SEMINARAS

„Kvantinio Shoro algoritmo klasikinė matematinė analizė“

Raimondas Čiegis

2025 m. balandžio 8 d.

09:00 val. S6(SRL-I) 502

Kvantiniai skaičiavimai "kelia" dideles bangas šiuolaikinių skaičiavimo algoritmų ir technologijų pasaulyje. Galėtume pasirinkti ne vieną kvantų tematiką, kurios užpildė HPC ir virtualaus modeliavimo mokslinius žurnalus, socialinius tinklus ir net pakeitė šeimininkių pokalbių tematiką populiariuose Vilniaus turguose. Taigi universitetuose matematikams jau kaip ir būtina tapti "raštingais" kvantinių algoritmų teorijoje (o dar geriau ir skaičiavimo įgūdžių srityje). Norėdami Jums palengvinti šį studijų procesą planuojame organizuoti seriją dirbtuvių/paskaitų, skirtų kvantiniams skaičiavimams.

Ko neplanuojame – supažindinti su technogeninėmis kvantų naujienomis. Jos atsiranda vos ne kiekvieną savaitę, pažadai ir prognozės fantastiški, o gražios ateities riba artėja labai greitai (kai kada man atrodo, kad jau kalbame apie "vakar"). Taip pat neplanuojame detaliai nagrinėti kvantinių duomenų perdavimo technologijų ir labai sudėtingų kvantinių procesų simuliacijos naudojant realaus dydžio kvantinių kubitų rinkinius (nors kaip tik šioje srityje ir yra gauti pagrindiniai kvantinių skaičiavimų pranašumo prieš klasikinius kompiuterius rezultatai – jų palyginimas yra "nesuvokiamai nepalyginamas").

Mes nagrinėsime kvantiniais vartais grindžiamus universaliuosius algoritmus (ne, ne Excel lentelių čia nebus). Pirmojo seminaro tikslas yra detaliai aptarti kvantinį Shoro algoritmą, kuris skirtas labai didelių sveikųjų skaičių faktorizavimui. Na, kad kalbėtume ne filologiškai, imkime skaičių N, kurio didumo eilė 2^2048. Kiek laiko reikėtų uždavinio sprendimui naudojant greičiausius faktorizavimo algoritmus ir galingiausius dabartinius lygiagrečiuosius super-kompiuterius? Kaip sudarytas legendinis Shoro algoritmas, kuris ir sujudino visą skaitmeninių technologijų pasaulį 1995 metais? O tai ir yra dabartinis virtualus skaitmeninis pasaulis, kuriame gyvename, dirbame, planuojame, ilsimės ir svajojame? Keli kertiniai momentai:

1. Algoritmas tikrai nebuvo naujas, jis buvo žinomas mažiausiai 25 metus.
2. Kaip dažnai matome šiuolaikinės matematikos taikymuose, naudojami skaičių teorijos/algebros gerai žinomi ir klasikiniai rezultatai.
3. Pirmas kvantinis etapas – skaičiuoti netiesinės funkcijos reikšmes labai didelėje aibėje taškų. Kvantiniai kompiuteriai tai moka atlikti labai, labai greitai, tai gerai žinoma kvantinių kompiuterių savybė.
4. Netikėta naujovė – algoritmo realizacijai pasitelkti Diskrečiąją Furje transformaciją bei jos greitąją versiją FFT. FFT yra daug greitesnė už DFT, bet visgi ir ji spręstų reikalingus uždavinius vėžlio greičiu, toks algoritmas yra nekonkurencingas lyginant jį su geriausiais faktorizavimo algoritmais. Bet Shoras naudoja kvantinę FT (QFT). Nesijaudinkite – jos apibrėžimas ir greitosios versijos beveik sutampa su DFT ir FFT. Bet kvantinis rezultatas gaunamas esmingai, esmingai greičiau.
5. Tada atliekame gautojo rezultato matavimą (taip, čia jau negalime pabėgti nuo legendinių kvantinių matavimų savybių, niuansų ir paradoksų).

6. Skaičiavimus užbaigiame naudodami įprastinius kompiuterius ir tai nėra didelio masto skaičiavimai. Vėl imsime gerai žinomus matematinius algoritmus.

Reziumė – kai tik kvantiniai kompiuteriai pradės stabiliai veikti, visa mūsų kasdieninė kriptografija taps "vaikų žaidimu". Beje, svarbi tema, kaip programuoti kvantinius kompiuterius? Tai irgi labai įdomi tema, tikiuosi, kad jai atsiras laiko kituose seminaruose.

Kviečiame visus atvykti į mokslinę diskusiją/dirbtuves.

Kviečiame dalyvauti.
Seminaro sekretorius A. Bugajev