Il problema di P e NP

Calcolo efficiente, sicurezza di Internet,
e i limiti della conoscenza umana

Linda Pagli
Dipartimento di Informatica
Università di Pisa

Clay Math Institute
Problemi del Millennio da $1M ciascuno

- Congettura di Birch and Swinnerton-Dyer
- Congettura di Hodge
- Equazioni di Navier-Stokes
- P vs NP
- ~~Congettura di Poincaré~~

- Ipotesi di Riemann
- Teoria di Yang-Mills

Introduzione

I Computer sono velocissimi.

Certi problemi richiedono tantissimo tempo!

Cominciamo con un esempio molto semplice:

Un semplice esempio

$7 \times 13 = ?$

Problema della Moltiplicazione
(Risposta 91)

Un altro semplice esempio

? x ? = 91

"Problema della fattorizzazione"
(Risposta: 7 x 13)

Un esempio più grande di moltiplicazione

1.634.733.645.809.253.848
443.133.883.865.090.859.
841.783.670.033.092.312.
181.110.842.389.333.100.
104.508.151.212.118.167.
511.579

X

1.900.871.281.664.822.113.
126.851.573.935.413.975
471.896.789.968.515.493.
666.638.539.088.027.103.
802.104.498.957.191.261.
465.571

= ?

La risposta è:

3.107.418.240.490.043.721.350.750.035.888.567.930.037.346.022.842.727.
545.720.161.948.823.206.440.518.081.504.556.346.829.671.723.286.782.
437.916.272.838.033.415.471.073.108.501.919.548.529.007.337.724.822.
783.525.742.386.454.014.691.736.602.477.652.346.609

Ha richiesto meno di un secondo di tempo di calcolo

Un esempio più grande di fattorizzazione

? x ? =

3.107.418.240.490.043.721.350.750.035.888.567.930.037.
346.022.842.727.545.720.161.948.823.206.440.518.081.
504.556.346.829.671.723.286.782.437.916.272.838.033.
415.471.073.108.501.919.548.529.007.337.724.822.
783.525.742.386.454.014.691.736.602.477.652.346.609

La risposta è:

1.634.733.645.809.253.848
443.133.883.865.090.859.
841.783.670.033.092.312.
181.110.842.389.333.100.
104.508.151.212.118.167.
511.579

x

1.900.871.281.664.822.113.
126.851.573.935.413.975
471.896.789.968.515.493.
666.638.539.088.027.103.
802.104.498.957.191.261.
465.571

Ha richiesto 20 anni di tempo di calcolo

Non ancora fattorizzato:

7403756347956171282804679609742957314259318888923128908 4
9362326389727650340282662768919964196251178439958943305 0
2127585370118968098286733173273108930900552505116877063 29
9072396380786710086096962537934650563796359

Numero di 212 cifre: RSA-704

Erano stati offerti 30.000 $, ma la gara è stata chiusa nel 2007 e nessuno ha vinto il premio.

La fattorizzazione è un ingrediente della crittografia

Per aprire un lucchetto a combinazione occorrono pochi secondi conoscendo le 4 cifre della combinazione (PIN)

Se non si ha il PIN di 4 cifre occorrono 10.000 prove per scoprire la combinazione giusta

presi due numeri primi p, q

Calcolare $n = p \times q$ " è facile "

Calcolare p, q da n " è difficile "

perché si devono provare tutti i divisori di n che, come per il lucchetto, sono in numero esponenziale rispetto al numero di cifre di n

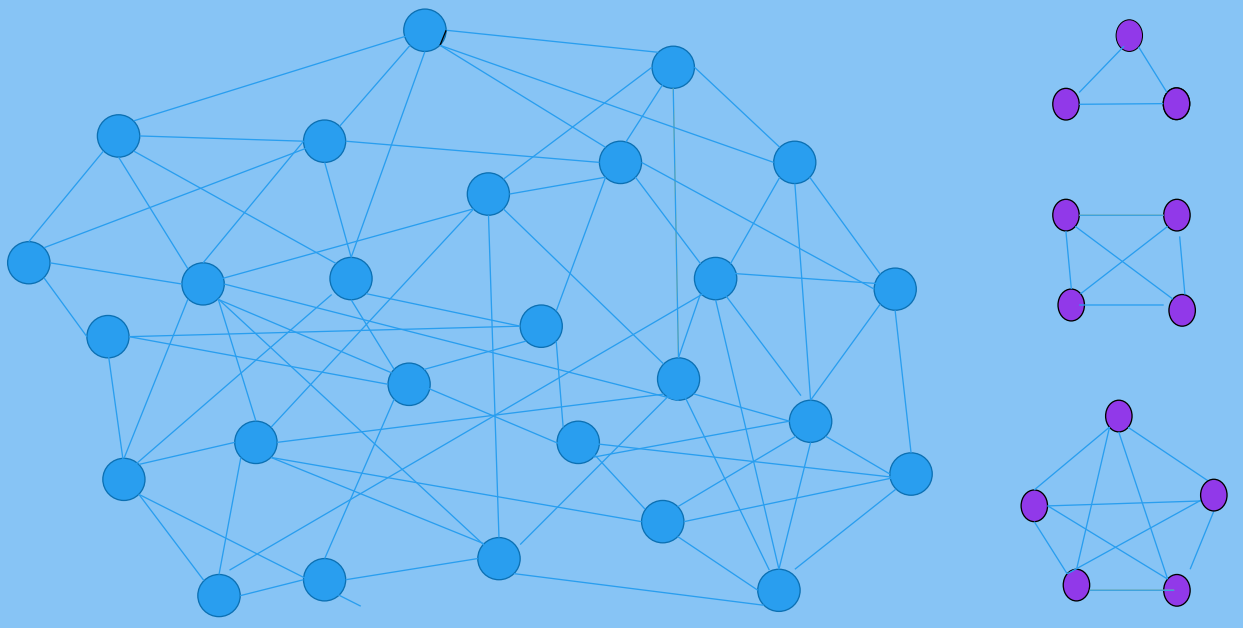
Ricerca col metodo "brute force" .

Ricerca esaustiva : molto lenta se lo spazio di ricerca è ampio.

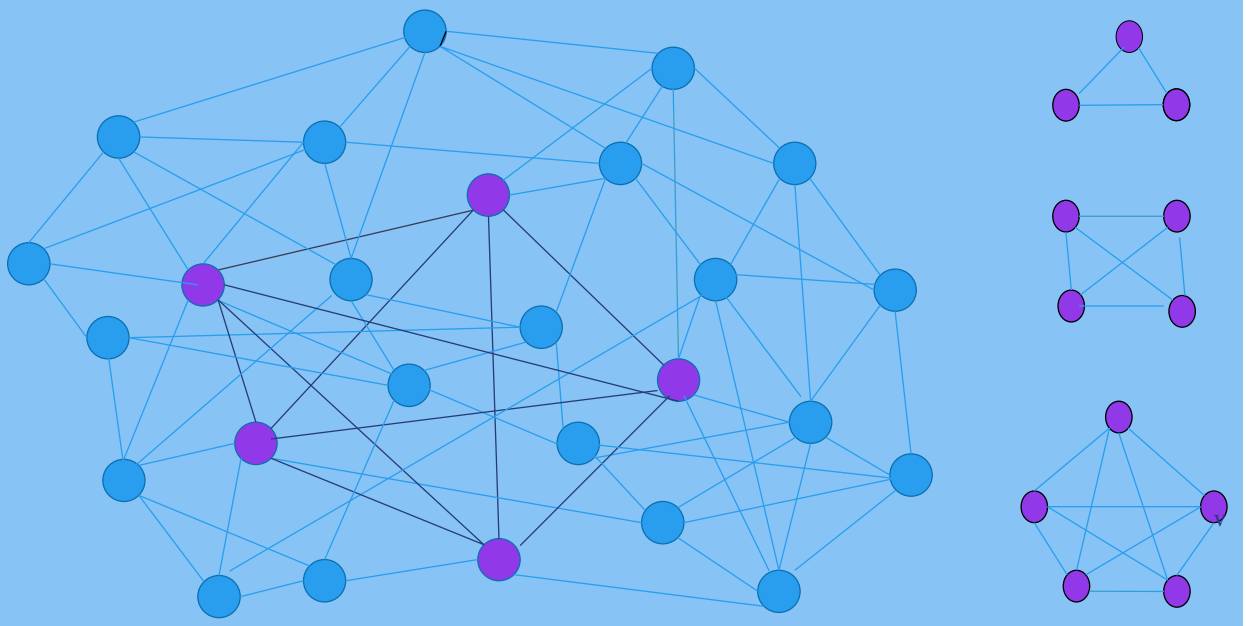
Ma la ricerca esaustiva è necessaria?

Non sappiamo rispondere

Problema della CLIQUE

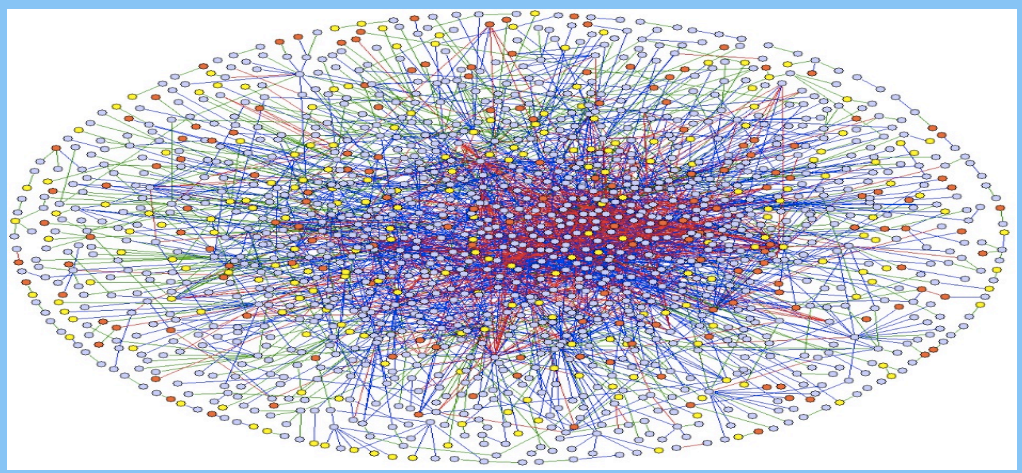


Problema della CLIQUE



Un problema di CLIQUE più grande

Trovare la clique più grande in un grafo di 100 nodi può richiedere fino a secoli di tempo di calcolo con una ricerca di tutte le possibilità.



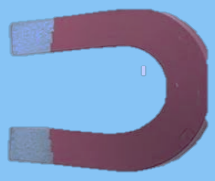
La ricerca esaustiva è necessaria ?
Non lo sappiamo.

Cercare un ago in un pagliaio

Trovato! Ci ho messo solo 10 giorni!

Cercare un ago…..

La ricerca esaustiva è necessaria?



No, se si ha a disposizione un magnete

Altri problemi difficili

- Scheduling
- Colorazione delle mappe
- Protein folding
- Isomorfismo di grafi
- Puzzle (Sudoku)
- Commesso viaggiatore
- Molti altri….

La questione di P e NP

Possiamo risolvere i problemi precedenti e altri che si risolvono facendo la ricerca esaustiva senza tale ricerca?

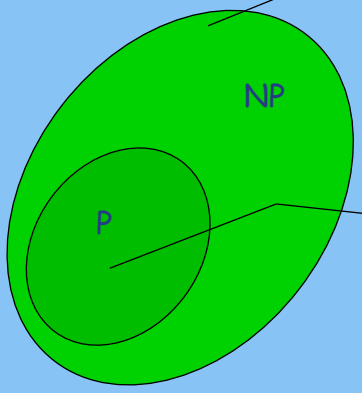
P e NP

- P "tempo Polinomiale"
  Problemi risolubili velocemente

- NP "tempo Non deterministico Polinomiale"
  Problemi verificabili velocemente

include i problemi precedenti

Le classi P e NP



Problemi facilmente verificabili

- Fattorizzazione
- K-Clique

Problemi facilmente risolvibili

- Moltiplicazione
- Ordinamento

P = NP

oppure

P ≠ NP

Storia recente della questione di P e NP

- 1960 Albori della teoria della complessità
  - Rabin, Blum, Hartmanis, Edmonds
- 1970 La questione di P e NP;NP-completezza
  - Cook, Levin,Karp

1956 Lettera di Gödel a Von Neuman
(scoperta negli anni 90)

- Anticipazione della questione P e NP

A volte la ricerca esaustiva può essere evitata

Test di primalità

Un modo strano per vedere se un numero è primo

Vecchio teorema. Per un primo p e a < p:

$a^{p-1} = 1 \pmod{p}$

Esempi:

p=7, a=2: $2^6 = 64 = 1 \pmod 7$

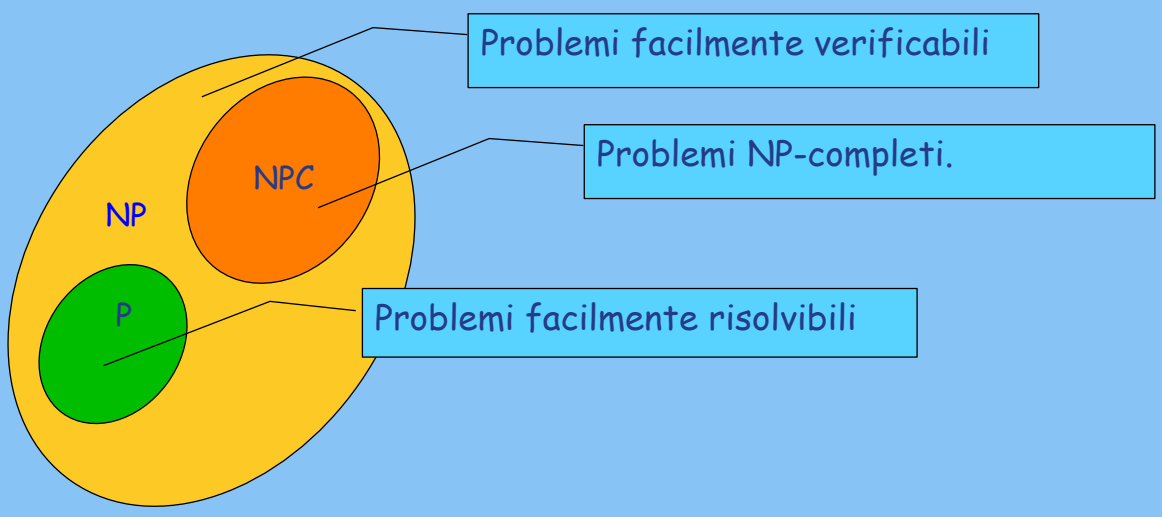
p=15, a=2: $2^{14} = 16.384 = 4 \neq 1 \pmod{15}$

quindi 15 non è primo!

I problemi "difficili" sono quasi tutti equivalenti

Se fossimo in grado di risolverne uno velocemente saremmo in grado di risolverli tutti

Le classi P , NP e NPC



Se un problema è NP-completo la speranza di trovare un algortimo efficiente è molto bassa!!

NP-completezza

Problemi NP-completi :

Se uno è facile allora tutti i problemi in NP sono facili!

Se uno è difficile allora tutti i problemi in NP sono difficili!

Clique:	NP-completo
Colorazione delle mappe:	NP-completo
Fattorizzazione:	non si sa

Migliaia di problemi NP-completi noti in Matematica, Biologia, Fisica, Economia,….

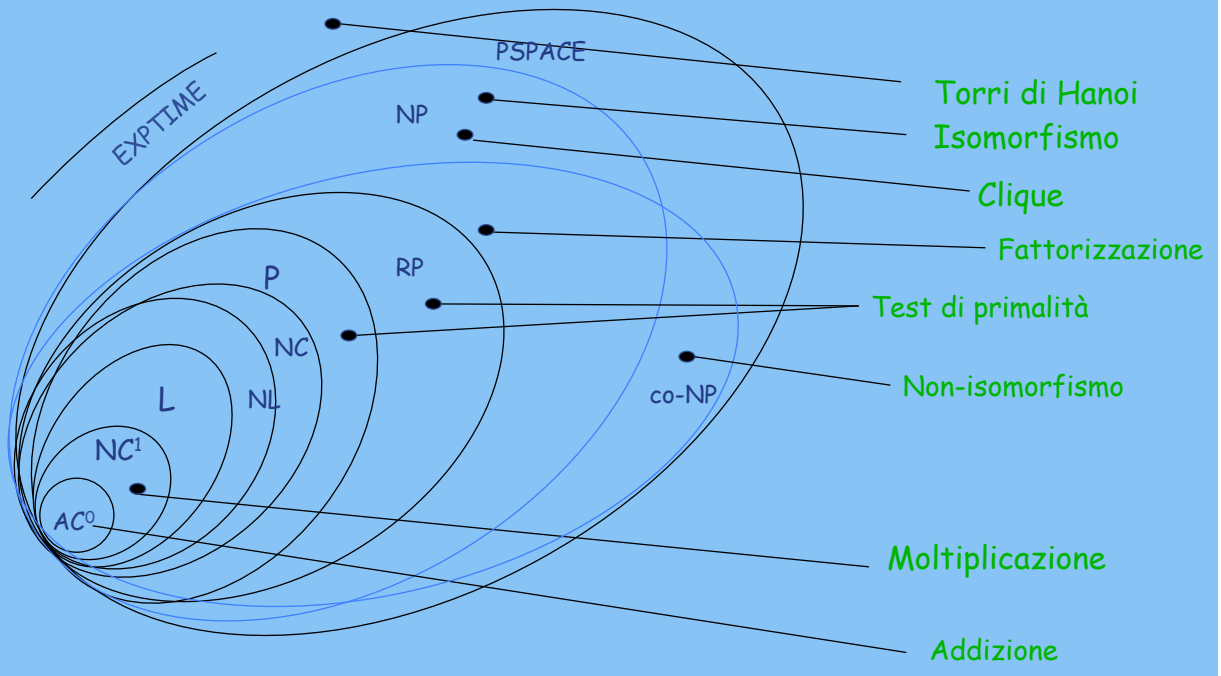
Protein Engineering vol. 7 no. 9 pp. 1059-1068, 1994
The protein threading problem with sequence amino acid interaction preferences is NP-complete
Richard H. Lathrop

Economic Theory vol. 23, no. 2 , pp. 445-454, 2004
Finding a Nash equilibrium in spatial games is NP-complete
R. Baron, J. Durieu, H. Haller and P. Solal

[math.GR] arXiv:0802.3839v1
Quadratic equations over free groups are NP-complete
O. Kharlampovich, I.G. Lysenok, A G Myasnikov N. Touikan

NP-completezza: segno di difficoltà.
Guida potenziale verso modelli e teorie migliori

Classi di complessità



Problemi:

Come provare che P ≠ NP ?

- Problema:
  Algoritmi molto sofisticati.

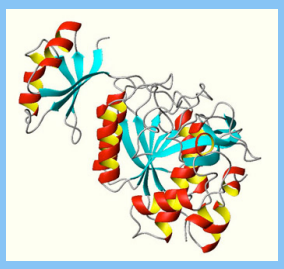
Bisognerebbe dimostrare che tutte le possibili strategie di risoluzione falliscono.

- Possibile strategie
  Limitare le capacità della macchina
  Individuare gli input difficili
  input di grandi dimensioni (tendenti all'infinito)

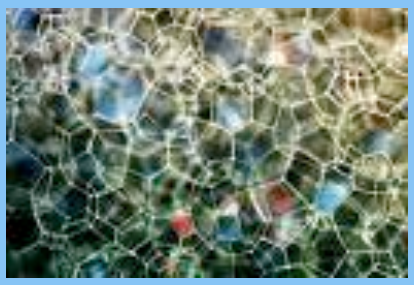
Cosa succede in natura?

Problemi NP-completi che la "natura risolve"

Biologia: Protein Folding — Minima energia



Fisica: Schiuma — Minima superficie



Economia: Equilibrio di Nash in giochi strategici

Possibilità:
Il modello è sbagliato o sono input speciali o P=NP

Novità: Scienze Naturali ⟷ Informatica

Conseguenze positive di P≠NP

P≠NP Alcuni dei problemi che vogliamo risolvere sono difficili.

I problemi difficili sono utili?

Crittografia: Se fattorizzazione è difficile:

- Codifica
- Firma digitale
- E-mail sicura
- Commercio elettronico
- Shopping on-line
- Poker on-line

Verrà mai risolto?

Servono nuove idee.

GRAZIE