Laički uvod u algoritamsku teoriju informacija

Mladen Nikolić

23. jun, 2010.

Overview

Overview

Izvori

- Gregory Chaitin, Meta Math!
- Gregory Chaitin, Algorithmic Information Theory

Tvorci

- Gregori Čejtin
- Andrej Kolmogorov
- Rej Solomonov
- ...

Teme

- Slučajnost
- Algoritamska složenost
- Nepotpunost aksiomatskih sistema
- ...

Motivacija

- Gedel — prve teoreme o nepotpunosti
- Tjuring — nepotpunost kao posledica neizracunljivosti
- Čejtin — nepotpunost i slučajnost

Filozofska poruka

- Matematika i nauka uopste traže strukturu i zakonitost u znanju i pojavama
- Istinitost tvrdnji ne mora imati nikakvog dubljeg razloga od nje same — ona može biti u nekom smislu slučajna!

Overview

Statistički pristup

- Kad je niska bitova "slučajna"?
- Ako prolazi statističke testove za uniformnu raspodelu?

Statistički pristup

- U svim primerima raspodele su uniformne:
- 0000000000000000000011111111111111111111
- 0101010101010101010101010101010101010101
- 0110001011011000111011110010011000100101
- Šta intuitivno doživljavamo kao slučajno?
- Zašto?

Niske mogu sadržati zakonitosti

- 0000000000000000000011111111111111111111
  (20 nula i 20 jedinica)
  for(i=0; i<20; i++) printf("0");
  for(i=0; i<20; i++) printf("1");

- 0101010101010101010101010101010101010101
  (20 puta 01)
  for(i=0; i<20; i++) printf("01");

- 0110001011011000111011110010011000100101
  (0110001011011000111011110010011000100101)
  printf("0110001011011000111011110010011000100101");

"Algoritamski" pristup

- Niska je slučajna ako se u njoj ne može primetiti zakonitost?
- Niska je slučajna ukoliko se ne može kompresovati?

Kolmogorovljeva složenost

- Kolmogorovljeva složenost: $K(s) = \min_{p()=s} |p|$
- L_1, L_2 — K_1, K_2
- $\forall s |K_1(s) - K_2(s)| < c$

Konačne slučajne niske

- Konačna niska s je slučajna ako

$$K(s) \geq |s|$$

- Ili bi trebalo $K(s) \geq |s| \pm c$?

Beskonačne slučajne niske

- Beskonačna niska s je slučajna ako postoji konstanta c tako da

$$\forall w(s = wp \Rightarrow K(w) \geq |w| - c)$$

Slučajnost i realni brojevi

- Na realan broj se može referisati sa verovatnoćom 0
- Realan broj je izračunljiv sa verovatnoćom 0
- Realan broj je slučajan sa verovatnoćom 1

Overview

Formalni aksiomatski sistem

- Formalni aksiomatski sistem opskrbljen programom koji proverava dokaze
- Složenost sistema je Kolmogorovljeva složenost programa koji nabraja teoreme dokazive u tom sistemu
- FAS predstavlja kompresovani zapis teorije

Elegantni programi

- Program p je elegantan ako nema manjeg programa koji daje isti izlaz $(K(p()) = |p|)$
- Problem "elegantnosti" je neodlučiv
- U okviru bilo kog FAS elegantnost se može dokazati samo za programe veličine najviše $K(FAS) + c$

Broj Ω

- Samoograničavajući (selfdelimiting) programi
- Broj Ω predstavlja verovatnoću zaustavljanja slučajno izabranog samoograničavajućeg programa

$$\Omega = \sum_{p\ se\ zaustavlja} \frac{1}{2^{|p|}}$$

Aproksimiranje broja Ω

- Neka je w_k aproksimacija koja se dobija tako što se pokrenu svi programi veličine najviše k u trajanju k koraka
- Svaki program veličine i koji se završi u tom vremenu doprinosi $\frac{1}{2^i}$ zbiru w_k
- $w_1 \leq w_2 \leq \ldots \leq \Omega$
- $w_k \rightarrow \Omega$ kada $k \rightarrow \infty$

Ω i halting problem

- Prvih n bitova broja Ω se mogu upotrebiti za rešavanje halting problema za programe veličine najviše n
  - Naći w_k takvo da je prvih n bitova te aproksimacije tačno
  - U tom trenutku su se završili svi programi dužine n koji se ikad završavaju

Ω je slučajan broj

- Program koji bi mogao da izračuna prvih n bitova broja Ω bi se mogao dopuniti sa c bita tako da izvrši prethodnu proceduru i da potom proizvede izlaz koji nije proizveo ni jedan od programa koji su se izvršili
- Taj izlaz nije mogao proizvesti ni jedan program veličine manje ili jednake n
- Stoga je složenost svakog programa koji proizvodi prvih n bitova broja Ω veća od $n - c$
- Takođe, ni u jednom aksiomatskom sistemu nije moguće odrediti više od $K(FAS) + c$ bitova broja Ω

Overview

Zaključak

- Bitovi broja Ω su direktno povezani sa zaustavljanjem programa
- Postoje značajna matematička tvrđenja u čijoj istinitosti nema zakonitosti ili dubljih razloga — čija se struktura čak može okarakterisati kao slučajna