Algoritmická (ne)rozhodnuteľnosť od Turinga po dnes

Michal mišof Forišek

Department of Theoretical Computer Science
Faculty of Mathematics, Physics and Informatics
Comenius University
Bratislava, Slovakia

September 2012

Zmena videnia nášho sveta

Pred Gödelom a Turingom

(Teda len pred 75-80 rokmi.)
Nádej v dokonalú matematiku, bezospornú, úplnú,
a v nej mechanické rozhodovanie pravdivosti tvrdení.

Po nich

Nikdy si nebudeme istí základmi matematiky.
Bezospornosť a úplnosť sa navzájom vylučujú.
Je nemožné mechanicky dokazovať, resp. generovať všetky pravdivé tvrdenia.

Zmena videnia nášho sveta

Pred Gödelom a Turingom

(Teda len pred 75-80 rokmi.)
Nádej v dokonalú matematiku, bezospornú, úplnú,
a v nej mechanické rozhodovanie pravdivosti tvrdení.

Po nich

Nikdy si nebudeme istí základmi matematiky.
Bezospornosť a úplnosť sa navzájom vylučujú.
Je nemožné mechanicky dokazovať, resp. generovať všetky pravdivé tvrdenia.

Pár slov o mechanickom dokazovaní

Dnešným aparátom to už vieme popísať prekvapivo ľahko.
Majme nejaký dostatočne silný* formálny systém.

- Čo je to dôkaz?
  Nejaký reťazec, ktorý vieme mechanicky „skontrolovať“.
  Teda: musí existovať rekurzívny predikát $JeDokaz(t, d)$.
  Potom ale je množina dokázateľných tvrdení rek. vyčísliteľná.
- Množina pravdivých tvrdení nie je rekurzívne vyčísliteľná.
  Redukciou z komplementu problému zastavenia:
  k danému stroju zostrojíme výrok
  „neexistuje k také, že náš stroj na k krokov zastane“.
- Dôsledok:
  bezospornosť $\Rightarrow$ existujú pravdivé nedokázateľné tvrdenia.

Pár slov o mechanickom dokazovaní

Dnešným aparátom to už vieme popísať prekvapivo ľahko.
Majme nejaký dostatočne silný* formálny systém.

- Čo je to dôkaz?
  Nejaký reťazec, ktorý vieme mechanicky „skontrolovať“.
  Teda: musí existovať rekurzívny predikát $JeDokaz(t, d)$.
  Potom ale je množina dokázateľných tvrdení rek. vyčísliteľná.
- Množina pravdivých tvrdení nie je rekurzívne vyčísliteľná.
  Redukciou z komplementu problému zastavenia:
  k danému stroju zostrojíme výrok
  „neexistuje k také, že náš stroj na k krokov zastane“.
- Dôsledok:
  bezospornosť $\Rightarrow$ existujú pravdivé nedokázateľné tvrdenia.

Pár slov o mechanickom dokazovaní

Dnešným aparátom to už vieme popísať prekvapivo ľahko.
Majme nejaký dostatočne silný* formálny systém.

- Čo je to dôkaz?
  Nejaký reťazec, ktorý vieme mechanicky „skontrolovať“.
  Teda: musí existovať rekurzívny predikát $JeDokaz(t, d)$.
  Potom ale je množina dokázateľných tvrdení rek. vyčísliteľná.
- Množina pravdivých tvrdení nie je rekurzívne vyčísliteľná.
  Redukciou z komplementu problému zastavenia:
  k danému stroju zostrojíme výrok
  „neexistuje k také, že náš stroj na k krokov zastane“.
- Dôsledok:
  bezospornosť $\Rightarrow$ existujú pravdivé nedokázateľné tvrdenia.

Kam sa šlo ďalej?

Za čias Turinga začalo delenie problémov na tie, ktoré idú riešiť algoritmicky, a tie, ktoré riešiť nejdú. Časom sa ukazuje jemnejšia škála na oboch stranách.

Za hranicou vypočítateľnosti

Aritmetická hierarchia: „čo by bolo, keby“
Problémy, ktoré vieme definovať v aritmetike prvého rádu.

Okolo hranice

Nie všetky čiastočne rozhodnuteľné problémy sú „rovnako ťažké“.
(Napr. simple sets – „jednoduché“ množiny.)

Kam sa šlo ďalej?

Pred hranicou vypočítateľnosti

Nová hlavná otázka:
Čo vieme riešiť *efektívne*?
(A čo je to vlastne efektívne riešenie, keď už sme pri tom?)

Prvý pokus o definíciu: polynomiálny čas

Výsledok:
1971 Cook: "The complexity of theorem proving procedures"
(SAT je NP-úplný, kladie otázku P=NP?)
1972 Karp: "Reducibility Among Combinatorial Problems"
(redukcie, 23 NP-úplných problémov)

Kam sa šlo ďalej?

Pred hranicou vypočítateľnosti

Nová hlavná otázka:
Čo vieme riešiť *efektívne*?
(A čo je to vlastne efektívne riešenie, keď už sme pri tom?)

Prvý pokus o definíciu: polynomiálny čas

Výsledok:
1971 Cook: "The complexity of theorem proving procedures"
(SAT je NP-úplný, kladie otázku P=NP?)
1972 Karp: "Reducibility Among Combinatorial Problems"
(redukcie, 23 NP-úplných problémov)

Je naozaj P = efektívne riešiteľné?

Nové prekvapenie

Nečakanú novú silu dáva možnosť použiť náhodné čísla.
(Najznámejšie praktické príklady: testovanie prvočíselnosti,
komunikačná zložitosť overenia zhody súborov,
odlíšenie počtu a a b konečným automatom.)

A ďalej a ďalej...

– ktoré problémy vieme efektívne paralelizovať?
– efektívne interaktívne dokazovanie, PCP, zero-knowledge
– ktoré problémy vieme riešiť online?
– kvantové algoritmy a iné nové modely

Je naozaj P = efektívne riešiteľné?

Nové prekvapenie

Nečakanú novú silu dáva možnosť použiť náhodné čísla.
(Najznámejšie praktické príklady: testovanie prvočíselnosti,
komunikačná zložitosť overenia zhody súborov,
odlíšenie počtu a a b konečným automatom.)

A ďalej a ďalej...

– ktoré problémy vieme efektívne paralelizovať?
– efektívne interaktívne dokazovanie, PCP, zero-knowledge
– ktoré problémy vieme riešiť online?
– kvantové algoritmy a iné nové modely

Chuťovka #1: Sila náhody

2PFA

Dvojsmerný konečný automat, read-only páska, minca.

Freivald, 1981

Rozpoznáme jazyk $\{a^n b^n : n \geq 0\}$.

- Vhodne zvolíme konštanty k, l.
- Overíme tvar a či $\#_a \equiv \#_b \pmod{k}$.
- Hráme turnaje s mincou.
- Ak niekto vyhrá $l : 0$, reject, inak accept.

Chuťovka #1: Sila náhody

2PFA

Dvojsmerný konečný automat, read-only páska, minca.

Freivald, 1981

Rozpoznáme jazyk $\{a^n b^n : n \geq 0\}$.

- Vhodne zvolíme konštanty k, l.
- Overíme tvar a či $\#_a \equiv \#_b \pmod{k}$.
- Hráme turnaje s mincou.
- Ak niekto vyhrá $l : 0$, reject, inak accept.

Chuťovka #1: Sila náhody

2PFA

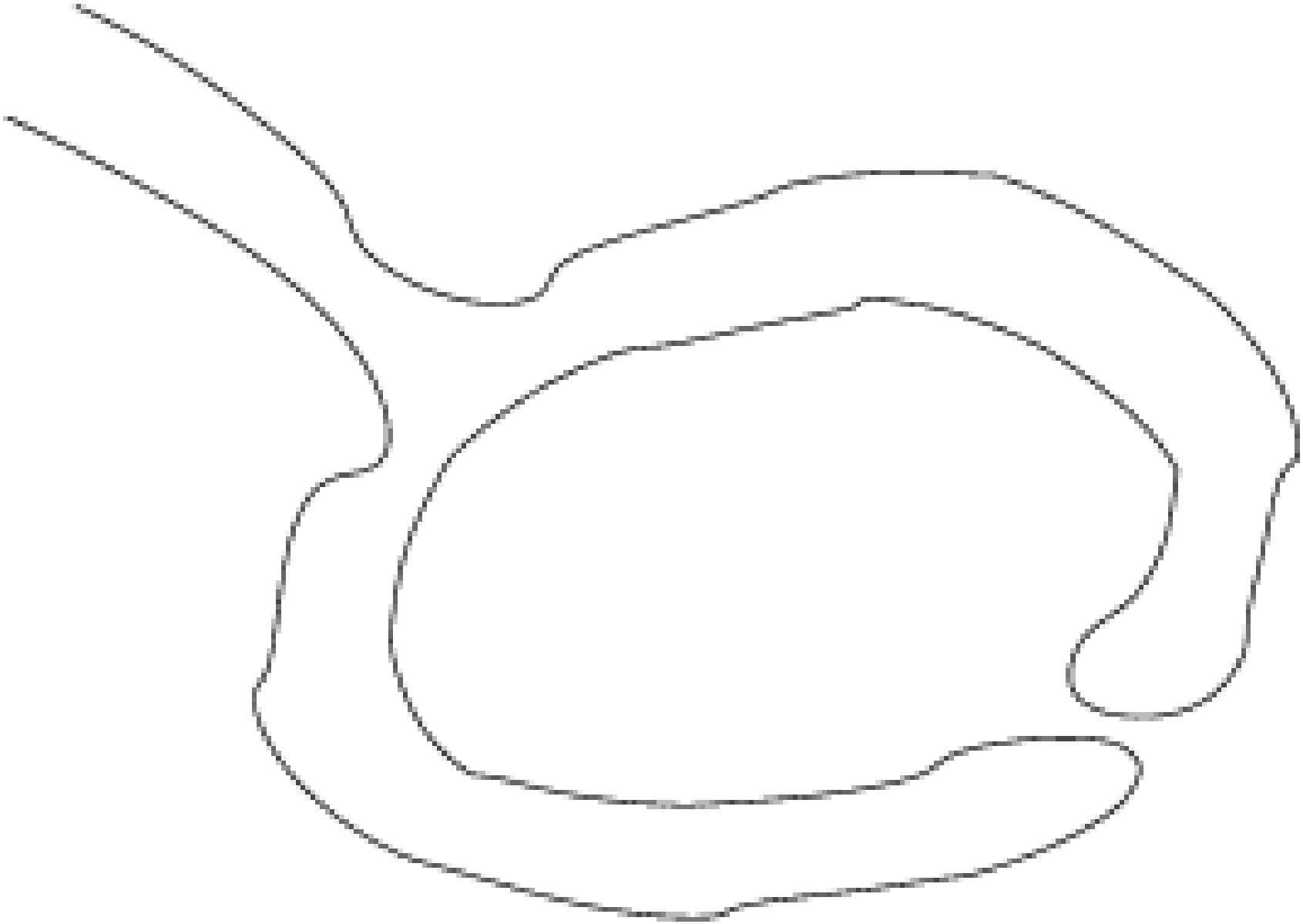
Dvojsmerný konečný automat, read-only páska, minca.

Freivald, 1981

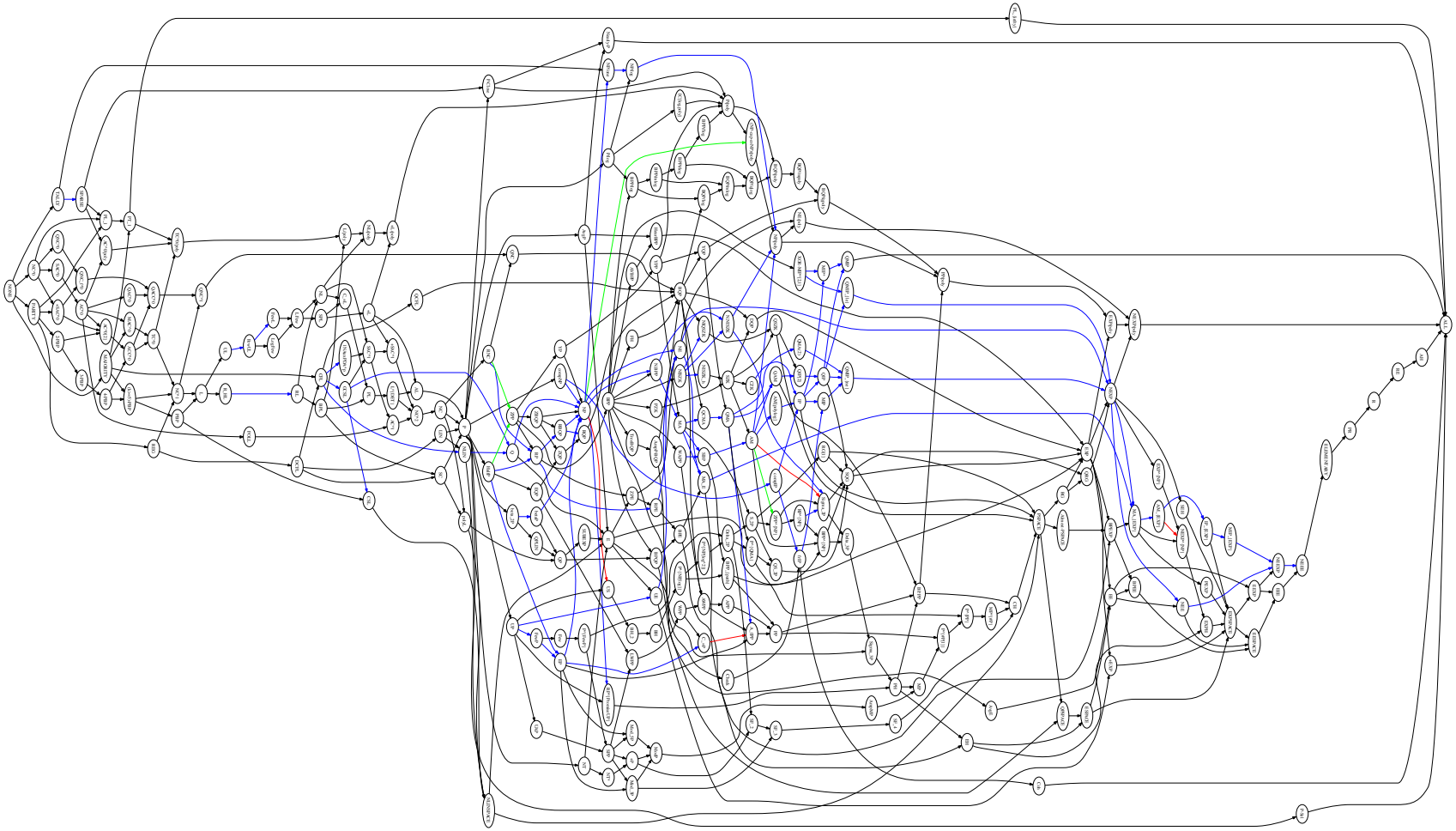
Rozpoznáme jazyk $\{a^n b^n : n \geq 0\}$.

- Vhodne zvolíme konštanty k, l.
- Overíme tvar a či $\#_a \equiv \#_b \pmod{k}$.
- Hráme turnaje s mincou.
- Ak niekto vyhrá $l : 0$, reject, inak accept.

Chuťovka #2: Zero knowledge



Complexity ZOO



Čo v takejto situácii?

Treba dobrých generálov :)

Kde treba najviac bojovať?

Zrejme posúvať hranicu *efektívnej* riešiteľnosti.

Čo v takejto situácii?

Treba dobrých generálov :)

Kde treba najviac bojovať?
Zrejme posúvať hranicu *efektívnej* riešiteľnosti.

Chuťovka #3: FPT a kernelizácia

Vertex cover

Mám n-vrcholový graf.
Chcem min. množinu vrcholov C incidentnú so všetkými hranami.
FPT otázka: existuje množina veľkosti k?

Kernelizácia

1. Izolovaný vrchol? Vyhodiť.
2. Vrchol stupňa $> k$? Použiť.
3. Ostalo viac ako k^2 hrán? Zamietnuť.
4. Hrubá sila.

(Lepšie algoritmy: kernel s $2k$ vrcholmi.)

Chuťovka #3: FPT a kernelizácia

Vertex cover

Mám n-vrcholový graf.
Chcem min. množinu vrcholov C incidentnú so všetkými hranami.
FPT otázka: existuje množina veľkosti k?

Kernelizácia

1. Izolovaný vrchol? Vyhodiť.
2. Vrchol stupňa $> k$? Použiť.
3. Ostalo viac ako k^2 hrán? Zamietnuť.
4. Hrubá sila.

(Lepšie algoritmy: kernel s $2k$ vrcholmi.)

Koniec

„Čínska kliatba“:
Kiež by si žil v zaujímavých časoch!

Zrejme máme túto smolu (či šťastie?)
Poďme do boja :)

Ďakujem za pozornosť!

Koniec

„Čínska kliatba“:
Kiež by si žil v zaujímavých časoch!

Zrejme máme túto smolu (či šťastie?)
Poďme do boja :)

Ďakujem za pozornosť!