SEMINARAS

2019 gegužės 14 d. 09:00, SRL-I 420

Jevgenijus Kirjackis

Apie sveikųjų skaičių daugybos algoritmus

Daugindami du n-skaitmenų skaičius įprastu mokykliniu stulpelio metodu naudojame n^2 daugybos operacijų. 1956 m. A. N. Kolmogorovas iškėlė hipotezę, jog bet kurio n-skaitmenų skaičių daugybos metodo apatinis sudėtingumo įvertis yra $\Omega(n^2)$, t.y greičiau sudauginti nepavyks ir "standartinis" metodas yra asimptotiškai optimalus. 1960 m A.N. Kolmogorovo vadovaujamame seminare "Matematinės problemos kibernetikoje", šita hipotezė buvo dar kartą įgarsinta. 23-jų metų amžiaus aspirantas Anatolijus Karacuba, panaudojus *skaldyk ir valdyk* metodą, atrado elegantišką sveikųjų skaičių daugybos algoritmą sudėtingumo $O\left(n^{\log_2 3}\right) \approx O\left(n^{1{,}59}\right)$ ir A.N. Kolmogorovo hipotezė buvo paneigta. Kai paaiškėjo, kad "natūralioji" asimptotika $\Omega(n^2)$ nėra apatinis įvertis dviejų n-skaitmenų skaičių sandaugai, matematikai pradėjo ieškoti dar greitesnių algoritmų. 1971 m Arnold Schönhage ir Volker Strassen publikuoja straipsnį, kuriame pritaiko jau tuo metu žinoma (Cooley ir Tukey, 1965) greitąją Furje transformaciją, kurios sudėtingumas $O\left(n\log n\right)$, sveikųjų skaičių daugybai ir pasiekia greičio $O\left(n\log n\cdot \log\log n\right)$. Be to jie suformulavo naują hipotezę apie tai, kad neįmanoma rasti algoritmo n-skaitmenų skaičių daugybai greitesnio už $O\left(n\log n\right)$. Martin Fürer (2007) dar šiek tiek priartino skaičių daugybos algoritmo greitį prie, galimai, apatinės ribos $O\left(n\log n\right)$. Jo algoritmas yra $O\left(n\log n\cdot 2^{O\left(\log^* n\right)}\right)$ sudėtingumo. Covanov and Thomé (2016) pristatė algoritmą sudėtingumo $O\left(n\log n\cdot 2^{2\log^* n}\right)$.

2019-03-18 sveikųjų skaičių daugybos algoritmas sudėtingumo $O\left(n\log n\right)$ matematikų bendruomenės vertinimui pateikė David Harvey and Joris van der Hoeven (https://hal.archives-ouvertes.fr/hal-02070778/document).

Kviečiame dalyvauti.
Seminaro sekretorius A. Bugajev