Kokie buvo 2021 – kvantinių skaičiavimų naujienos ir legendos

R. Čiegis

Vilniaus Gedimino technikos universitetas
e-mail: rc@vgtu.lt

Vasario 8 d., 2022, Vilnius

Pasibaigė 2021 metai, įdomu pažvelgti, kokias naujienas jie atnešė.

Prisiminkime pagrindinius klausimus, kurie visada užduodami, kai kalbame apie kvantinius skaičiavimus:

1. Ar galime užtikrintai teigti, kad jau pateikti eksperimentiniai rezultatai, patvirtinantys kvantinių kompiuterių esminę viršenybę (supremacy) lyginant su tradiciniais superkompiuteriais?

2. Kiek kubitų (qubits) yra naudojama didžiausiame kvantiniame kompiuteryje?

3. Kiek laiko be klaidų gali skaičiuoti šiuolaikiniai kvantiniai kompiuteriai (triukšmų prakeiksmas)?

Gerai žinome, kad:

1. Kvantinių skaičiavimų teorijos optimistiniai kompiuterių pajėgumų įverčiai leidžia tikėtis tokio skaičiavimų masto (eksponentinis $O(2^p)$ įvertis), kuris leistų naudoti UNIKALIAS technologijas ir servisus. Tai užpildys tikru turiniu skaitmeninio pasaulio, didžiųjų duomenų analizės, dirbtinio intelekto ir personalių (jums asmeniškai pritaikytų) servisų pažadus.

2. Šia linkme nukreiptos milžiniškos investicijos, nors didžioji dalis specialistų prognozuoja, kad labiausiai tikėtina, jog universalieji kvantiniai kompiuteriai atsiras tik po 15-20 metų (na, na, ar tikrai taip negreit?).

2. Šia linkme nukreiptos milžiniškos investicijos, nors didžioji dalis specialistų prognozuoja, kad labiausiai tikėtina, jog universalieji kvantiniai kompiuteriai atsiras tik po 15-20 metų (na, na, ar tikrai taip negreit?).

Palyginimui priminsiu, kad tiesioginės investicijos 2015 metais siekė 93 milijonus, 2019 metais – 187 milijonus, o 2021 – 1 milijardą eurų.

2. Šia linkme nukreiptos milžiniškos investicijos, nors didžioji dalis specialistų prognozuoja, kad labiausiai tikėtina, jog universalieji kvantiniai kompiuteriai atsiras tik po 15-20 metų (na, na, ar tikrai taip negreit?).

Palyginimui priminsiu, kad tiesioginės investicijos 2015 metais siekė 93 milijonus, 2019 metais – 187 milijonus, o 2021 – 1 milijardą eurų.

Prognozuojama, kad per sekančius kelis metus šios sumos augs iki 3-5 milijardų kasmet.

Quantum advantage – viršenybė

Išvardinsime pavyzdžius svarbių universalių uždavinių, kuriuos spręs kvantiniai kompiuteriai. Taip bus vertinamas jau pasiektas potencialas keisti mūsų įprastines veiklas:

Quantum advantage – viršenybė

Išvardinsime pavyzdžius svarbių universalių uždavinių, kuriuos spręs kvantiniai kompiuteriai. Taip bus vertinamas jau pasiektas potencialas keisti mūsų įprastines veiklas:

1. Kriptografija. Spręsti sveikųjų skaičių faktorizavimo ir diskrečiojo logaritmo skaičiavimo uždavinius, taip eliminuojant populiariausius šiuolaikinius viešojo rakto kriptografijos algoritmus.

Quantum advantage – viršenybė

Išvardinsime pavyzdžius svarbių universalių uždavinių, kuriuos spręs kvantiniai kompiuteriai. Taip bus vertinamas jau pasiektas potencialas keisti mūsų įprastines veiklas:

1. Kriptografija. Spręsti sveikųjų skaičių faktorizavimo ir diskrečiojo logaritmo skaičiavimo uždavinius, taip eliminuojant populiariausius šiuolaikinius viešojo rakto kriptografijos algoritmus.

2. Optimizavimas. Globaliojo optimizavimo NP klasės uždavinių sprendimas, taikymai logistikoje, dirbtinio intelekto metoduose, robotikoje.

Quantum advantage – viršenybė

Išvardinsime pavyzdžius svarbių universalių uždavinių, kuriuos spręs kvantiniai kompiuteriai. Taip bus vertinamas jau pasiektas potencialas keisti mūsų įprastines veiklas:

1. Kriptografija. Spręsti sveikųjų skaičių faktorizavimo ir diskrečiojo logaritmo skaičiavimo uždavinius, taip eliminuojant populiariausius šiuolaikinius viešojo rakto kriptografijos algoritmus.

2. Optimizavimas. Globaliojo optimizavimo NP klasės uždavinių sprendimas, taikymai logistikoje, dirbtinio intelekto metoduose, robotikoje.

3. Finansų matematika. Finansų rinkos, kriptovaliutos, ekonomika.

Situacija 2020 metų pabaigoje:

Google kvantinis kompiuteris ir lūžis skaičiavimuose

Situacija 2020 metų pabaigoje:

Google kvantinis kompiuteris ir lūžis skaičiavimuose

On October 23, 2019, John M. Martinis and his team published a paper on Nature with title "Quantum supremacy using a programmable superconducting processor", where they presented how they achieved quantum supremacy for the first time using a 53-qubits quantum computer.

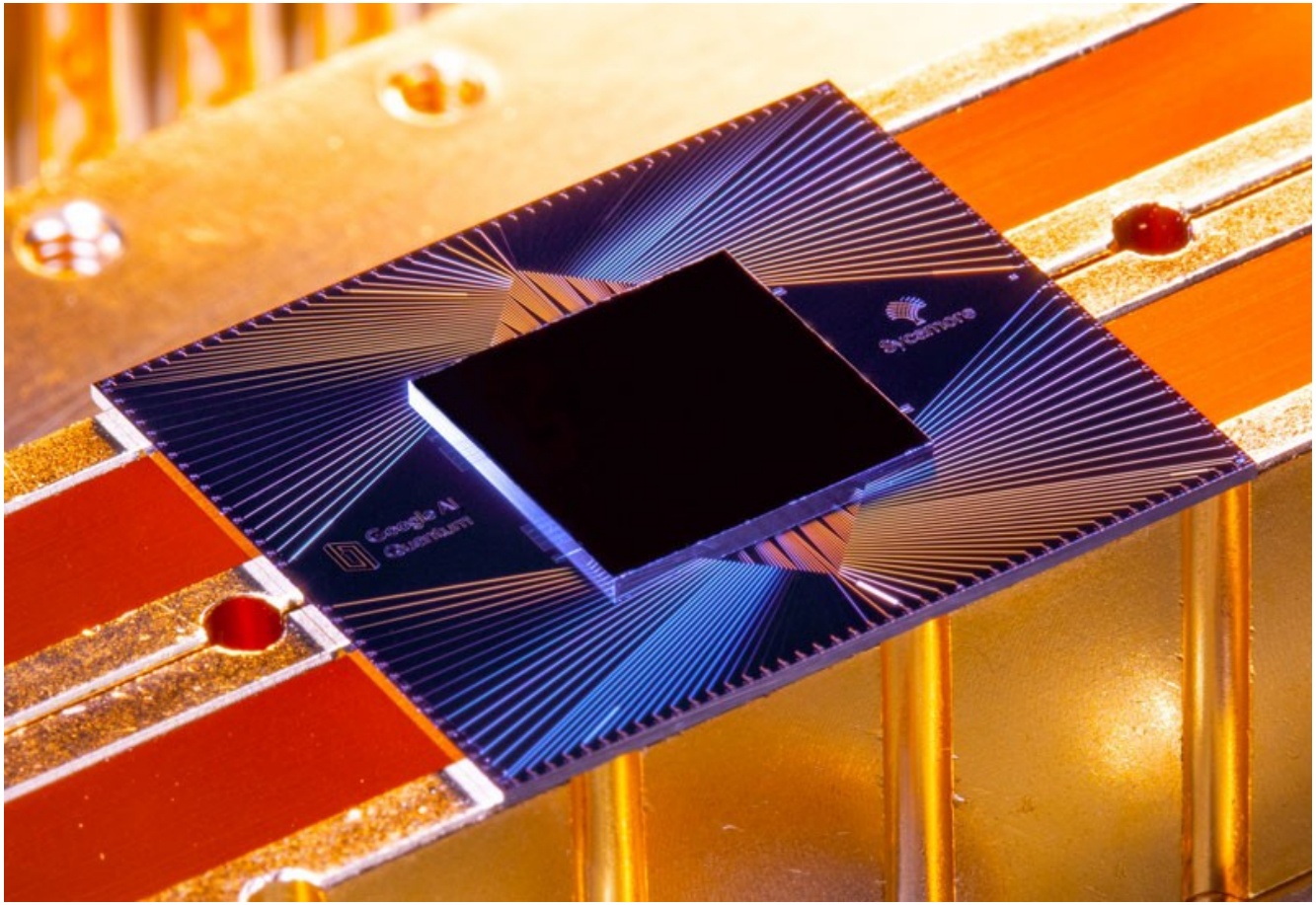

Fig1. Sycamore procesorius (chip)

Paskelbta, kad per 200 sekundžių buvo išspręstas specialus milžiniškos apimties modeliavimo uždavinys, kurį šiuolaikiniai superkompiuteriai spręstų 10 000 metų.

Tai pirmasis eksperimentas, parodęs, kad kvantiniai greičiai yra tikrai pasiekiami naudojant jau egzistuojančius kvantinius kompiuterius.

Paskelbta, kad per 200 sekundžių buvo išspręstas specialus milžiniškos apimties modeliavimo uždavinys, kurį šiuolaikiniai superkompiuteriai spręstų 10 000 metų.

Tai pirmasis eksperimentas, parodęs, kad kvantiniai greičiai yra tikrai pasiekiami naudojant jau egzistuojančius kvantinius kompiuterius.

Aišku, kad buvo išsakyta gausybė abejonių: o, bet, tačiau, tik, klaidos vertinant, klaidos neteisingai interpretuojant ir t.t.

Paskelbta, kad per 200 sekundžių buvo išspręstas specialus milžiniškos apimties modeliavimo uždavinys, kurį šiuolaikiniai superkompiuteriai spręstų 10 000 metų.

Tai pirmasis eksperimentas, parodęs, kad kvantiniai greičiai yra tikrai pasiekiami naudojant jau egzistuojančius kvantinius kompiuterius.

Aišku, kad buvo išsakyta gausybė abejonių: o, bet, tačiau, tik, klaidos vertinant, klaidos neteisingai interpretuojant ir t.t.

Pvz. IBM specialistai tvirtino, kad Google testo uždavinį, pakeitus matematinį sprendimo algoritmą, galima išspręsti šiuolaikiniais kompiuteriais per 60 valandų. Beje, šis pranešimas nebuvo skelbtas recenzuojamame žurnale.

Paskelbta, kad per 200 sekundžių buvo išspręstas specialus milžiniškos apimties modeliavimo uždavinys, kurį šiuolaikiniai superkompiuteriai spręstų 10 000 metų.

Tai pirmasis eksperimentas, parodęs, kad kvantiniai greičiai yra tikrai pasiekiami naudojant jau egzistuojančius kvantinius kompiuterius.

Aišku, kad buvo išsakyta gausybė abejonių: o, bet, tačiau, tik, klaidos vertinant, klaidos neteisingai interpretuojant ir t.t.

Pvz. IBM specialistai tvirtino, kad Google testo uždavinį, pakeitus matematinį sprendimo algoritmą, galima išspręsti šiuolaikiniais kompiuteriais per 60 valandų. Beje, šis pranešimas nebuvo skelbtas recenzuojamame žurnale.

Tik laikas, bei tolimesni entuziastų, optimistų rezultatai galės išsklaidyti šiuos rimtus argumentus.

Sulaukėme 2021 metų.

Liepos 10, 2021 Kinijos mokslininkų grupė paskelbė naujausius rezultatus.

Liepos 10, 2021 Kinijos mokslininkų grupė paskelbė naujausius rezultatus.
Jie sukonstravo 2D programuojamą kvantinį kompiuterį Zuchongzhi, kuriame integruoti 66 kubitai.

Liepos 10, 2021 Kinijos mokslininkų grupė paskelbė naujausius rezultatus.
Jie sukonstravo 2D programuojamą kvantinį kompiuterį Zuchongzhi, kuriame integruoti 66 kubitai.
Tai 12 kubitų daugiau, nei Google kompiuteryje (teorinis galingumas padidėjo 4096 kartus).

Liepos 10, 2021 Kinijos mokslininkų grupė paskelbė naujausius rezultatus.
Jie sukonstravo 2D programuojamą kvantinį kompiuterį Zuchongzhi, kuriame integruoti 66 kubitai.
Tai 12 kubitų daugiau, nei Google kompiuteryje (teorinis galingumas padidėjo 4096 kartus).

In their demonstration, the researchers used only 56 of those qubits to tackle a well-known computer problem–sampling the output distribution of random quantum circuits. The task requires a variety of computer abilities that involve mathematical analysis, matrix theory, the complexity of certain computations and probability theory.

Liepos 10, 2021 Kinijos mokslininkų grupė paskelbė naujausius rezultatus.
Jie sukonstravo 2D programuojamą kvantinį kompiuterį Zuchongzhi, kuriame integruoti 66 kubitai.
Tai 12 kubitų daugiau, nei Google kompiuteryje (teorinis galingumas padidėjo 4096 kartus).

In their demonstration, the researchers used only 56 of those qubits to tackle a well-known computer problem–sampling the output distribution of random quantum circuits. The task requires a variety of computer abilities that involve mathematical analysis, matrix theory, the complexity of certain computations and probability theory.
A task approximately 100-300 times more challenging than the one carried out by Sycamore in 2019.

This task would take a conventional supercomputer approximately eight years to complete.

This task would take a conventional supercomputer approximately eight years to complete.

Zuchongzhi completed the task in less than an hour and a half.

This task would take a conventional supercomputer approximately eight years to complete.

Zuchongzhi completed the task in less than an hour and a half.

Matome labai svarbią žinią – kvantiniai skaičiavimai tampa fundamentinio mokslo dalimi – skirtingos grupės, laboratorijos, mokslininkai pakartoja ir patikslina ankstesnius eksperimentus.

This task would take a conventional supercomputer approximately eight years to complete.

Zuchongzhi completed the task in less than an hour and a half.

Matome labai svarbią žinią – kvantiniai skaičiavimai tampa fundamentinio mokslo dalimi – skirtingos grupės, laboratorijos, mokslininkai pakartoja ir patikslina ankstesnius eksperimentus.

The Zuchongzhi machine is capable of tackling more than just one kind of task – a big step closer to real general purpose quantum computers.

This task would take a conventional supercomputer approximately eight years to complete.

Zuchongzhi completed the task in less than an hour and a half.

Matome labai svarbią žinią – kvantiniai skaičiavimai tampa fundamentinio mokslo dalimi – skirtingos grupės, laboratorijos, mokslininkai pakartoja ir patikslina ankstesnius eksperimentus.

The Zuchongzhi machine is capable of tackling more than just one kind of task – a big step closer to real general purpose quantum computers.

It also showed that adding just three more qubits than that used by Sycamore could increase the power of a quantum computer exponentially.

More importantly, it demonstrates that computer scientists are moving ever closer to the real prize–the development of a generalized quantum computer that can be used for a set of real-world applications that traditional computers will never be able to handle.

More importantly, it demonstrates that computer scientists are moving ever closer to the real prize–the development of a generalized quantum computer that can be used for a set of real-world applications that traditional computers will never be able to handle.

Reziumuojant, yra vertinama, kad Kinijos kvantinis kompiuteris yra maždaug 1 000 000 kartų galingesnis už Google kompiuterį (įspūdingas tik 2 metų šuolis).

Lenktynėse tarp JAV ir Kinijos lyderiai aiškiai pasikeitė.

Lenktynėse tarp JAV ir Kinijos lyderiai aiškiai pasikeitė.

Bet tai dar ne 2021 metų pasakojimo pabaiga.

2021 lapkričio mėnesį IBM paskelbė informaciją, kad jie sukonstravo 127-kubitų kvantinį superkompiuterį Eagle.

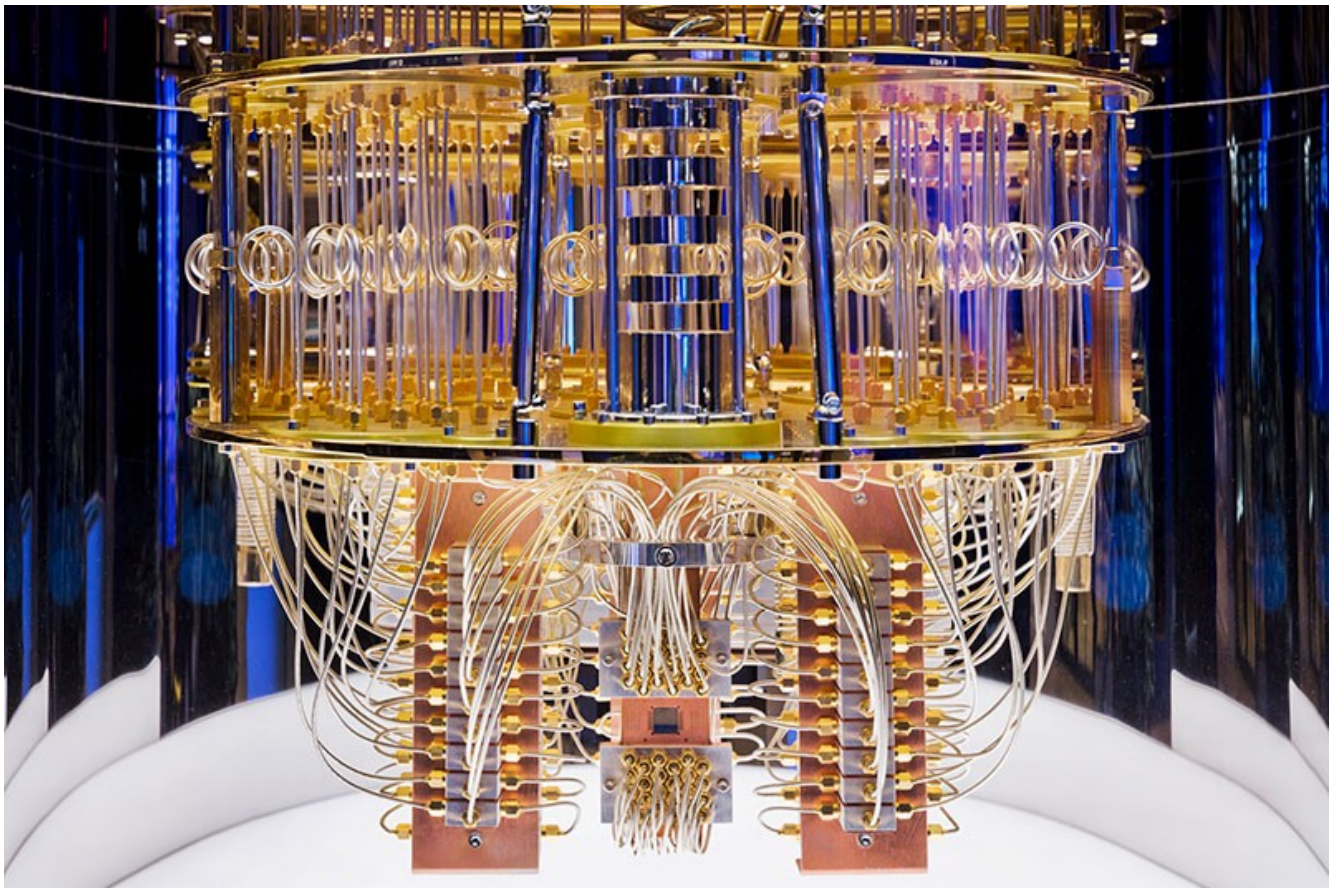

Fig2. Eagle procesorius (chip)

Kubitų realizacijai vėl panaudota superlaidumo technologija.

Kubitų realizacijai vėl panaudota superlaidumo technologija.

Kubitų skaičius padidėjo dvigubai, taigi galingumo šuolis yra milžiniškas – daugiklis $O(2^{64})$ kartų.

Kubitų realizacijai vėl panaudota superlaidumo technologija.

Kubitų skaičius padidėjo dvigubai, taigi galingumo šuolis yra milžiniškas – daugiklis $O(2^{64})$ kartų.

Kol kas IBM nepateikė skaičiavimo eksperimentų rezultatų. Laukiama, kad jie irgi turėtų išspręsti tą patį uždavinį, kaip ir Google bei USTC mokslininkų grupės.

Kubitų realizacijai vėl panaudota superlaidumo technologija.

Kubitų skaičius padidėjo dvigubai, taigi galingumo šuolis yra milžiniškas – daugiklis $O(2^{64})$ kartų.

Kol kas IBM nepateikė skaičiavimo eksperimentų rezultatų. Laukiama, kad jie irgi turėtų išspręsti tą patį uždavinį, kaip ir Google bei USTC mokslininkų grupės.

IBM claims to have created a more programmable and adaptable processor.

Toks tvirtinimas leidžia tikėtis, jog bus bandoma spręsti ir papildomus testus, kurie artimesni mūsų išvardintiems taikomiesiams algoritmams.

Viskas svarbu, kai kalbame apie kvantinius skaičiavimus

Viskas svarbu, kai kalbame apie kvantinius skaičiavimus

But the processing power of a quantum circuit is not just about how many qubits it has. It also depends on how fast they operate

Viskas svarbu, kai kalbame apie kvantinius skaičiavimus

But the processing power of a quantum circuit is not just about how many qubits it has. It also depends on how fast they operate

and on how resistant they are to errors that could scramble a calculation, due for example to random fluctuations.

IBM paskelbė ir artimiausių 2 metų planus – tai matyt įdomiausia informacija

IBM paskelbė ir artimiausių 2 metų planus – tai matyt įdomiausia informacija

IBM unveiled a road map for the emerging technology that would see the company producing a quantum processor with 433 qubits by the end of 2022 year and one with at least 1,121 qubits by 2023 (named Condor).

IBM paskelbė ir artimiausių 2 metų planus – tai matyt įdomiausia informacija

IBM unveiled a road map for the emerging technology that would see the company producing a quantum processor with 433 qubits by the end of 2022 year and one with at least 1,121 qubits by 2023 (named Condor).

A quantum computer of that size ought to be able to perform many useful business applications, the company has said.

Realybė ir artimiausios ateities iššūkiai

Realybė ir artimiausios ateities iššūkiai

"The current state of the art is that no experiment has demonstrated quantum advantage for practical tasks yet," says physicist Chao-Yang Lu, who co-led the USTC effort.

Solving real-world problems such as simulating drug molecules or materials using quantum chemistry will require quantum computers to get drastically bigger and more powerful.

Realybė ir artimiausios ateities iššūkiai

"The current state of the art is that no experiment has demonstrated quantum advantage for practical tasks yet," says physicist Chao-Yang Lu, who co-led the USTC effort.

Solving real-world problems such as simulating drug molecules or materials using quantum chemistry will require quantum computers to get drastically bigger and more powerful.

Quantum engineer Andrew Dzurak at the University of New South Wales in Sydney, Australia, thinks that with 1,000-qubit chips such as IBM's planned Condor, the technology might start to prove its worth. It is hoped that some useful and even commercially valuable problems can be solved using quantum computers in this thousand-to-million-qubit range. But to do really paradigm-shifting stuff, you are going to need millions of physical qubits.

Dealing with errors is particularly difficult, because the laws of physics prevent quantum computers from using the error-correcting methods of classical machines, which typically require keeping multiple copies of each bit.

Pasitelkus loginius kubitus (jie gaunami sujungus kelis kubitus į dubliuojančių kubitų grupes) bus smarkiai pailgintas kubitų skaičiavimo iki pirmos klaidos laikas – vieno iš svarbiausių kvantinių skaičiavimų prakeiksmų poveikio kontrolė.

Some other approaches to building quantum computers hope to benefit from qubits with lower intrinsic error rates.

2022 metai žada daug naujienų, bus įdomu.

Skaičių faktorizavimas

Šią seminaro pranešimo dalį paskatino pokalbiai su Jevgenijum apie kvantinių kompiuterių galimybes spręsti "tikrus" uždavinius.

Taigi vieną aktualų taikomąjį uždavinį vėl panagrinėkime detaliau, įvertinkime, koks kvantinis kompiuteris bus pajėgus jį spręsti (ar bus?)

Skaičių faktorizavimas

Šią seminaro pranešimo dalį paskatino pokalbiai su Jevgenijum apie kvantinių kompiuterių galimybes spręsti "tikrus" uždavinius.

Taigi vieną aktualų taikomąjį uždavinį vėl panagrinėkime detaliau, įvertinkime, koks kvantinis kompiuteris bus pajėgus jį spręsti (ar bus?)

Reikia išskaidyti duotąjį skaičių N į pirminius daugiklius $N = pq$.

Skaičių faktorizavimas

Šią seminaro pranešimo dalį paskatino pokalbiai su Jevgenijum apie kvantinių kompiuterių galimybes spręsti "tikrus" uždavinius.

Taigi vieną aktualų taikomąjį uždavinį vėl panagrinėkime detaliau, įvertinkime, koks kvantinis kompiuteris bus pajėgus jį spręsti (ar bus?)

Reikia išskaidyti duotąjį skaičių N į pirminius daugiklius $N = pq$.

Tai klasikinis ir labai gražus skaičių teorijos uždavinys – grynoji matematika.

Skaičių faktorizavimas

Šią seminaro pranešimo dalį paskatino pokalbiai su Jevgenijum apie kvantinių kompiuterių galimybes spręsti "tikrus" uždavinius.

Taigi vieną aktualų taikomąjį uždavinį vėl panagrinėkime detaliau, įvertinkime, koks kvantinis kompiuteris bus pajėgus jį spręsti (ar bus?)

Reikia išskaidyti duotąjį skaičių N į pirminius daugiklius $N = pq$.

Tai klasikinis ir labai gražus skaičių teorijos uždavinys – grynoji matematika.

Tačiau pradėjus plačiai (visur) naudoti RSA viešojo rakto algoritmą – skaičių faktorizavimas tapo labai aktualiu taikomuoju uždaviniu.

Šiandien žinomi sparčiausi faktorizavimo algoritmai yra stochastiniai, paminėsime kvadratinį ir bendrąjį skaičių lauko rėčius. Jų sudėtingumas yra superpolinominis, pvz. antrojo algoritmo sudėtingumo euristinis įvertis yra:

$$O\left(\exp\left(1.9(\ln N)^{\frac{1}{3}}(\ln\ln N)^{\frac{2}{3}}\right)\right).$$

p=116067837367648677168889

q=4642713494705947086712 7

45 skaitmenų skaičius

N=53886971484811770419399036201271583757280790 3

p=116067837367648677168 89
q=464271349470594708671 27

45 skaitmenų skaičius
N=53886971484811770419399036201271583757280790 3

Python faktorizavimo metodas (inga serveris, 4 branduoliai)

p=116067837367648677168889

q=4642713494705947086712 7

45 skaitmenų skaičius

N=53886971484811770419399036201271583757280790 3

Python faktorizavimo metodas (inga serveris, 4 branduoliai)

python -m primefac N

p=1160678373676486771688 9

q=4642713494705947086712 7

45 skaitmenų skaičius

N=538869714848117704193990362012715837572807903

Python faktorizavimo metodas (inga serveris, 4 branduoliai)

python -m primefac N

538869714848117704193990362012715837572807903:
4642713494705947086712 7 1160678373676486771688 9

p=1160678373676486771688 9

q=4642713494705947086712 7

45 skaitmenų skaičius

N=538869714848117704193990362012715837572807903

Python faktorizavimo metodas (inga serveris, 4 branduoliai)

python -m primefac N

538869714848117704193990362012715837572807903:
4642713494705947086712 7 1160678373676486771688 9

CPU laikas: nuo 24 iki 64 sekundžių.

Shor'o algoritmas

1. Algoritmas hibridinis – dalis skaičiavimų yra atliekami įprastiniais kompiuteriais, o kita dalis kvantiniu kompiuteriu.

2. Tai stochastinis algoritmas – eilinio eksperimento metu sprendinio radimo tikimybė nėra lygi 1, bet ji didelė.

3. Pamatysime, kad skaičiavimų trukmė priklauso ne tik nuo kubitų skaičiaus.

1. Pasirenkame skaičių a, tarkime, kad $\gcd(a, N) = 1$.
2. Apibrėžiame funkciją $f(x) = a^x \mod N$.
3. Randame funkcijos $f(x)$ periodą $f(x + r) = f(x)$.
4. Jeigu $r = 2l - 1$, tai grįžtame į 1 žingsnį.
5. Jeigu $a^{r/2} \equiv -1 \pmod N$, tai grįžtame į 1 žingsnį.
6. Skaičiuojame skaičiaus N pirminį daugiklį $\gcd(a^{r/2} \pm 1, N)$.

1. Pasirenkame skaičių a, tarkime, kad $\gcd(a, N) = 1$.
2. Apibrėžiame funkciją $f(x) = a^x \mod N$.
3. Randame funkcijos $f(x)$ periodą $f(x + r) = f(x)$.
4. Jeigu $r = 2l - 1$, tai grįžtame į 1 žingsnį.
5. Jeigu $a^{r/2} \equiv -1 \pmod N$, tai grįžtame į 1 žingsnį.
6. Skaičiuojame skaičiaus N pirminį daugiklį $\gcd(a^{r/2} \pm 1, N)$.

$N = 15, \quad a = 2, \quad r = 4, \quad \gcd(2^2 \pm 1, 15).$

Kvantinė algoritmo dalis – periodo radimas

1. Randame tokį $M = 2^m$, kad $N^2 \leq M < 2N^2$.

Kvantinė algoritmo dalis – periodo radimas

1. Randame tokį $M = 2^m$, kad $N^2 \leq M < 2N^2$.
2. Paruošiame pradinį *ket*-vektorių

$$|\psi\rangle = \frac{1}{M} \sum_{x=0}^{M-1} |x\rangle \, .$$

Kvantinė algoritmo dalis – periodo radimas

1. Randame tokį $M = 2^m$, kad $N^2 \leq M < 2N^2$.
2. Paruošiame pradinį *ket*-vektorių

$$|\psi\rangle = \frac{1}{M} \sum_{x=0}^{M-1} |x\rangle \, .$$

3. Skaičiuojame funkcijos $f(x)$ reikšmes kiekviename taške

$$U_f(|\psi, 0\rangle) = \frac{1}{M} \sum_{x=0}^{M-1} |x, f(x)\rangle \, .$$

Kvantinė algoritmo dalis – periodo radimas

1. Randame tokį $M = 2^m$, kad $N^2 \leq M < 2N^2$.
2. Paruošiame pradinį *ket*-vektorių

$$|\psi\rangle = \frac{1}{M} \sum_{x=0}^{M-1} |x\rangle \, .$$

3. Skaičiuojame funkcijos $f(x)$ reikšmes kiekviename taške

$$U_f(|\psi, 0\rangle) = \frac{1}{M} \sum_{x=0}^{M-1} |x, f(x)\rangle \, .$$

Tai sudėtingiausia algoritmo dalis. Shor'as sukonstravo kartotinio kėlimo kvadratu metodo kvantinį algoritmą. Jo realizavimui reikia $O\big((\log N)^2(\log\log N)(\log\log\log N)\big)$ loginių vartų.

4. Pritaikome diskrečiąją Furje transformaciją ir gauname tokią kvantinės sistemos būseną (tai ir yra pagrindinė Shor'o inovacija)

$$\frac{1}{M^2}\sum_{x=0}^{M-1}\sum_{y=0}^{M-1}\omega^{xy}\left|y, f(x)\right\rangle, \quad \omega = e^{2\pi i/M}.$$

4. Pritaikome diskrečiąją Furje transformaciją ir gauname tokią kvantinės sistemos būseną (tai ir yra pagrindinė Shor'o inovacija)

$$\frac{1}{M^2}\sum_{x=0}^{M-1}\sum_{y=0}^{M-1}\omega^{xy}\left|y, f(x)\right\rangle, \quad \omega = e^{2\pi i/M}.$$

Šią sumą pertvarkome taip, kad galėtume prognozuoti matavimo rezultatus

$$\frac{1}{M^2}\sum_{z=0}^{N-1}\sum_{y=0}^{M-1}\left(\sum_{x=\{0,\ldots,M-1\},f(x)=z}\omega^{xy}\right)\left|y, z\right\rangle.$$

4. Pritaikome diskrečiąją Furje transformaciją ir gauname tokią kvantinės sistemos būseną (tai ir yra pagrindinė Shor'o inovacija)

$$\frac{1}{M^2}\sum_{x=0}^{M-1}\sum_{y=0}^{M-1}\omega^{xy}\left|y, f(x)\right\rangle, \quad \omega = e^{2\pi i/M}.$$

Šią sumą pertvarkome taip, kad galėtume prognozuoti matavimo rezultatus

$$\frac{1}{M^2}\sum_{z=0}^{N-1}\sum_{y=0}^{M-1}\left(\sum_{x=\{0,\ldots,M-1\},f(x)=z}\omega^{xy}\right)\left|y, z\right\rangle.$$

Greitosios Furje transformacijos kvantinis algoritmas realizuojamas panaudojant $\frac{1}{2}\big(\log M(\log M+1)\big)$ loginius vartus.

Parodysime, kaip atliekama tokia transformacija (Shor'o variantas).

Parodysime, kaip atliekama tokia transformacija (Shor'o variantas).

Pažymėkime H_j Hadamard transformaciją, kai ją pritaikome j-ajam kubitui ir S_{jk} transformaciją, kurią pritaikome dviem kubitams (j-ajam ir k-ajam)

$$S_{jk} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \exp(i\theta_{k-j}) \end{pmatrix}, \quad \theta_{k-j} = \pi/2^{k-j}.$$

Parodysime, kaip atliekama tokia transformacija (Shor'o variantas).

Pažymėkime H_j Hadamard transformaciją, kai ją pritaikome j-ajam kubitui ir S_{jk} transformaciją, kurią pritaikome dviem kubitams (j-ajam ir k-ajam)

$$S_{jk} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \exp(i\theta_{k-j}) \end{pmatrix}, \quad \theta_{k-j} = \pi/2^{k-j}.$$

Tada kvantinę Furje transformaciją galime apibrėžti rekursija:

$$QFT_{0,m-1} = H_0 S_{01} \dots S_{0,m-1}\, QFT_{1,m-1},$$
$$QFT_{m-1,m-1} = H_{m-1}.$$

5. Atliekame matavimą ir gauname rezultatą $|y, z\rangle$.

5. Atliekame matavimą ir gauname rezultatą $|y, z\rangle$.

Tokio rezultato tikimybė

$$P(|y,z\rangle) = \left| \frac{1}{M} \sum_{x=\{0,\ldots,M-1\},\, f(x)=z} \omega^{xy} \right|^2 = \frac{1}{M^2} \frac{\sin^2(\pi bry/M)}{\sin^2(\pi ry/M)},$$

$$b = 1 + \left\lfloor \frac{M^2 - x_0 - 1}{r} \right\rfloor,$$

čia x_0 yra mažiausia x reikšmė, kai $f(x_0) = z$.

5. Atliekame matavimą ir gauname rezultatą $|y, z\rangle$.

Tokio rezultato tikimybė

$$P(|y,z\rangle) = \left| \frac{1}{M} \sum_{x=\{0,\ldots,M-1\},\, f(x)=z} \omega^{xy} \right|^2 = \frac{1}{M^2} \frac{\sin^2(\pi bry/M)}{\sin^2(\pi ry/M)},$$

$$b = 1 + \left\lfloor \frac{M^2 - x_0 - 1}{r} \right\rfloor,$$

čia x_0 yra mažiausia x reikšmė, kai $f(x_0) = z$.

Šios tikimybės yra didelės, kai $\frac{yr}{M}$ yra artimas kokiam nors sveikam skaičiui c.

Tikimybės nepriklauso nuo z.

Mes žinome $\frac{y}{M}$, o norime rasti $\frac{c}{r}$.

Mes žinome $\frac{y}{M}$, o norime rasti $\frac{c}{r}$.

Panaudodami tęsiamų trupmenų metodą apskaičiuojame artinį $\frac{d}{s}$, tenkinantį tokias sąlygas

$$a)\ s < N,$$
$$b)\ \left|\frac{y}{M} - \frac{d}{s}\right| < \frac{1}{2M}.$$

Tada yra labai didelė tikimybė, kad s yra periodas r, arba periodo kartotinis skaičius.

1. Rastojo kandidato s tikrinimą atliekame įprastiniu kompiuteriu, skaičiavimai atliekami labai greitai.

2. Todėl papildomai tikriname ir skaičiaus s kaimynus $s \pm l$, $l = 1, \ldots, L$.

3. Jeigu nepavyksta rasti N skaidinio, tai kartojame visą algoritmą su kitu a.