P = NP?

Konstantin Tretjakov, EIO õppesessioon, 31.01.2015

Clay Mathematics Institute Prize

Millennium Problems

Yang–Mills and Mass Gap

Experiment and computer simulations suggest the existence of a "mass gap" in the solution to the quantum versions of the Yang-Mills equations. But no proof of this property is known.

Riemann Hypothesis

The prime number theorem determines the average distribution of the primes. The Riemann hypothesis tells us about the deviation from the average. Formulated in Riemann's 1859 paper, it asserts that all the 'non-obvious' zeros of the zeta function are complex numbers with real part 1/2.

P vs NP Problem

If it is easy to check that a solution to a problem is correct, is it also easy to solve the problem? This is the essence of the P vs NP question. Typical of the NP problems is that of the Hamiltonian Path Problem: given N cities to visit, how can one do this without visiting a city twice? If you give me a solution, I can easily check that it is correct. But I cannot so easily find a solution.

Navier–Stokes Equation

This is the equation which governs the flow of fluids such as water and air. However, there is no proof for the most basic questions one can ask: do solutions exist, and are they unique? Why ask for a proof? Because a proof gives not only certitude, but also understanding.

Hodge Conjecture

The answer to this conjecture determines how much of the topology of the solution set of a system of algebraic equations can be defined in terms of further algebraic equations. The Hodge conjecture is known in certain special cases, e.g. when the solution set has dimension less than four. But in

Mis teeb head mõistatust?

Näiteks,

see on, minu arust, tore mõistatus:

- Kaks jõge voolavad üksteise kõrval. Üks on valge, teine punane.

Mis teeb head mõistatust?

- Mõistatus on hea, kui
  - Selle lahendamiseks tuleb mõelda.
  - Teades vastust (mõnikord koos väikse tõestusega) me saame efektiivselt kindlaks teha, et vastus on tõepoolest õige.

“Halvad” ülesanded

“Halvad” ülesanded

Peatumisprobleem:

Ei ole võimalik teha algoritmi, mis ütleks *suvalise* etteantud programmi kohta, kas see programm kunagi peatub.

“Halvad” ülesanded

Rice’ teoreem:

Ei ole võimalik teha algoritmi, mis ütleks *suvalise* etteantud programmi kohta, kas temal on olemas omadus X.

Rice' teoreemi tõestus*

```
while True:
        do_something()

print("Hello, world")
```

Ülesannete hierarhia

- **Väga vastikud** (neid mille lahendamiseks võib-olla ei leidugi algoritmi)
- **„Mõistatused“** (neid mille puhul saab vastuse õigsust efektiivselt kontrollida)
- **„Lihtsad“** (neid, mille kohta me teame efektiivset lahendamisalgoritmi).

Ülesannete hierarhia

- **Undecidable**

- **Decidable**
- **EXPSPACE**
- **EXPTIME**
- **PSPACE**
- **NP**
- **P**
- **NC**
- **Context free**
- **Regular**

Ülesannete hierarhia

- **Undecidable**

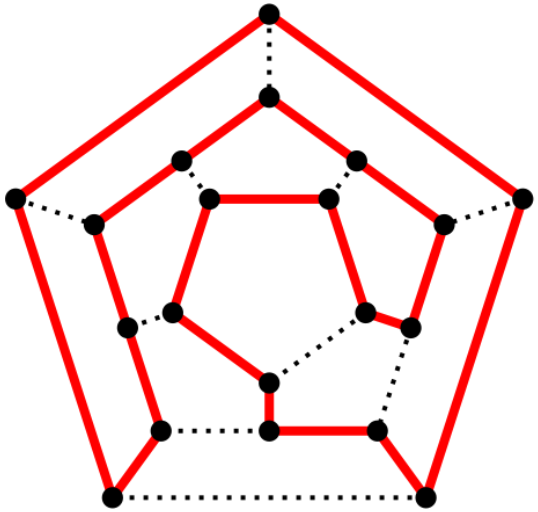
- **Decidable**
- **EXPSPACE**
- **EXPTIME**
- **PSPACE**
- **NP** ← „Mõistatused“
- **P** ← „Lihtsad“
- **NC**
- **Context free**
- **Regular**

NP ja P

NP-ülesanded on sellised, mille puhul **saab efektiivselt vastust kontrollida**.

NP ja P

NP-ülesanded on sellised, mille puhul **saab efektiivselt vastust kontrollida**.



8			4		6			7
						4		
	1					6	5	
5		9		3		7	8	
				7				
	4	8		2		1		3
	5	2					9	
		1						
3			9		2			5

NP ja P

NP-ülesanded on sellised, mille puhul **saab efektiivselt vastust kontrollida**.

P-ülesanded on sellised, mille puhul **saab efektiivselt vastust leida**.

NP ja P

Kas iga P ülesanne on ka NP ülesanne?

NP ja P

Kas iga NP ülesanne on ka P ülesanne?

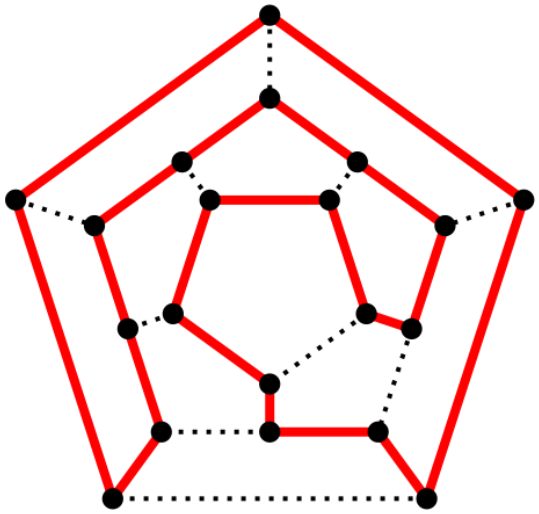
NP ja P

Kas iga NP ülesanne on ka P ülesanne?

Kuidas sellele vastata?

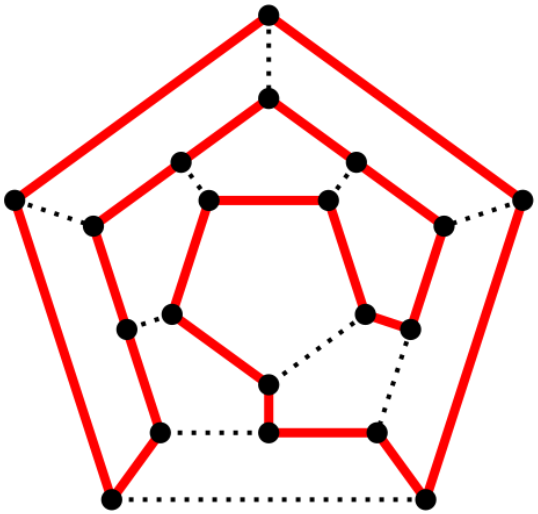
Kuidas sellele vastata?

Näiteks, Hamiltoni tee on üks NP-probleem.



Kui ma pakun vastusena tippude jada „a, b, c, d…“, siis saab efektiivselt kindlaks teha, et see jada on tõepoolest Hamiltoni tee.

Kuidas sellele vastata?



Selle kindlaks tegemine on sisuliselt järgmise loogilise avalduse verifitseerimine:

(a ühendatud b-ga) & (b ühendatud c-ga) &
… & a != b & a ! =c & … & y != z

SAT

- Aga me võiksime seega unustada Hamiltoni tee probleemist ning küsida hoopis lihtsalt seda, kas vastava avaldise jaoks:

  (a ühendatud b-ga) & (b ühendatud c-ga) &
  … & a != b & a ! =c & … & y != z

leidub mõni muutujate väärtustus (a, b, c…) mis teeb seda tõeseks.

Vaheküsimus

- Kas SAT on NP?
- Kas SAT on P?

SAT

- Kui me saaksime efektiivselt SAT probleemi lahendada, oleks meil automaatselt efektiivne viis ka Hamiltoni tee probleemi lahendamiseks.

- **Iga** NP probleemi puhul kehtib see, et selle „vastuse kontrollimise“ osa saab kirja panna loogilise avaldise kujul (saab teha isegi nii, et see avaldis sisaldaks ainult boolean-tüüpi muutujaid).

Kuidas sellele vastata?

Seega kui keegi leiutaks viisi SAT probleemi efektiivselt lahendada, saaksime me kohe **kõik** NP probleemid efektiivselt lahendada.

Kuidas sellele vastata?

Seega kui keegi leiutaks viisi SAT probleemi efektiivselt lahendada, saaksime me kohe **kõik** NP probleemid efektiivselt lahendada.

SAT ei ole tavaline NP ülesanne. Ta on **NP-täielik** ülesanne.

Kuidas sellele vastata?

Seega kui keegi leiutaks viisi SAT probleemi efektiivselt lahendada, saaksime me kohe **kõik** NP probleemid efektiivselt lahendada.

SAT ei ole tavaline NP ülesanne. Ta on **NP-täielik** ülesanne.

Cook'i teoreem

Kordame üle

- Mis asi on Rice' teoreem?
- Mis asi on Cook'i teoreem?
- Mis asi on NP?
- Mis asi on SAT?
- Kas Hamiltoni tee olemasolu kindlakstegemise problem on NP-täielik?
- Kas iga NP probleem on NP-täielik?
- Kui sa leiaksid SAT jaoks efektiivse lahenduse, kas sa võiksid pretendeerida Clay auhinnale?
- Millega seoses seal loengu alguses LEGO pilt oli?

Küsimus

- Kas sinu arust P = NP?
- Kas see on hea või halb?

Miks P != NP on hea

Avaliku võtme krüptograafia

Teeb kõigile kättesaadavaks

Avalik võti

Sina kasutad seda
et panka sisse logida

.. ning saadad avaliku võtmega
krüpteeritud sõnumeid

Avaliku võtme krüptograafia

Teeb kõigile kättesaadavaks

Avalik võti

Sina kasutad seda
et panka sisse logida

.. ning saadad avaliku võtmega krüpteeritud sõnumeid

Pank saab su sõnumit efektiivselt lahti krüpteerida kasutades „salajast võtit“.

Avaliku võtme krüptograafia

Teeb kõigile kättesaadavaks

Avalik võti

Sina kasutad seda
et panka sisse logida

.. ning saadad avaliku võtmega
krüpteeritud sõnumeid

Pank saab su sõnumit
efektiivselt lahti krüpteerida
kasutades „salajast võtit“.

Tänu P != NP-le töötavad

- HTTPS, SSL, SSH, TLS jne
- Digitaalsed signatuurid ja sertifikaadid
- ID-kaardid
- Tarkvara valideerimine
- E-valimised
- Bitcoin
- Digitaalne ajatembeldus
- Internet pokkerimängud ja muu selline

Küsimused?

$$P = NP$$

* *Kui N=1 või P=0*