción del problema inicial al 5094 casos.
- 40000 líneas de código Java:
  - enumeración de hiperplanos "tame" y demostración de desigualdades no lineales.

La conjetura de Kepler: la demostración de Thomas Hales

1998 : Thomas Hales anuncia una prueba de la conjetura de Kepler:

- 300 páginas manuscritas:
  - reducción del problema inicial al 5094 casos.
- 40000 líneas de código Java:
  - enumeración de hiperplanos "tame" y demostración de desigualdades no lineales.

Reduce el problema a 1039 desigualdades de la forma:

$$\frac{\begin{array}{c}-x_1x_3 - x_2x_4 + x_1x_5 + x_3x_6 - x_5x_6 + \\ x_2(-x_2 + x_1 + x_3 - x_4 + x_5 + x_6)\end{array}}{\sqrt{4x_2\begin{pmatrix} x_2x_4(-x_2 + x_1 + x_3 - x_4 + x_5 + x_6) + \\ x_1x_5(x_2 - x_1 + x_3 + x_4 - x_5 + x_6) + \\ x_3x_6(x_2 + x_1 - x_3 + x_4 + x_5 - x_6) \\ -x_1x_3x_4 - x_2x_3x_5 - x_2x_1x_6 - x_4x_5x_6 \end{pmatrix}}} < \tan\left(\frac{\pi}{2} - 0.74\right)$$

La conjetura de Kepler: el proyecto Flyspeck

"The referees put a level of energy into this that is, in my experience, unprecedented."

"The news from the referees is bad, from my perspective. They have not been able to certify the correctness of the proof, and will not be able to certify it in the future, because they have run out of energy to devote to the problem." [Respuesta del editor de Annals of Mathematics].

Se considera que la demostración de Hales es correcta al 99 %.

La conjetura de Kepler: el proyecto Flyspeck

"The referees put a level of energy into this that is, in my experience, unprecedented."

"The news from the referees is bad, from my perspective. They have not been able to certify the correctness of the proof, and will not be able to certify it in the future, because they have run out of energy to devote to the problem." [Respuesta del editor de Annals of Mathematics].

Se considera que la demostración de Hales es correcta al 99 %.

El proyecto Flyspeck:

- Acrónimo de FPK: Formal Proof of the Kepler conjecture.
- 2003 - ?: se estima una duración aproximada de 20 años (en 2010 al 50 %).
- 16 personas involucradas en el proyecto.

La clasificación de los grupos finitos simples

Teorema

Todo grupo finito simple es isomorfo a:

- *un grupo cíclico con orden primo,*
- *un grupo alternante de grado al menos 5,*
- *un grupo de Lie simple, o*
- *uno de los 26 grupos simples esporádicos.*

La clasificación de los grupos finitos simples

Teorema

Todo grupo finito simple es isomorfo a:

- *un grupo cíclico con orden primo,*
- *un grupo alternante de grado al menos 5,*
- *un grupo de Lie simple, o*
- *uno de los 26 grupos simples esporádicos.*

- 1983: Gorenstein anuncia la clasificación de los grupos finitos simples (no incluye grupos "quasithin"),
- 2004: Aschbacher y Smith publican una clasificación completa,
- $\sim$ 500 artículos, $\sim$ 100 autores, $\sim$5000 páginas.

El teorema de Feit-Thompson

Teorema (El teorema de Feit-Thompson)

Todo grupo finito de order impar es resoluble.

El teorema de Feit-Thompson

Teorema (El teorema de Feit-Thompson)

Todo grupo finito de order impar es resoluble.

- Importancia: todo grupo finito simple de orden impar es un grupo cíclico de orden primo.

El teorema de Feit-Thompson

Teorema (El teorema de Feit-Thompson)

Todo grupo finito de order impar es resoluble.

- Importancia: todo grupo finito simple de orden impar es un grupo cíclico de orden primo.

  "While it was usually mentioned in courses on algebra, it is only fair to say that nobody ever did anything about it, simply because nobody had any idea how to get even started." [Brauer]

El teorema de Feit-Thompson

Teorema (El teorema de Feit-Thompson)

Todo grupo finito de order impar es resoluble.

- Importancia: todo grupo finito simple de orden impar es un grupo cíclico de orden primo.

  "While it was usually mentioned in courses on algebra, it is only fair to say that nobody ever did anything about it, simply because nobody had any idea how to get even started." [Brauer]
- 2 volúmenes, 255 páginas.

Formalización del teorema de Feit-Thompson

Llevada a cabo por el proyecto Mathematical Components:

- proyecto liderado por Georges Gonthier.
- 15 personas, 6 años (2006–12), 170000 líneas de código, 15000 definiciones, 4300 teoremas.

Formalización del teorema de Feit-Thompson

Llevada a cabo por el proyecto Mathematical Components:

- proyecto liderado por Georges Gonthier.
- 15 personas, 6 años (2006–12), 170000 líneas de código, 15000 definiciones, 4300 teoremas.

Logros de este proyecto:

- formalización de un gran teorema,
- formalización de varias teorías necesarias para la prueba de Feit-Thompson: enlace.

Formalización del teorema de Feit-Thompson

Llevada a cabo por el proyecto Mathematical Components:

- proyecto liderado por Georges Gonthier.
- 15 personas, 6 años (2006–12), 170000 líneas de código, 15000 definiciones, 4300 teoremas.

Logros de este proyecto:

- formalización de un gran teorema,
- formalización de varias teorías necesarias para la prueba de Feit-Thompson: enlace.

"The Feit-Thompson Theorem is the first steppingstone in a much larger result, the classification of finite simple groups, which is known as the monster theorem because it's one of those theorems where belief in it resides in the belief of a few selected people who have understanding of it."[G. Gonthier]

Otras aplicaciones

Verificación de software/hardware:

- el microprocesador ARM,
- el sistema operativo L4,
- un compilador de C,
- sistemas de identificación biométrica,
- fragmentos críticos de código relacionado con vuelos espaciales,
- ...

¿Qué más hace falta?

Problemas:

- De Brujin factor: una formalización ocupa 4 veces el tamaño de una prueba informal en latex,
- formalizar una página de un libro de texto de matemáticas puede costar una semana,
- diversidad de herramientas,
- el proceso de formalización es distinto a la demostración usual en matemáticas,
- es necesaria más automatización.

¿Qué más hace falta?

Problemas:

- De Brujin factor: una formalización ocupa 4 veces el tamaño de una prueba informal en latex,
- formalizar una página de un libro de texto de matemáticas puede costar una semana,
- diversidad de herramientas,
- el proceso de formalización es distinto a la demostración usual en matemáticas,
- es necesaria más automatización.

Objetivo:

- lograr una aceptación similar a los sistemas de cálculo simbólico,
- uso para: descartar casos triviales, asegurarnos que el desarrollo de una demostración es el correcto, capacitar a los revisores de una revista para reproducir una demostración, . . .

Terminando...

"Formalization of mathematics can be a very rewarding activity in its own right. It combines the pleasure of computer programming (craftsmanship, and the computer doing things for you), with that of mathematics (pure mind, and absolute certainty.) People who do not like programming or who do not like mathematics probably will not like formalization. However, for people who like both, formalization is the best thing there is."[F. Wiedijk]

¿Pueden los ordenadores ayudarnos en la demostración de teoremas?

Jónathan Heras

School of Computing, University of Dundee, UK
http://www.computing.dundee.ac.uk/staff/jheras/

Curso de Actualización en Matemáticas
20 de marzo de 2013