SEMINARAS

2013 rugsėjo 17 d. 8:45, SRL-I 402 kab.

Raimondas Čiegis

"Kvantiniai algoritmai - kaip sprendžiami neišsprendžiami uždaviniai".

Šiame seminare pratęsime kvantinių algoritmų analizę.

Šią vasarą apie kvantinius kompiuterius pasklido daug naujos informacijos, apie jų galimybes rašo, kalba ir rodo visos svarbiausios informacijos sklaidos priemonės. Taigi naują metinį seminarų ciklą pradėsime kvantinių algoritmų analize.

Paskaitoje susipažinsime su dviejų svarbių uždavinių kvantiniais sprendimo algoritmais. Pateiksime tik pagrindinę informaciją, o algoritmų realizavimo detales panagrinėsime kituose seminaruose.

1. Pirmasis uždavinys - sveikojo skaičiaus skaidymas į pirminių skaičių sandaugą. Šiuolaikinės matematikos metodais toks uždavinys sprendžiamas labai neefektyviai, ir tai gera žinia - nes populiarusis kriptografinis RSA algoritmas yra saugus kaip tik todėl, kad niekas negali apskaičiuoti atvirai paskelbto kodavimo rakto slaptosios dalies (žinomais metodais uždavinys būtų išspręstas tada, kai ši informacija niekam jau nebus įdomi) .

Tačiau taip yra tik iki tol, kol kažkam pavyks sukonstruoti pakankamai stabiliai veikiantį kvantinį kompiuterį. Susipažinsime su Shoro algoritmu, kuriame panaudota visai kita strategija skaičiui skaidyti į pirminius daugiklius. Ji netinkama įprastiniams kompiuteriams, bet puikiai išnaudoja kvantinių kompiuterių savybes. Gaunamas eksponentinis algoritmo sudėtingumo pagreitėjimas. Kaip tik paskelbus Shoro algoritmą ir prasidėjo kvantinių skaičiavimų tematikos ažiotažas.

2. Antrasis uždavinys - informacijos paieška nesutvarkytoje duomenų aibėje. Visų žinomų algoritmų sudėtingumas yra *O(N)* eilės, jei *N* yra duomenų kiekis. Ir vėl kuriami "kvantiniai algoritmai", kurie visai neperspektyvūs naudojant įprastinius kompiuterius. Kol kas uždavinio sudėtingumą pavyksta sumažinti tik iki $O(\sqrt{N})$, bet šis "tik" reiškia milijonus kartų greitesnę informacijos paiešką svarbių milžiniškų šiuolaikinių duomenų saugyklų analizėje.

Seminaro pabaigoje suformuluosime planą temų, kurios bus nagrinėjamos kitose specializuotose šios tematikos paskaitose.

Kviečiame dalyvauti.
Seminaro sekretorius A. Bugajev