Prove

Scuola Estiva di Logica
Palazzo Feltrinelli, Gargnano, 25 agosto 2011

Andrea Asperti

Dipartimento di Scienze dell'Informazione
UniversitÃ degli Studi di Bologna

25/08/2011

Abstract

L'avvento degli strumenti di ausilio alla dimostrazione formale (interactive theorem provers) ha riaperto il dibattito sulla nozione di dimostrazione matematica e sulla loro funzione.

In questo talk presentiamo e discutiamo alcune posizioni contrastanti, cercando di chiarire il ruolo dei sistemi suddetti nella pratica matematica.

Content

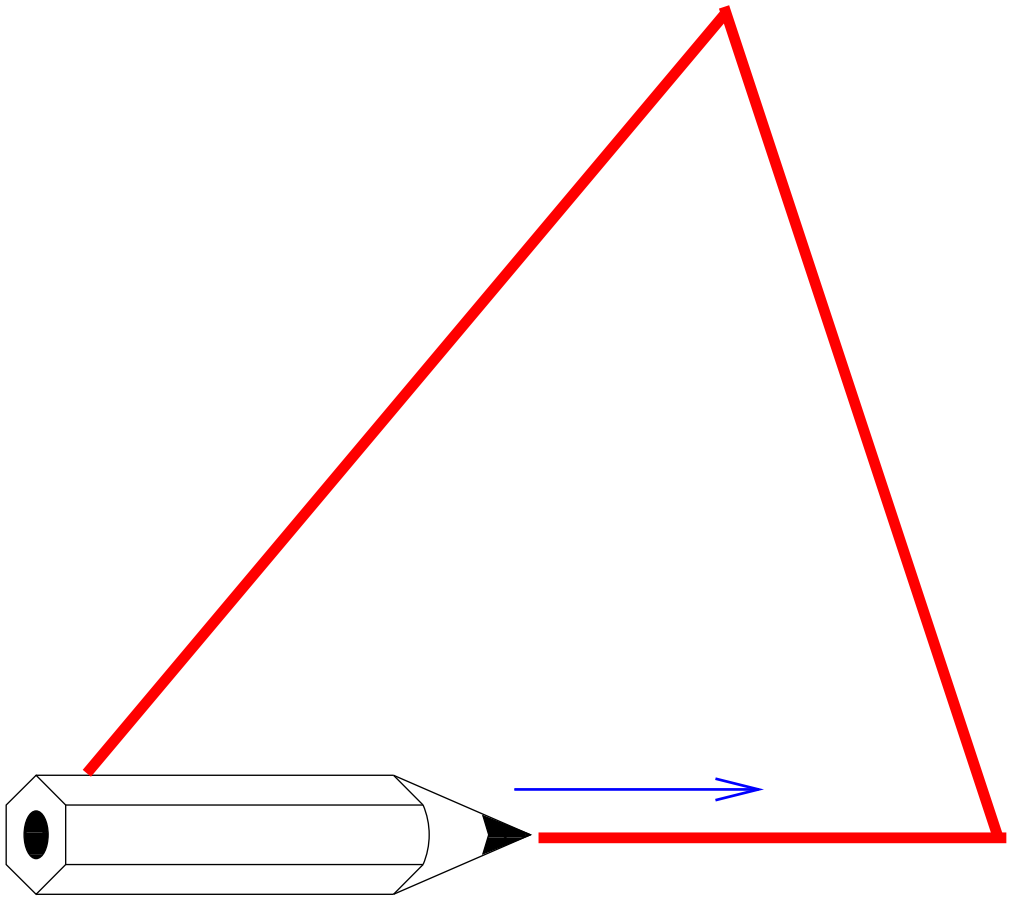
Content

Content

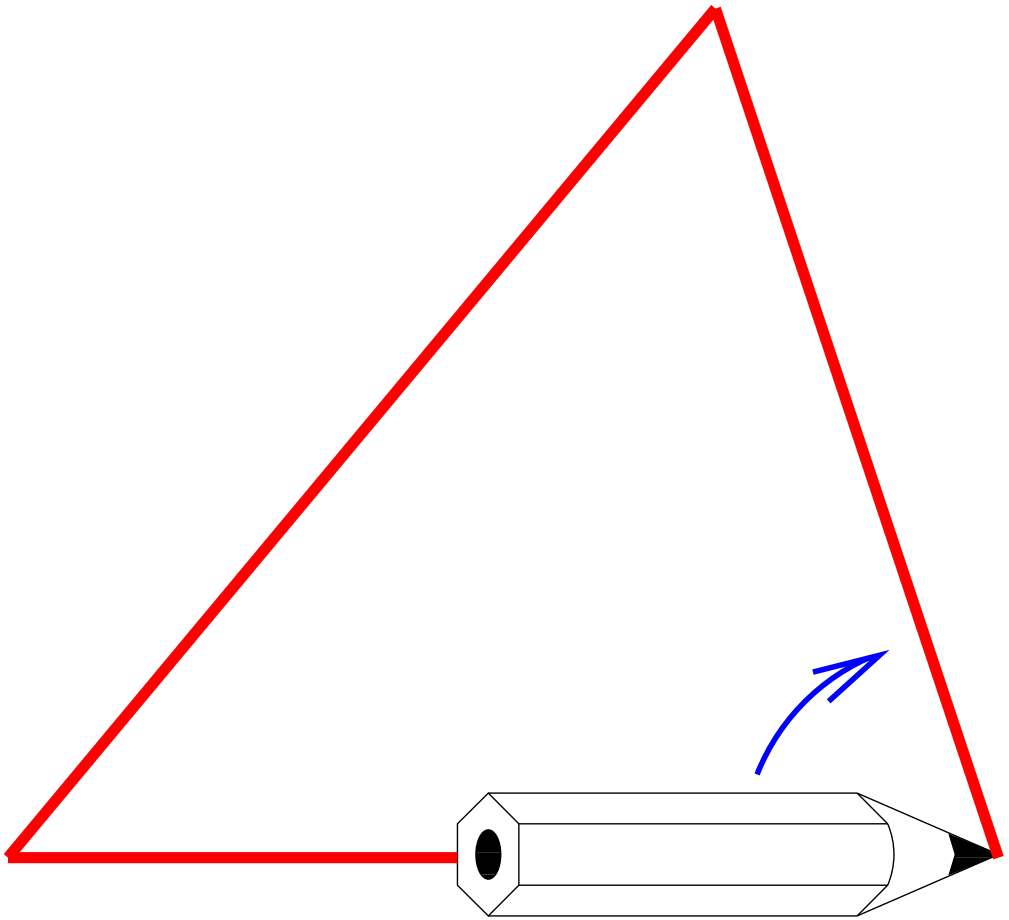
Content

Content

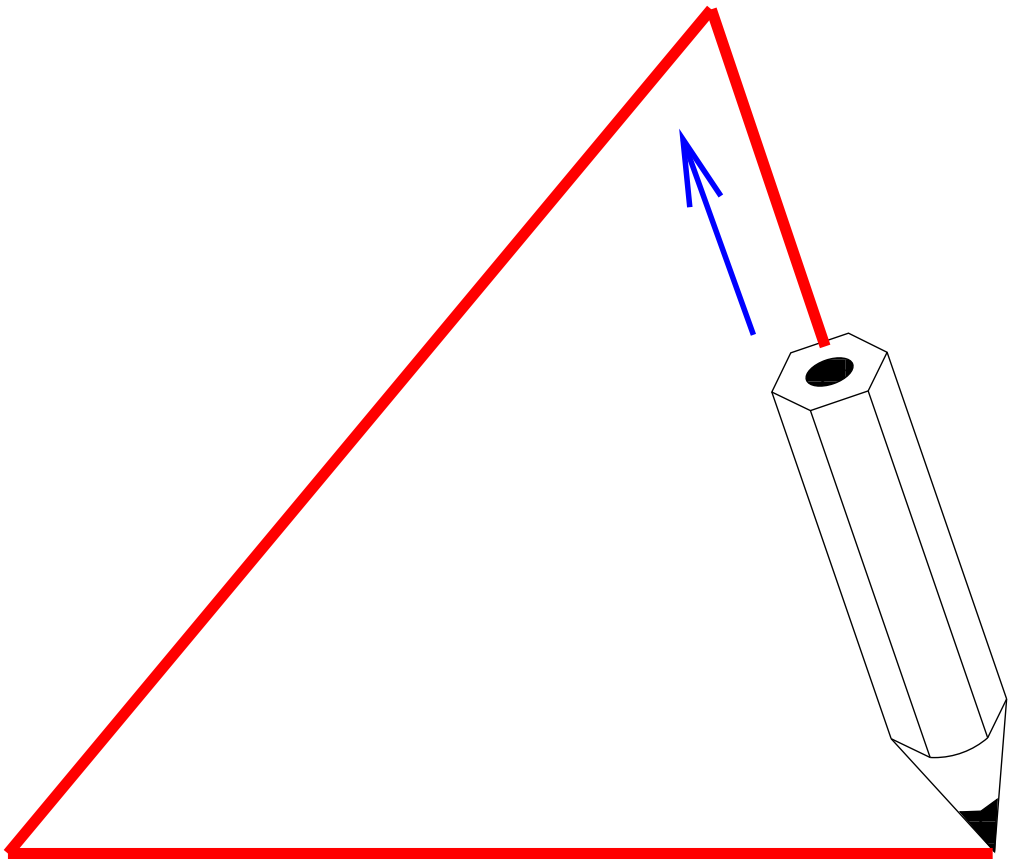
Il teorema di Euclide



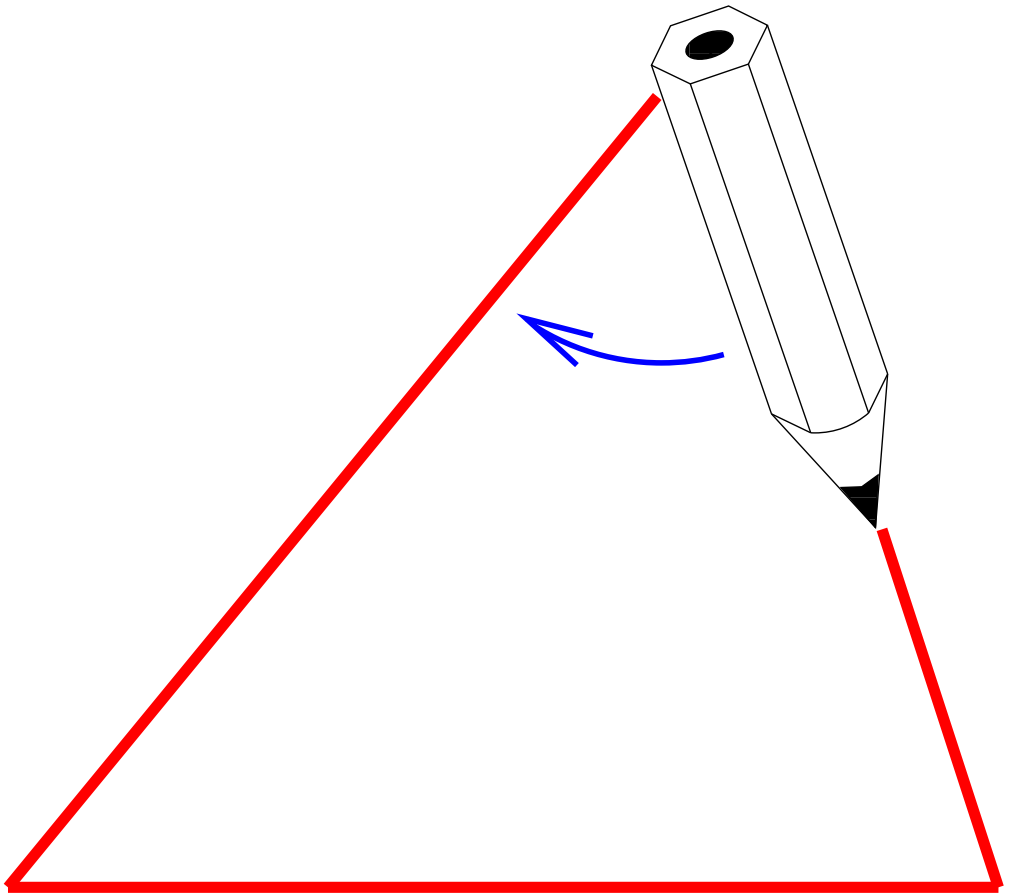
Il teorema di Euclide



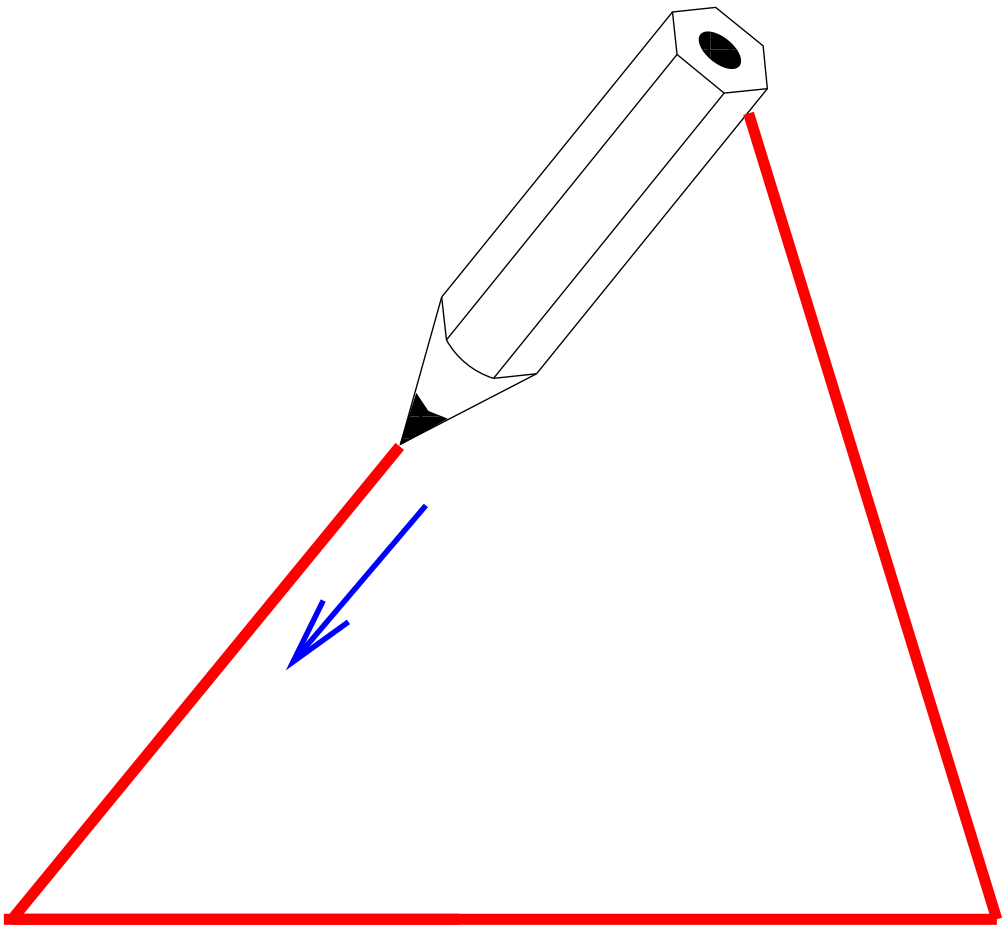
Il teorema di Euclide



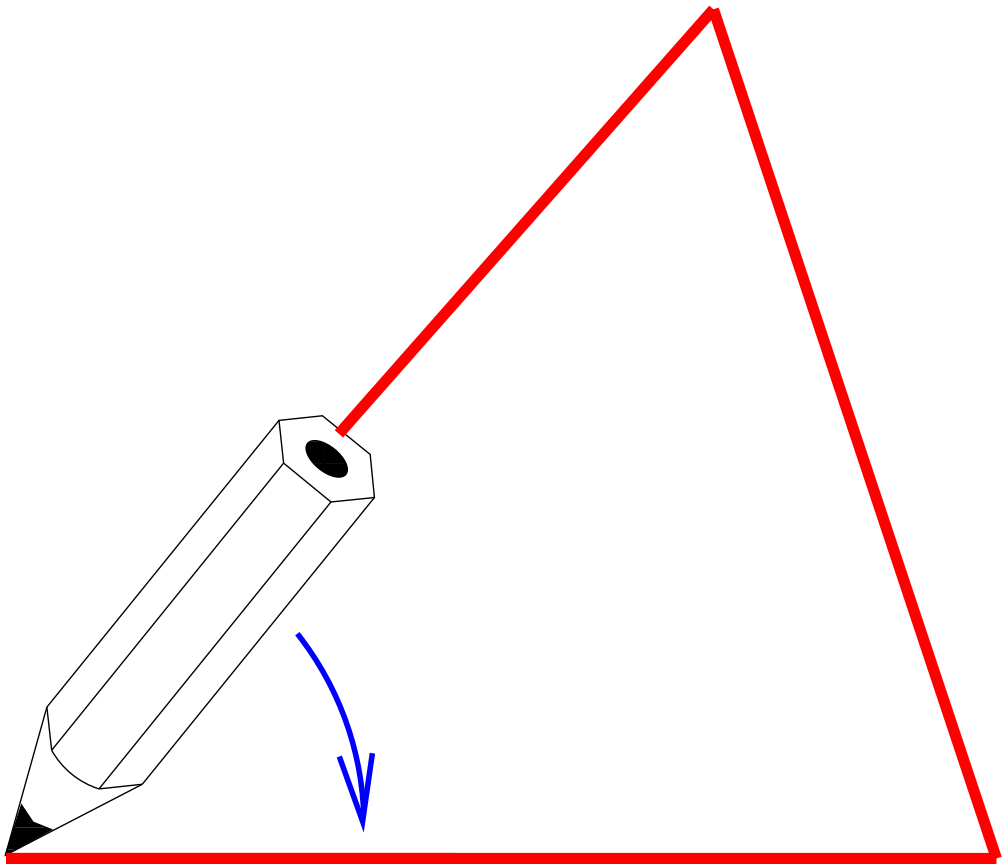
Il teorema di Euclide



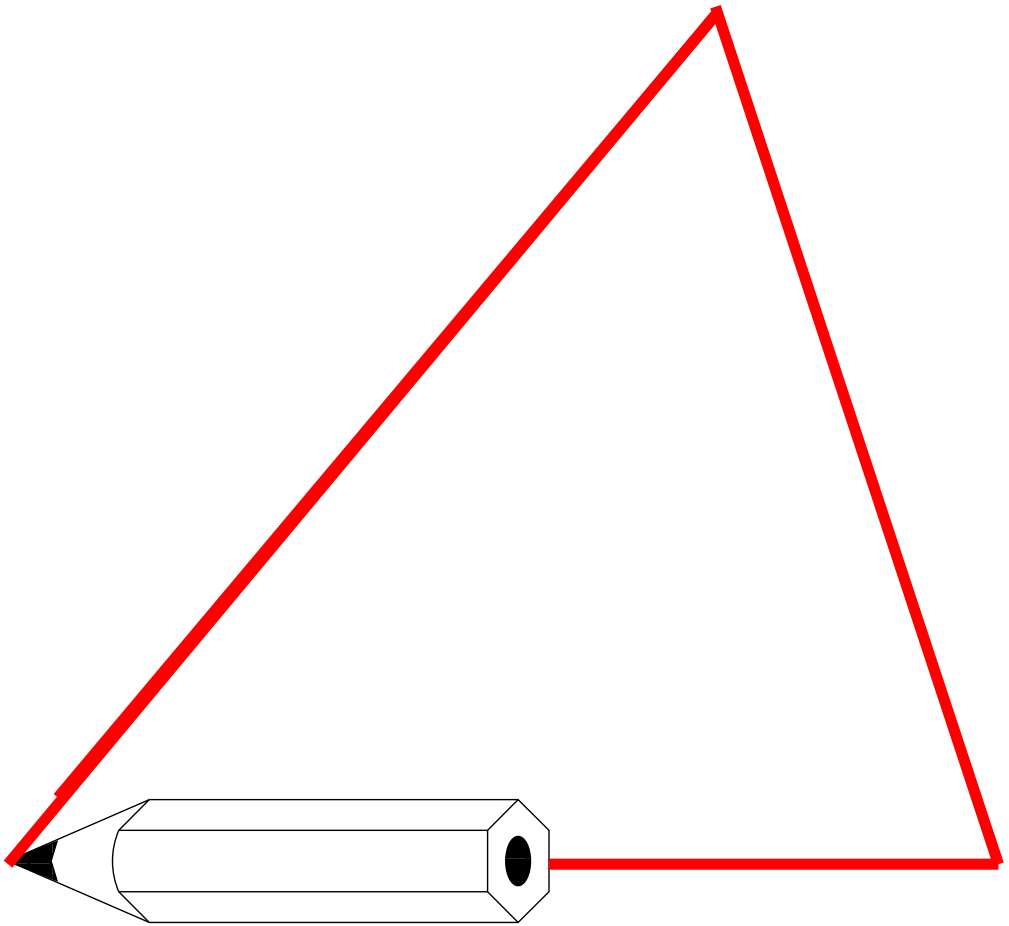
Il teorema di Euclide



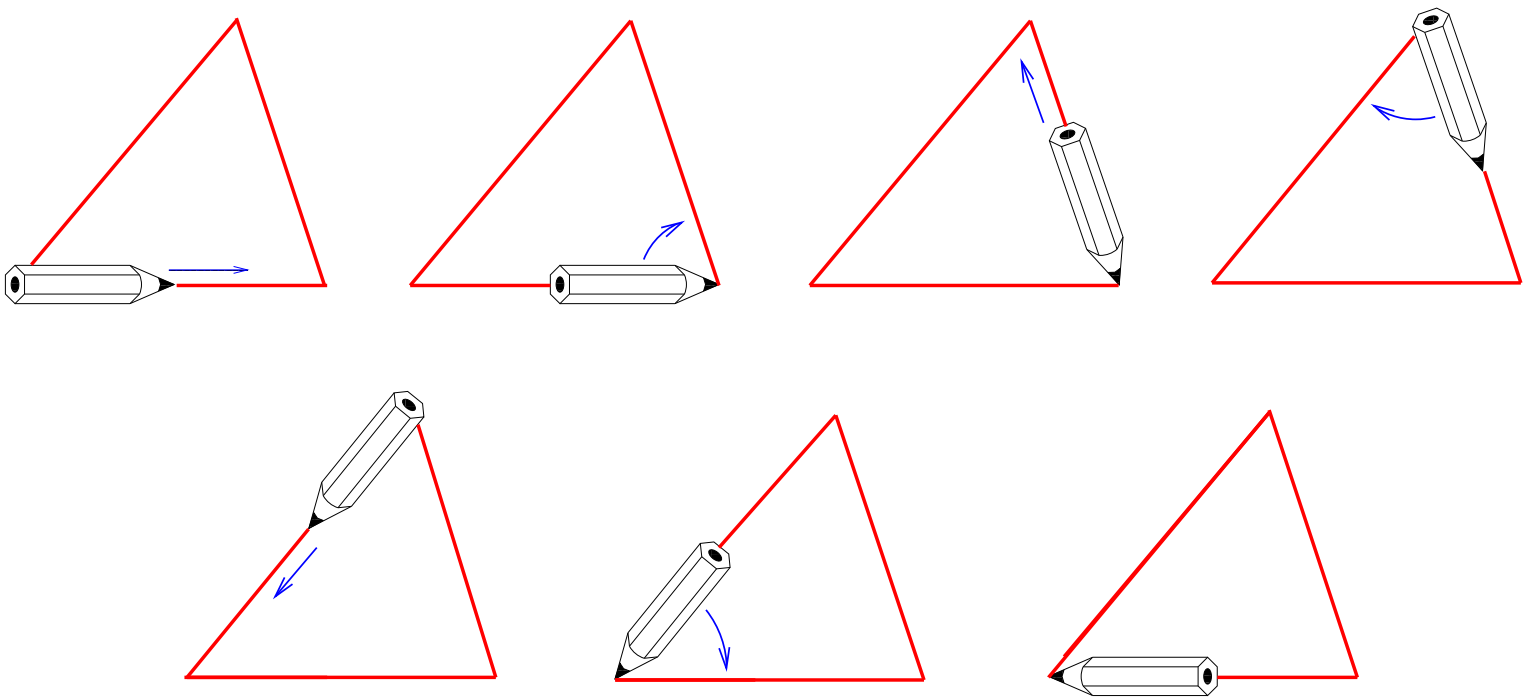
Il teorema di Euclide



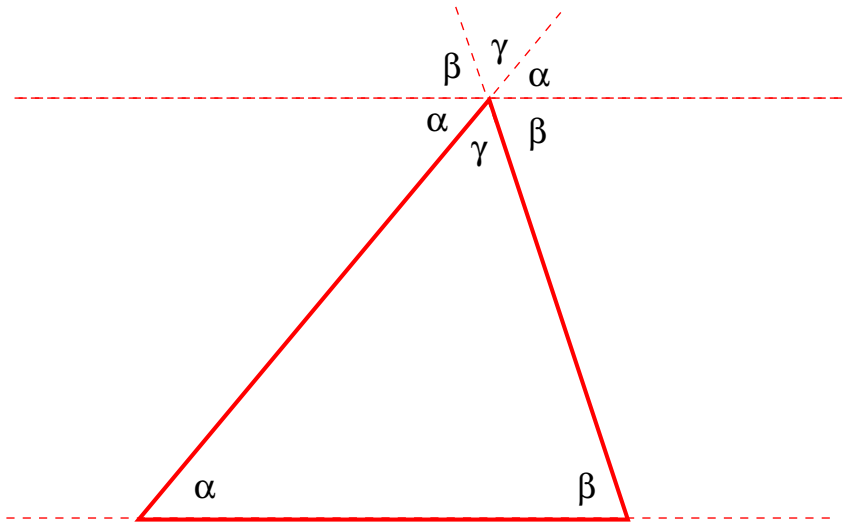
Il teorema di Euclide



Il teorema di Euclide



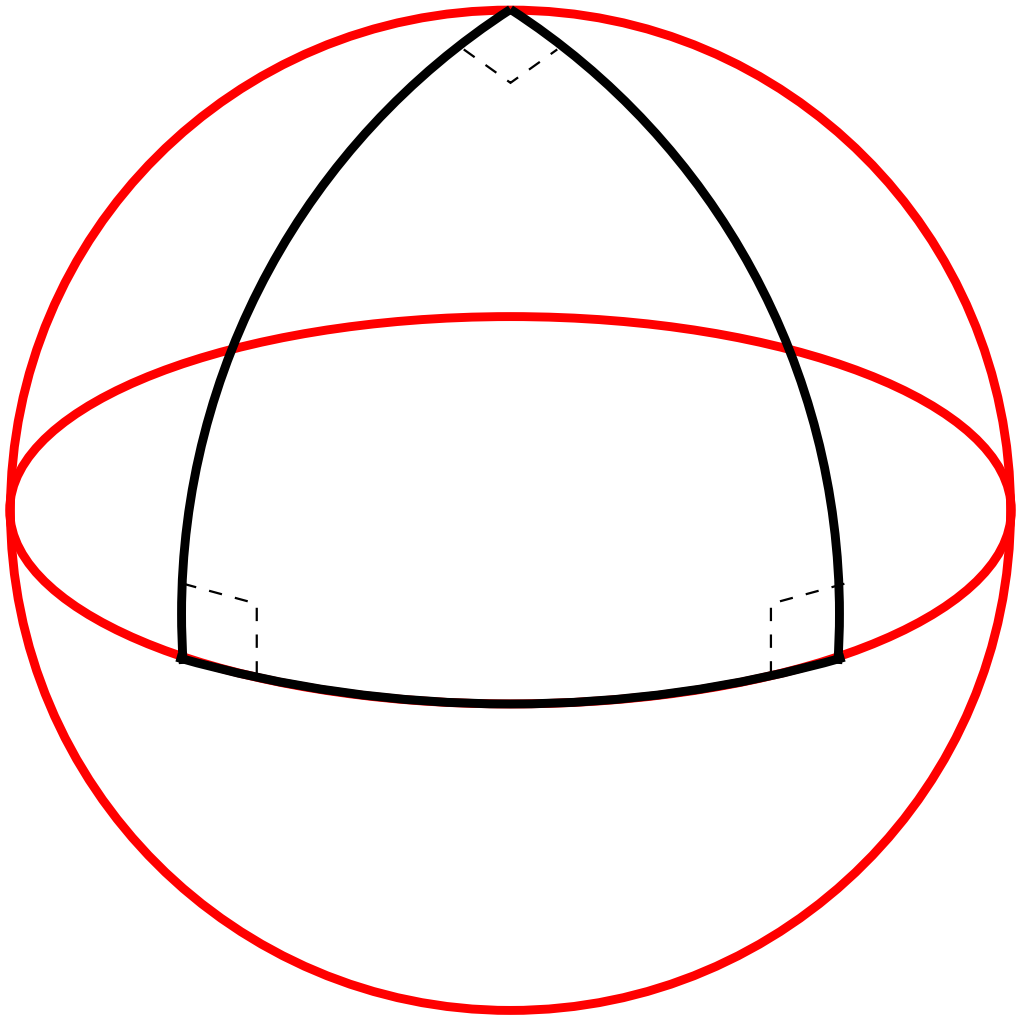
Discussione (da MKM mailing list)



Dana Scott

The proof is fine and really is the same as the classical proof. To see this, translate (by parallel translation) all the three angles of the triangle up to the line through the top vertex of the triangle parallel to the lower side. [...]

Il teorema di Euclide



Discussione (da MKM mailing list)

Arnon Avron

If this "proof" is taught to students as a full, valid proof, then I do not see how the teacher will be able to explain to those students where the hell Euclid's fifth postulate (or the parallels axiom) is used here, or even what is the connections between the theorem and parallel lines.

Dana Scott

I should have commented in my explanation of the proof that if you translate the line on which the base of the triangle sits along each of the sides up to the vertex, then both actions result in the same line – the unique parallel.

Thought experiments

Secondo Lakatos, le "prove" non dimostrano nulla: sono solo "thought experiments" che non conducono necessariamente ai risultati attesi.

Lakatos - 1976

After Columbus one should not be surprised if one does not solve the problem one has set out to solve.

Messaggio e certificato

Duplice funzione epistemologica delle prove:

- **Messaggio**: fornire intuizione sulla validità di un asserto; comunicare nuove tecniche e nuovi risultati.
- **Certificato**: fornire evidenze che permettano di verificare la correttezza di un enunciato.

Messaggio e certificato

Hardy - 1928

There is strictly speaking no such thing as a mathematical proof; we can, in the last analysis, do nothing but point; [...] proofs are what Littlewood and I call *gas*, rhetorical flourishes designed to affect psychology, pictures on the board in the lecture, devices to stimulate the imagination of pupils. [16]

N.G.De Brujin - 2004

If you can't explain your mathematics to a machine it is an illusion to think you can explain it to a student. [6]

Un semplice esempio

Somma dei primi n naturali positivi.

- **Messaggio**

$$\begin{array}{cccccc} 1 & 2 & \dots & n-1 & n \\ n & n-1 & \dots & 2 & 1 \\ \hline n+1 & n+1 & \dots & n+1 & n+1 \end{array}$$

- **Certificato (induzione)**

$$\frac{(n-1)\cdot n}{2} + n = \frac{n\cdot(n+1)}{2}$$

A social process

R.A. De Millo, R.J. Lipton, A.J. Perlis -1979

We believe that, in the end, it is a social process that determines whether mathematicians feel confident about a theorem. [9]

Lakatos

"Certainty" is far from being a sign of success, it is only a symptom of lack of imagination, of conceptual poverty. It produces smug satisfaction and prevents the growth of knowledge. [...] The risk is to construct formalized languages in which artificially congealed states of science are expressed. [...] Science teaches us not to respect anygiven conceptual-linguistic framework lest it should turn into a conceptual prison. [19]

or a solypstic activity?

L.Lamport - 1980

A theorem either can or cannot be derived from a set of axioms. I don't believe that the correctness of a theorem is to be decided by a general election. [20]

T.Coquand - 2008

The history of mathematics has stories about false results that went undetected for long periods of time. However, it is generally believed that if a published mathematical argument is not valid, it will be eventually detected as such. While the process of finding a proof may require creative insight, the activity of checking a given mathematical argument is an objective activity; mathematical correctness should not be decided by a social process. [8]

Il problema della complessità

R.A. De Millo, R.J. Lipton, A.J. Perlis -1979

Russell did succeed in showing that ordinary working proofs can be reduced to formal, symbolic deductions. But he failed, in three enormous, taxing volumes, to get beyond the elementary facts of arithmetic. He showed what can be done in principle and what cannot be done in practice.
[...] A formal demonstration of one of Ramanujan's conjectures assuming set theory and elementary analysis would take about two thousand pages. [2]

Il problema della complessità

Bourbaki - 1950

The tiniest proof at the beginning of the Theory of Sets would already require several hundreds of signs for its complete formalization. [5]

Harrison - 2008

The arrival of the computer changes the situation dramatically. [...] checking conformance to formal rules is one of the things computers are very good at. [...] the Bourbaki claim that the transition to a completely formal text is routine seems almost an open invitation to give the task to computers. [17]

Un parallelo con la compilazione

Maurer - 1979

We can make an analogy here with compiling a higher level language program into a machine language. Originally this was done by hand [...], then compilers came along and started to do the job automatically. [...] nobody is ever going to read the object code produced by a compiler; one simply trusts the compiler. [22]

Interactive Provers: sistemi che interpretano un linguaggio matematico di "alto livello" (procedurale o dichiarativo) e generano una formale che viene verificata automaticamente.

Prove, traccie, suggerimenti

L'insieme delle formule aritmetiche valide è un insieme produttivo.

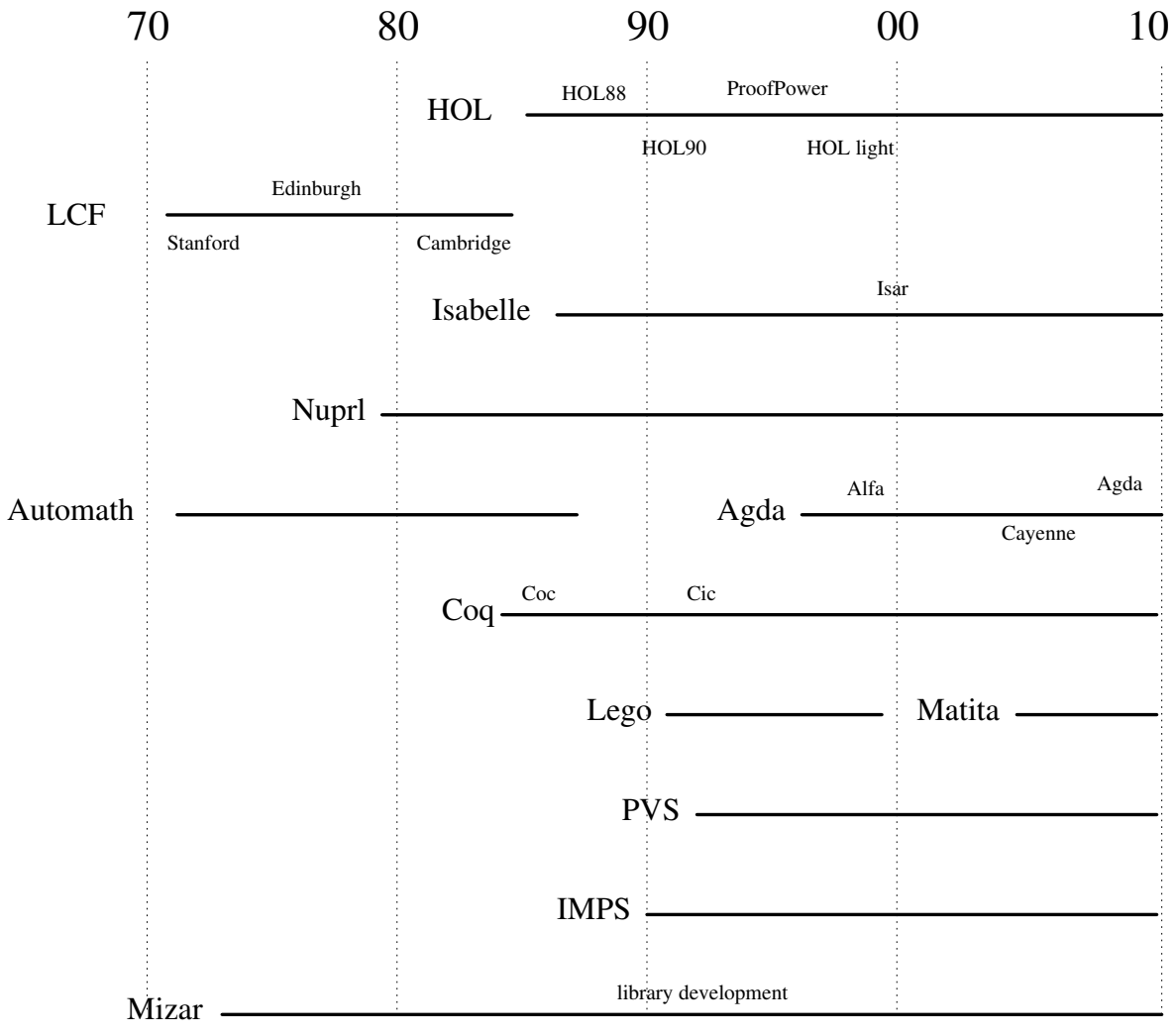
Un sistema formale fornisce una approssimazione ricorsivamente enumerabile delle formule valide (tipicamente come proiezione esistenziale di un insieme ricorsivo di coppie dimostrazione -enunciato).

In senso lato, una prova è una qualunque informazione aggiuntiva che permetta di *decidere* la dimostrabilità di φ (ad esempio, un intero che fornisce un upper bound alla dimensione della dimostrazione).

Prove, traccie, suggerimenti

- la dimensione della traccia può essere resa arbitrariamente piccola a scapito del tempo di ricostruzione.

Sistemi di supporto alla dimostrazione formale



Alcuni recenti risultati

- **Distribuzione asintotica dei numeri primi**, formalizzato da J.Avigad et. al. in Isabelle. 30.000 lines, 43 files. [4]
- **Teorema dei quattro colori**, formalizzato da G.Gonthier in Coq. 60.000 lines, 132 files. [11]
- **Teorema della curva di Jordan**, formalizzato da Tom Hales in HOL light. 75000 lines, 15 files [15] (poi dimostrato anche in Mizar)

Principali progetti in via di sviluppo: Flyspeck

- **Flyspeck** Nel 1988 Hales sostenne di avere una dimostrazione della congettura di Keplero (il modo più compatto per disporre sfere nello spazio é quello normalmente usato per impilare arance su di un banco).

  La prova si basava su di un numero considerevole di disuguaglianze verificate con l'ausilio di un calcolatore e il lavoro venne in un primo tempo rifiutato per pubblicazione dagli Annals of Mathematics.

  Flyspeck [14] è incentrato sulla verifica formale dell'intero teorema.

Principali progetti in via di sviluppo: gruppi finiti

- **Il teorema di classificazione dei gruppi finiti**.
  Il risultato matematico è la sintesi di un lavoro collettivo di un centinaio di autori per un totale di oltre 10000 pagine, distribuite in oltre 500 articoli.

  Uno dei risultati principali, il teorema di Feit-Thomson (odd-order theorem) [10] prende da solo 55 pagine.

  La formalizzazione del teorema di Feit-Thomson è l'obiettivo del progetto congiunto INRIA-Microsoft "mathematical components" diretto da G. Gonthier [12].

Nuova era della matematica

- Prove di dimensioni eccezionali.
- Prove con forte contenuto computazionale.

MacKenzie 2005

It is a scenario that has repeated itself, with variations, several times in recent years: A high-profile problem is solved with an extraordinarily long and difficult megaproof, sometimes relying heavily on computer calculation and often leaving a miasma of doubt behind it.
[...] The computer, which at first sight seems to be part of the problem, may also be the solution. [21]

Stato dell'arte

- **Rapporto tra lunghezza della prova formale e quella cartacea** (fattore di De Brujin): ≈ 4 (tra due 2 e 10).
- **Costo della formalizzazione** 1-1.5 settimane per pagina

Bibliografia


A.Asperti and J.Avigad. Zen and the art of formalization.
Mathematical Structures in Computer Science, 21(4), pp.679-682, 2011.


A.Asperti, H.Geuvers and R.Natarajan.
Social processes, program verification and all that.
Mathematical Structures in Computer Science, 19(5), pp.877-896, 2009.


A.Asperti and C.Sacerdoti Coen.
Some Considerations on the Usability of Interactive Provers.
Proc. of CICM 2010, LNCS 6167, pp. 147-156. 2010.


J.Avigad, K.Donnelly, D.Gray, and P.Raff.
A formally verified proof of the prime number theorem.
ACM Trans. Comput. Log., 9(1), 2007.


N.Bourbaki. The architecture of mathematics. *Monthly*, 57:221–232, 1950.


N.G.De Bruijn. Memories of the automath project.
Invited Lecture at the Mathematics Knowledge Management Symposium, 25-29 November 2003, Heriot-Watt University, Edinburgh, Scotland.


R.L.Constable, S.F. Allen, H. M. Bromley, W. R. Cleaveland, J. F. Cremer, R. W. Harper, D. J. Howe, T. B. Knoblock, N. P. Mendler, P. Panangaden, J. T. Sasaki, and S. F. Smith.
Implementing Mathematics with the Nuprl Development System.
Prentice-Hall, NJ, 1986.


T.Coquand. Draft of the formath project.


R. A. DeMillo, R. J. Lipton, and Alan J. Perlis.
Social processes and proofs of theorems and programs. *Commun. ACM*, 22(5):271–280, 1979.


W. Feit and J. G. Thompson. Solvability of groups of odd order.
Pacific Journal of Mathematics, 13:775–1029, 1963.


G. Gonthier.The four colour theorem: Engineering of a formal proof.
Proceedings of the 8th Asian Symposium on Computer Mathematics, ASCM 2007, Singapore, 2007.


G. Gonthier, A. Mahboubi, L. Rideau, E. Tassi, and L.Thery.
A modular formalisation of finite group theory.
TPHOLS 2007, LNCS 4732, pp 86–101, 2007.


G. Gonthier. Formal proof - the four color theorem.
Notices of the American Mathematical Society, 55:1382–1394, 2008.


T.Hales. Formal proof.
Notices of the American Mathematical Society, 55:1370–1381, 2008.


T.Hales. The jordan curve theorem, formally and informally.
The American Mathematical Monthly, 114:882–894, 2007.


G. H. Hardy. Mathematical proof. *Mind*, 38:1–25, 1928.


J.Harrison. Formal proof - theory and practice.
Notices of the American Mathematical Society, 55:1395–1406, 2008.


M.Kerber. Proofs, Proofs, Proofs, and Proofs. Proc. of CICM 2010, LNCS 6167, pp. 345-354. 2010.


I. Lakatos. *Proofs and Refutations: The Logic of Mathematical Discovery*.
Cambridge University Press, 1976.


L.Lamport. Letter to the editor. *Communications of the ACM*, 22:624, 1979.


D.MacKenzie. What in the name of euclid is going on here?
Science, 207(5714):1402–1403, 2005.


W. D. Maurer. Letter to the editor. *Communications of the ACM*, 22:625–629, 1979.