VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
PROGRAMŲ SISTEMŲ BAKALAURO STUDIJŲ PROGRAMA

Kvantiniai skaičiavimai baigtiniuose kūnuose

Quantum Computing for Finite Fields

Bakalauro baigiamasis darbas

Atliko:	Leonardas Mačiulis	(parašas)
Darbo vadovas:	lekt. Irus Grinis	(parašas)
Darbo recenzentas:	asist. dr. Haroldas Giedra	(parašas)

Vilnius – 2021

Santrauka

Baigtiniai kūnai, ypač GF(p) ir GF(p^n) yra plačiai taikomi matematiniai objektai. Tobulėjant kvantiniams kompiuteriams klasikiniais kompiuteriais atliekamus skaičiavimus baigtiniuose kūnuose siekiama paspartinti kvantiniais skaičiavimais. Šiame darbe kvantinių operatorių grandinėmis įgyvendinami veiksmai baigtiniuose kūnuose GF(p) remiantis reikšmių kvantinių Furjė transformacijų sudėtimi. Įgyvendinti veiksmai baigtiniuose kūnuose panaudojami tiesinės lygčių sistemos baigtiniame kūne GF(p) sprendimui perrenkant kintamųjų būsenas Groverio paieška. Tiesinės lygčių sistemos sprendimo kvantinių operatorių grandinės veikimas išbandomas vykdant kvantiniu kompiuteriu.

Raktiniai žodžiai: baigtiniai kūnai, kvantiniai kompiuteriai, kvantinė Furjė transformacija, Groverio paieška, tiesinių lygčių sistemos

Summary

Finite fields, most notably GF(p) and GF(p^n), are mathematical objects with a wide variety of applications. With the advent of quantum computing, algorithms are being researched to provide speedups over classical computing for finite fields. In this work, arithmetic operations for finite fields are implemented in quantum logic gate circuits using the quantum Fourier transform. The implemented arithmetic operations are used to build a quantum circuit for solving systems of linear equations over GF(p) by applying Grover's search algorithm. Finally, attempts are made at running the quantum circuit to solve systems of linear equations on a quantum device.

Keywords: finite fields, quantum computers, quantum Fourier transform, Grover's search, systems of linear equations

TURINYS

ĮVADAS 4

1. KVANTINIAI SKAIČIAVIMAI 5
   1.1. Kvantinės būsenos 5
   1.2. Operatoriai 7
   1.3. Kvantinių skaičiavimų paklaidos 11

2. BAIGTINIAI KŪNAI 12
   2.1. Baigtiniai kūnai GF(p) 12
   2.2. Baigtinių kūnų taikymai 12

3. KVANTINIAI SKAIČIAVIMAI GF(P) 14
   3.1. Kvantinė Furjė transformacija 14
   3.2. Sudėtis 16
   3.3. Atimtis 18
   3.4. Daugyba 18
   3.5. Perėjimas prie modulinės aritmetikos 19
   3.6. Dalyba 21
   3.7. Tiesinės lygčių sistemos sprendimas GF(p) 22

REZULTATAI IR IŠVADOS 27

LITERATŪRA 29

PRIEDAI 29
   1 priedas. Programų išeities tekstai 30

Įvadas

Baigtiniais kūnais vadinamos baigtinės aibės, kuriose apibrėžti įprasti matematiniai veiksmai: sudėtis, atimtis, daugyba bei dalyba ir galioja įprastos šių matematinių veiksmų savybės. Baigtiniai kūnai dažniausiai siejami su pirminio skaičiaus p liekanų aibės baigtiniais kūnais GF(p) ir daugianarių liekanų aibės baigtiniais kūnais GF(p^k). Baigtiniai kūnai naudojami didelio periodo generuojant pseudoatsitiktinių skaičių sekas, sudarant klaidas taisančius kodus, skaičiuojant vienakryptes funkcijas kriptografijoje. Baigtinių kūnų svarbą liudija klasikiniais kompiuteriais baigtiniuose kūnuose nuolat koduojant ir šifruojant kasdieninius tinklu perduodamus pranešimus atliekami skaičiavimai.

Klasikiniai kompiuteriai skaičiuoja klasikinių bitų registrais, kurie gali būti tik vienoje iš galimų bitų sistemos būsenų. Kvantiniai kompiuteriai skaičiuoja kvantinių bitų kubitų registrais, kurių būsena turi daugiau matmenų nei klasikinių registrų būsena. Papildomi matmenys įgalina kubitų sistemą būti keliose klasikinėse būsenose vienu metu skirtingais santykiais, taip kvantiniai kompiuteriai sugeba apdoroti daugiau duomenų vienu žingsniu. Tikimasi, kad dalis šiuo metu tik $\mathcal{O}(2^n)$ greičio perrinkimu klasikiniais skaičiavimais sprendžiamų uždavinių kvantiniais skaičiavimais galės būti išspręsti žymiai greičiau. Vienas žinomiausių kvantinių algoritmų — Šoro algoritmas — skirtas skaičiaus skaidymui pirminiais daugikliais, kuriame reikalingas greitas natūraliojo skaičiaus kėlimo laipsniu moduliu algoritmas. Pirminio skaičiaus p liekanų aibės baigtinių kūnų GF(p) kvantinių skaičiavimų tyrimai gali padėti patobulinti Šoro ir kitus kvantinius algoritmus.

Šio baigiamojo darbo tikslas — skaičiavimus baigtiniuose kūnuose atlikti kvantiniu kompiuteriu tikintis kvantinių skaičiavimų pranašumų. Darbo metu skaičiavimai baigtiniuose kūnuose bus įgyvendinami kvantiniu simuliatoriumi ir kvantiniu kompiuteriu vykdomomis kvantinių operatorių grandinėmis. Darbo tikslui pasiekti keliami šie uždaviniai:

1. kvantinių operatorių grandinėmis įgyvendinti sudėties, atimties, daugybos ir dalybos veiksmus baigtiniuose kūnuose GF(p);
2. naudojant įgyvendintas skaičiavimų baigtiniuose kūnuose grandines išspręsti tiesinių lygčių sistemą baigtiniame kūne GF(p);
3. patikrinti, kaip įgyvendinta lygčių sistemą sprendžianti kvantinių operatorių grandinė veikia tikrame kvantiniame įrenginyje.

1. Kvantiniai skaičiavimai

Šiame skyriuje apibrėžiamos sąvokos, naudojamos tolimesniuose skaičiavimuose. Apie tai plačiau rašoma [ABB+21; YM08; JAA+18; KWA19].

1.1. Kvantinės būsenos

Klasikinio kompiuterio būseną nusako atmintyje saugomi duomenys. Klasikinio kompiuterio atmintį sudaro bitais vadinami informacijos vienetai, turintys vieną iš dviejų būsenų — 0 ir 1. Klasikinių kompiuterių informacijos vienetus bitus kvantiniuose kompiuteriuose atitinka kvantiniai bitai — kubitai. Kubitas yra dvimatė kvantinė sistema, turinti dvi nepriklausomas bazinėmis vadinamas būsenas $|0\rangle$ ir $|1\rangle$. Kubitas yra dvimatė sistema, todėl kubito būsenos nurodomos dvimačiais kompleksinių skaičių vektoriais. Kubito bazines būsenas galima užrašyti dvimačiais vektoriais

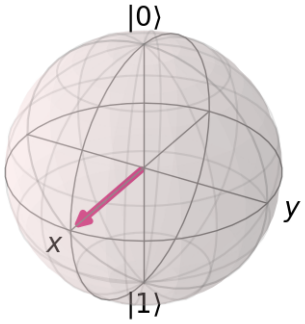
$$|0\rangle = \begin{pmatrix} 1+0i \\ 0+0i \end{pmatrix}, \tag{1}$$

$$|1\rangle = \begin{pmatrix} 0+0i \\ 1+0i \end{pmatrix}. \tag{2}$$

Kitaip nei vienmatis, dvi galimas būsenas turintis klasikinis bitas, kubitas gali būti superpozicijos būsenoje, kuri nėra nei $|0\rangle$, nei $|1\rangle$, tačiau gali būti išreikšta bazinių būsenų suma

$$|\psi\rangle = c_1|0\rangle + c_2|1\rangle, \tag{3}$$

kur c_1 ir c_2 yra kompleksiniai skaičiai, vadinami būsenų $|0\rangle$ ir $|1\rangle$ amplitudėmis. Dvimatė kubito būsena dažnai vaizduojama Blocho vektoriumi Blocho sferoje. Blocho sferos šiaurinis ir pietinis poliai atintinka bazines kubito būsenas $|0\rangle$ ir $|1\rangle$. Superpozicijos apibūdinimui palengvinti įvardijamos ir kitos būsenos. Blocho sferos $+X$ ir $-X$ kryptys atitinka būsenas $|+\rangle$ ir $|-\rangle$, Blocho sferos $+Y$ ir $-Y$ kryptys atitinka būsenas $|\circlearrowright\rangle$ ir $|\circlearrowleft\rangle$.



1 pav. Blocho sfera, kurioje pavaizduotas kubito būseną $|+\rangle$ atitinkantis Blocho vektorius. Paveikslas gautas „Qiskit“ simuliatoriumi.

Klasikinė n bitų sistema turi 2^n būsenų ir n matmenų. Kaip ir klasikinės sistemos, kvan-

tinės kubitų sistemos gali būti jungiamos į daugiamates n kubitų sistemas, turinčias 2^n bazinių būsenų — matmenų. Vienodas informacijos vienetų skaičius kvantinėse sistemose turi daugiau matmenų nei klasikinėse. Ši savybė suteikia pranašumų naudojant kvantines sistemas skaičiavimuose. Būsenų vektoriai jungiami tensorine sandauga

$$|xy\rangle := |x\rangle \otimes |y\rangle = \begin{pmatrix} x_1 \begin{pmatrix} y_1 \\ y_2 \\ ... \\ y_n \end{pmatrix} \\ x_2 \begin{pmatrix} y_1 \\ y_2 \\ ... \\ y_n \end{pmatrix} \\ ... \\ x_n \begin{pmatrix} y_1 \\ y_2 \\ ... \\ y_n \end{pmatrix} \end{pmatrix}. \tag{4}$$

Vykdant kvantinius skaičiavimus kubitai gali būti matuojami. Matavimo metu stebimos daugiamatės kvantinės kubitų sistemos superpozicijos bazinės būsenos, kurių matavimo tikimybės lygios

$$P_{|b\rangle}(|\psi\rangle) = |\langle\psi|b\rangle|^2 = |\langle\psi| \cdot |b\rangle|^2, \tag{5}$$

kur b yra bazinė kubitų sistemos būsena, pavyzdžiui, $|011\rangle$ trijų kubitų sistemoje. Skaičiuojant stebimos būsenos tikimybę taikyta transponuotos kompleksinių jungtinių skaičių matrica — Ermito jungtinė matrica:

$$A^{\dagger}_{n\times m} = \overline{A^{T}_{n\times m}} = \begin{pmatrix} \overline{a_{11}} & \overline{a_{21}} & ... & \overline{a_{n1}} \\ \overline{a_{12}} & \overline{a_{22}} & ... & \overline{a_{n2}} \\ ... & ... & ... & ... \\ \overline{a_{1m}} & \overline{a_{2m}} & ... & \overline{a_{nm}} \end{pmatrix}. \tag{6}$$

Kvantinės sistemos būsenoms galima suskaičiuoti atitinkamus Ermito jungtinius vektorius

$$|\psi\rangle = \langle\psi|^{\dagger}, \tag{7}$$

$$\langle\psi| = |\psi\rangle^{\dagger}. \tag{8}$$

1.2. Operatoriai

Kvantinės sistemos būsenos keičiamos operatoriais. Operatoriumi vadinama unitarinė kvadratinė kompleksinių skaičių matrica, kuri nurodo kiekvienos bazinės sistemos būsenos poveikį pereinant į kiekvieną bazinės sistemos būseną. Unitarine matrica vadinama kvadratinė matrica, kurios Ermito jungtinė matrica lygi atvirkštinei:

$$U^\dagger = U^{-1}, \quad UU^{-1} = U^{-1}U = I. \tag{9}$$

Unitarinės matricos visada turi atvirkštines, todėl kiekvienas kvantinių skaičiavimų operatorius yra apverčiamas. Apverčiamumas užtikrina, kad kvantiniais skaičiavimais apdorojus pradinius duomenis, gautus duomenis galima išskaidyti į pradinius. Apverčiamumas gali supaprastinti atvirkštinių funkcijų radimą, tačiau apsunkina klasikiniuose kompiuteriuose įprastus veiksmus. Pavyzdžiui, atmintis negali būti atlaisvinta perrašant neatlikus matavimo ir neprarandant sistemos superpozicijos. Atmintis atlaisvinama atvirkštiniais operatoriais sugrąžinant kubitų būsenas arba pasitelkiant išskirtines dalykinės srities duomenų savybes.

Adamaro operatoriumi būsenos vektorius pasukamas taip, kad būsenos $|0\rangle$ ir $|1\rangle$ pakeičiamos būsenomis $|+\rangle$ ir $|-\rangle$. Tiek būsena $|+\rangle$, tiek $|-\rangle$ matavimo metu turi lygias tikimybes tapti $|0\rangle$ ir $|1\rangle$, taip sukuriama kvantiniuose skaičiavimuose naudinga klasikinius bitus 0 ir 1 vienu metu reiškianti superpozicija. Adamaro operatorius užrašomas unitarine matrica

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{10}$$

Adamaro operatorius yra pats sau atvirkštinis:

$$H^{-1} = H^\dagger = H. \tag{11}$$

Paulio operatoriai X, Y, Z pasuka būsenos vektorių 180° apie X, Y ar Z ašis. Paulio operatorius atitinka unitarinės matricos

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{12}$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \tag{13}$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{14}$$

Paulio operatoriai yra patys sau atvirkštiniai:

$$X^{-1} = X^\dagger = X, \tag{15}$$

$$Y^{-1} = Y^\dagger = Y, \tag{16}$$

$$Z^{-1} = Z^\dagger = Z. \tag{17}$$

$$\tag{18}$$

Paulio operatorius X atlieka loginį būsenų $|0\rangle$ ir $|1\rangle$ neigimą, todėl dar vadinamas neigimo operatoriumi.

Kvantiniams skaičiavimams reikalingi dvinariai operatoriai, veikiantys du kubitus vienu metu. Paprasčiausi dvinariai operatoriai — valdomi Paulio operatoriai. Valdomas operatorius valdančiajam kubitui esant būsenoje $|1\rangle$ valdomąjį kubitą veikia Paulio operatoriumi. Valdančiajam kubitui esant būsenoje $|0\rangle$ valdomasis kubitas nėra veikiamas operatoriumi. Valdančiojo kubito superpozicijos atveju valdomasis kubitas įgyja nuo valdančiojo kubito priklausomą superpoziciją. Jei pirmasis kubitas yra valdantis, antrasis — valdomasis, tada dvinariai valdomi Paulio operatoriai CX, CY, CZ užrašomi unitarinėmis matricomis

$$CX = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \tag{19}$$

$$CY = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \end{pmatrix}, \tag{20}$$

$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}. \tag{21}$$

Valdomi operatoriai gali priklausyti nuo daugelio valdančiųjų kubitų. Valdomasis kubitas veikiamas operatoriumi, jei visi valdantieji kubitai yra būsenoje $|0\rangle$. Trinaris valdomas Paulio operatorius, dar vadinamas Tofolio operatoriumi, kurio pirmasis ir antrasis kubitai valdantie-

ji, trečiasis — valdomasis, gali būti užrašytas unitarine matrica

$$CCX = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}. \tag{22}$$

Valdomus operatorius galima sukurti bet kokiam valdančiųjų kubitų skaičiui:

$$C^nX = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & 0 & 0 \\ 0 & 0 & \dots & 0 & 1 & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 & 0 & 1 \\ 0 & 0 & \dots & 0 & 0 & 1 & 0 \end{pmatrix}_{2n \times 2n}. \tag{23}$$

Visi Paulio operatoriai yra jų pačių atvirkštiniai operatoriai, todėl antrą kartą paveikus arba nepaveikus Paulio operatoriumi atstatoma ankstesnė valdomojo kubito būsena. Taigi, visi valdomi Paulio operatoriai yra patys sau atvirkštiniai:

$$C^nX^{-1} = C^nX, \tag{24}$$

$$C^nY^{-1} = C^nY, \tag{25}$$

$$C^nZ^{-1} = C^nZ. \tag{26}$$

$$\tag{27}$$

Yra ir kitų kvantiniuose skaičiavimuose naudojamų operatorių. Paulio Z operatorių primenantis fazės posūkio operatorius $P(\theta)$ būsenos Blocho vektorių pasuka θ radianų apie Blocho sferos Z ašį. Fazės posūkio operatorius užrašomas unitarine matrica

$$P(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}. \tag{28}$$

Galima sudaryti ir valdomą fazės posūkio operatorių

$$CP(\theta) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\theta} \end{pmatrix}. \tag{29}$$

Fazės posūkio operatoriaus $P(\theta)$ poveikį galima panaikinti atsukant vektorių priešinga kryptimi operatoriumi $P(-\theta)$. Taigi, fazės posūkio operatoriams atvirkštiniai operatoriai

$$P(\theta)^{-1} = P(-\theta), \tag{30}$$

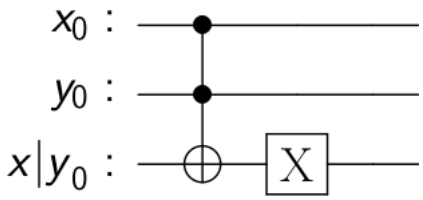
$$CP(\theta)^{-1} = CP(-\theta). \tag{31}$$

$$\tag{32}$$

Kubitai gali būti jungiami į daugiamates kvantines sistemas tensorine sandauga, tad ir pavienius kubitus veikiantys operatoriai tensorine sandauga gali būti sujungiami į vieną visą kubitų sistemą veikiantį operatorių:

$$U_1|\psi_1\rangle \otimes U_2|\psi_2\rangle \otimes \cdots \otimes U_n|\psi_n\rangle = (U_1 \otimes U_2 \otimes \cdots \otimes U_n)|\psi_1\psi_2 \ldots \psi_n\rangle. \tag{33}$$

Nors operatoriai suprantami kaip kompleksinių skaičių matricos, kvantinius skaičiavimus atliekantys operatoriai įprastai vaizduojami paprastesnių operatorių grandinėmis. Kiekvieno kubito būsena kiekviename žingsnyje vaizduojama atskira tiese. Kubito tiesėje nubrėžti ženklai žymi kubito būseną veikiantį operatorių, prie ženklo prijungtos tiesės — valdančiuosius kubitus. Veiksmai atliekami iš kairės į dešinę.



2 pav. Šeferio funkcijos $x|y = \neg(x \wedge y)$ grandinė.

Visos klasikiniuose skaičiavimuose taikomos loginės formulės gali būti išreikštos Šeferio funkcija $x|y = \neg(x \wedge y)$, kurią galima įgyvendinti kvantiniais operatoriais:

$$NAND|xy0\rangle = (I^{\otimes 2}X)CCX|xy0\rangle. \tag{34}$$

2 pav. kvantinių operatorių grandine pavaizduotas Šeferio funkciją įgyvendinantis operatorius. Grandinei atvirkščią galima rasti atliekant atvirkštinius operatorius atvirkščia tvarka.

1.3. Kvantinių skaičiavimų paklaidos

Bet kuri klasikinė loginių operatorių grandinė gali būti išreikšta kvantinių operatorių grandine, sudaryta iš Šeferio funkcijų, tačiau kvantinių kompiuterių įrangoje vykdomi kvantiniai skaičiavimai įgyja paklaidų, neaptinkamų šiuolaikiniuose klasikiniuose kompiuteriuose. Klasikinių kompiuterių vykdomi tranzistoriais įgyvendinti veiksmai yra tikslūs. Klasikinių kompiuterių paklaidos dažniausiai siejamos su slankaus kablelio skaičių paklaidomis, tinklų trikdžiais, elektromagnetinės spinduliuotės poveikiu arba įrangos dėvėjimusi. Kitaip nei patikimų klasikinių kompiuterių, šiuolaikinių kvantinių kompiuterių operatoriai nėra tikslūs: kiekvienas kubito būsenos vektoriaus posūkis įrangoje nėra atliekamas idealiai. Kvantinių kompiuterių paklaidas lemia dekoherencijos reiškinys, ypač ryškus ilgose grandinėse.

Dekoherencija vyksta kubitų sistemai sąveikaujant su aplinka. Sąveikos metu kubitų sistemos būsenos susiejamos su išorinių dalelių būsena. Nenuspėjami ryšiai su kubitų sistemos išore nenuspėjamai keičia kubitų sistemos būseną. Dekoherencijos metu sistemos būsena nematuojama, tačiau kubitų būsenos įgauna paklaidas, kurių neįmanoma ištaisyti neišmatavus išorinės sistemos. Dekoherencijos pasekmės mažinamos laikant kubitų sistemą artimoje absoliučiam nuliui temperatūroje, naudojant dekoherencijai atsparesnes trumpas kvantinių operatorių grandines arba vykdant kvantinių operatorių grandinę daug kartų siekiant statistiškai pašalinti dekoherencijos triukšmą.

2. Baigtiniai kūnai

2.1. Baigtiniai kūnai GF(p)

Baigtinis kūnas GF(p), dar vadinamas Galua lauku, kur p — pirminis skaičius, yra aibė iš p elementų, kurioje apibrėžti sudėties ir daugybos veiksmai.

$$\mathrm{GF}(p) = \{0, 1, \ldots p-1\}, \quad p \text{ — pirminis skaičius} \tag{35}$$

Baigtiniame kūne apibrėžtiems veiksmams galioja asociatyvumo, komutatyvumo ir distributyvumo dėsniai, yra vienetinis sudėties elementas nulis ir vienetinis daugybos elementas vienetas:

$$a, b, c \in \mathrm{GF}(p),$$
$$(a+b)+c = a+(b+c), \quad (ab)c = a(bc), \tag{36}$$
$$a+b = b+a, \quad ab = ba, \tag{37}$$
$$a(b+c) = ab+ac, \tag{38}$$
$$0+a = a, \quad 1 \cdot a = a. \tag{39}$$

Be to, baigtiniame kūne kiekvienam elementui a yra priešingas elementas $-a$, kurį pridedant gaunamas atimties veiksmas, bei kiekvienam nenuliniam elementui a yra atvirkščias elementas a^{-1}, kurį sudauginus gaunamas dalybos veiksmas.

Nors bet kokia savybes tenkinanti p elementų aibė gali būti vadinama baigtiniu kūnu GF(p), dažniausiai GF(p) siejamas su daliklio p liekanų aibe. Skaičiavimas natūraliaisiais skaičiais moduliu p tenkina visas šio kūno savybes, todėl GF(p) veiksmus galima apibrėžti kaip

$$a, b \in \mathrm{GF}(p),$$
$$a+b = (a+b) \bmod p, \tag{40}$$
$$a-b = (a-b) \bmod p, \tag{41}$$
$$ab = (ab) \bmod p, \tag{42}$$
$$\frac{a}{b} = (ab^{-1}) \bmod p, \quad (bb^{-1}) \bmod p = 1. \tag{43}$$

2.2. Baigtinių kūnų taikymai

Baigtiniuose kūnuose apibrėžti visi keturi aritmetikos veiksmai, turintys įprastas savybes, todėl baigtinį elementų skaičių turintys baigtiniai kūnai gali pavaduoti begalines aibes. Paprastesnėse baigtinėse aibėse lengviau įrodyti teoremas ir skaičiuoti.

Baigtinių kūnų veiksmai nesudėtingai skaičiuojami, todėl skaičiavimus galima greitai atlikti nesudėtingomis elektroninėmis grandinėmis. Baigtiniai kūnai taikomi tiesiniuose grįžtamojo ryšio poslinkio registruose (LFSR — „Linear Feedback Shift Register“), kurie naudojami

didelio periodo pseudoatsitiktinių skaičių sekoms generuoti. Greitai generuojamos pseudoatsitiktinių skaičių sekos pritaikomos išskirstant pasikartojančius bitus. Šiuo būdu paremtas 128b/130b kodavimas, naudotas perduodant PCI-e 3.0 duomenis.

Baigtinių kūnų savybės pritaikomos kodavime. Rido—Solomono klaidas taisančių kodų abėcėlės sudaro baigtinius laukus. BCH klaidas taisančių kodų leistini žodžiai priklauso pasirinkto generatoriaus sandaugai baigtiniame lauke.

Viena iš dažniausių baigtinių kūnų taikymo sričių — kriptografija. Skaičiavimai baigtiniuose kūnuose paprastesni, reikalauja mažesnio atminties kiekio, todėl jais paremti šifravimo algoritmai veikia greitai. Nors skaičiavimai yra paprasti, kai kurie uždaviniai baigtiniuose kūnuose labai sunkiai išsprendžiami. Kriptografijoje dažniausiai taikomas diskretaus logaritmo sudėtingumas. Kėlimas laipsniu baigtiniuose kūnuose gali būti atliktas greitai, tačiau nėra žinomas greitas algoritmas laipsnio rodiklio radimui diskrečiu logaritmu:

$$a^x \equiv b \pmod{p} \text{ — žinant } a \text{ ir } x, \text{ lengva rasti } b,$$
$$x \equiv \log_a b \pmod{p} \text{ — žinant } a \text{ ir } b, \text{ sunku rasti } x.$$

Diskretusis logaritmas taikomas Difio—Helmano raktų apsikeitimo algoritme kaip vienakryptė funkcija. Įvairios baigtinių kūnų savybės taikomos ir RSA bei AES šifruose.

3. Kvantiniai skaičiavimai GF(p)

Šiame skyriuje įgyvendinami kvantiniai skaičiavimo algoritmai, aprašyti [BBF03; Bea03; RG17] ir pritaikomi įvairiems veiksmams su konstantomis ir kintamaisiais.

3.1. Kvantinė Furjė transformacija

Klasikiniuose skaičiavimuose taikoma dvejetainė skaičiavimo sistema, tačiau kvantiniuose skaičiavimuose dvejetainė skaičiavimo sistema turi trūkumų. Skaičiavimams kvantinių operatorių grandinėse naudojama Furjė skaičiavimo sistema, kuri gaunama būseną dvejetaine sistema pakeitus kvantine Furjė transformacija

$$\mathrm{QFT}|x\rangle = |\tilde{x}\rangle. \tag{44}$$

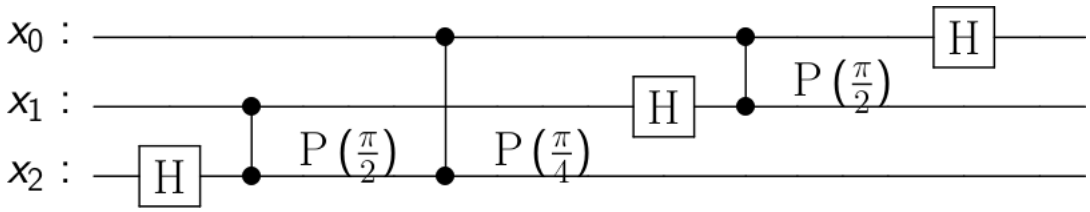
Diskreti Furjė transformacija vektoriui $(x_0, x_0 \dots x_{N-1})$ suskaičiuoja vektorių $(y_0, y_1 \dots y_{N-1})$ pagal formulę

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i \frac{jk}{N}}. \tag{45}$$

Kvantinė Furjė transformacija kvantinei būsenai $\sum_{j=0}^{N-1} x_j|j\rangle$ suskaičiuoja būseną $\sum_{j=0}^{N-1} y_k|k\rangle$ pagal tą pačią 45 formulę. Kvantinę Furjė transformaciją galima užrašyti kaip

$$\begin{aligned}
\mathrm{QFT}|x\rangle = \mathrm{QFT}|x_1 x_2 \dots x_n\rangle \quad &= \\
= \frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{\frac{2\pi i}{2}x}|1\rangle\right) &\otimes \\
\otimes \left(|0\rangle + e^{\frac{2\pi i}{2^2}x}|1\rangle\right) \quad &\otimes \\
\otimes \dots \quad &\otimes \\
\otimes \left(|0\rangle + e^{\frac{2\pi i}{2^{n-1}}x}|1\rangle\right) \quad &\otimes \\
\otimes \left(|0\rangle + e^{\frac{2\pi i}{2^n}x}|1\rangle\right). &
\end{aligned} \tag{46}$$

Taip užrašyta formulė rodo, kad kvantine Furjė transformacija gauta būsena sudaryta iš kiekvienam kubitui suteiktų posūkių. Kiekvieno kubito amplitudė pasukama kubito dvejeto laipsnį atitinkančia dalimi pradinį dvejetainį skaičių kartų. Kubitų būsenos būna lygiavertėse superpozicijose XY plokštumoje Blocho sferoje, kuriose vienodai tikėtina stebėti tiek $|0\rangle$, tiek $|1\rangle$.



3 pav. QFT grandinė.

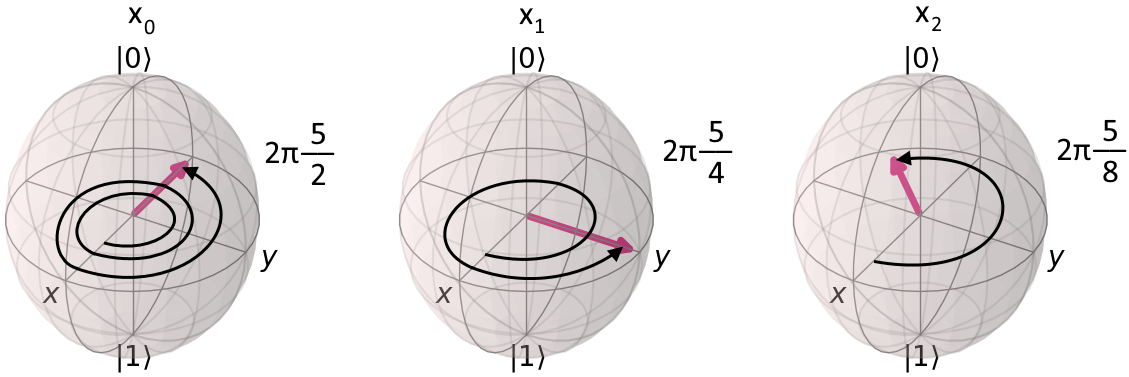
Kvantinę Furjė transformaciją galima įgyvendinti kvantinių operatorių grandine nenaudojant papildomų kubitų. Dvejetainėje būsenoje $|x_n \dots x_1 x_0\rangle$ Adamaro operatoriumi kubito x_n būsenos vektorius paverčiamas į Blocho sferos XY plokštumoje esančias būsenas. Jei kubito x_n būsena $|0\rangle$, kubito būsena keičiama į $|+\rangle$, kurios būsenos vektoriaus fazė yra $2\pi\frac{0\cdot 2^n}{2^{n+1}}$. Kubito būsena $|1\rangle$ keičiama į $|-\rangle$, kurios būsenos vektoriaus fazė yra $2\pi\frac{1\cdot 2^n}{2^{n+1}}$. Prie kubito x_n valdomais fazės posūkio operatoriais pridedami vis mažesni posūkiai, atitinkantys valdančiojo kubito dalį dvejetainėje skaičiavimo sistemoje. Fazei tapus

$$2\pi\frac{x_n 2^n + x_{n-1}2^{n-1} + \cdots + x_1 2^1 + x_0 2^0}{2^{n+1}} = 2\pi\frac{x}{2^{n+1}}$$

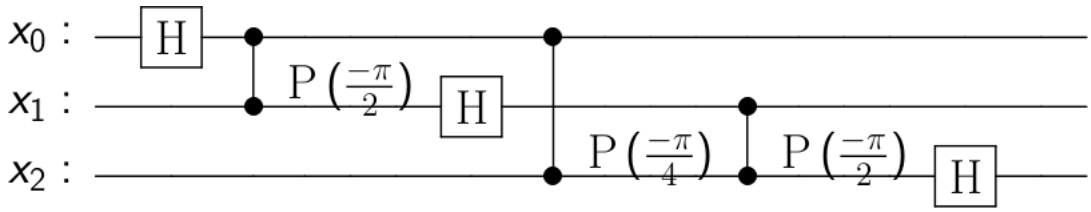
gaunama galutinė kvantinės Furjė transformacijos kubito x_n būsena

$$P\left(2\pi\frac{x - x_n 2^n}{2^{n+1}}\right)H|x_n\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi\frac{x}{2^{n+1}}i}|1\rangle\right).$$

Algoritmas kartojamas, kol gaunama visos būsenos kvantinė Furjė transformacija. 4 pav. pavaizduota būsena $|\tilde{5}\rangle$ Furjė skaičiavimo sistemoje. Vienetų kubito x_0 būsenos vektorius pasuktas puse rato rodant $5 \bmod 2 = 1$. Dvejetų kubito x_1 fazė pasukta ketvirčiu rodant $5 \bmod 4 = 1$. Ketvertų kubito x_2 fazė pasukta penkiais aštuntadaliais rodant $5 \bmod 8 = 5$.



4 pav. Būsena $|\tilde{5}\rangle$, pavaizduota kubitų Blocho sferose.



5 pav. QFT^{-1} grandinė.

Kvantine Furjė transformacija dvejetainiai skaičiai paverčiami Furjė skaičiavimo sistemos skaičiais. Atvirkštinė kvantinė Furjė transformacija Furjė skaičiavimo sistemos skaičius verčia dvejetainiais. Kvantinių skaičiavimų operatoriai yra unitariniai, todėl kiekvienas kvantinių operatorių grandine įgyvendintas veiksmas gali būti apverstas. Apvertus kvantinės Furjės transformacijos kvantinių operatorių grandinę gaunama atvirkštinė kvantinė Furjė transformacija. 5 pav. pavaizduota atvirkštinės kvantinės Furjė transformacijos grandinė, gauta apvertus 3 pav. pavaizduotą kvantinės Furjė transformacijos kvantinių operatorių grandinę.

3.2. Sudėtis

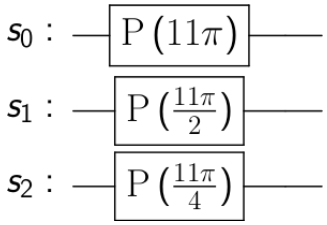
Klasikiniuose skaičiavimuose bitais saugomų dvejetainių skaičių $\overline{x_n \dots x_1 x_0}$ ir $\overline{y_n \dots y_1 y_0}$ suma $\overline{s_n \dots s_1 s_0}$ moduliu 2^{n+1} atliekama sudėties algoritmu

$$
\begin{aligned}
s_0 &= x_0 \oplus y_0, \\
c_0 &= x_0 \wedge y_0, \\
s_i &= x_{i-1} \oplus y_{i-1} \oplus c_{i-1}, \\
c_i &= (x_{i-1} \wedge y_{i-1}) \bigvee ((x_{i-1} \oplus y_{i-1}) \wedge c_{i-1}) .
\end{aligned}
$$

Nors klasikines logines grandines galima įgyvendinti kvantinių operatorių grandinėmis, kvantinių operatorių grandinė privalo būti apverčiama kiekviename žingsnyje. Skaičiuojant klasikiniu kompiuteriu kintamasis mintyje c_i kiekviename žingsnyje perrašoma naujai suskaičiuota verte. Kvantinių operatorių grandinėje c_i priklauso nuo ankstesnių $c_{i-1} \dots c1, c_0$, todėl kiekviena suskaičiuota vertė turėtų būti saugoma iki algoritmo pabaigos. Šio trūkumo išvengia kvantine Furjė transformacija paremta sudėties kvantinių operatorių grandinė. Kvantinės Furjė transformacijos metu skirtingas dvejetų laipsnių vertes nusakantys bitai pakeičiami visos dvejetainio skaičiaus vertės būsenos vektoriaus posūkiu skirtingais dvejeto laipsnius atitinkančiais periodais. Kubitų būsenos vektorių posūkiu saugomo skaičiaus $|\widetilde{x_n \dots x_1} x_0\rangle$ ir konstantos

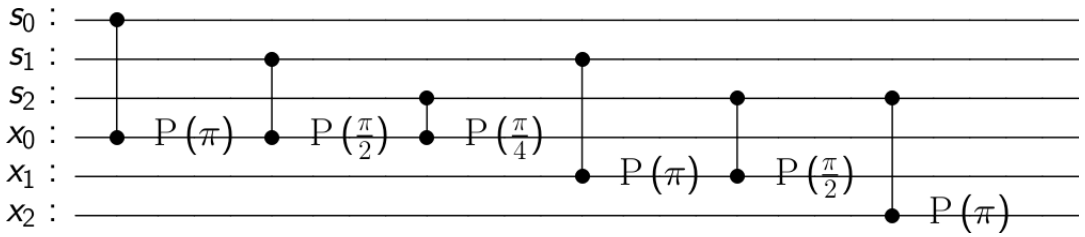
y sudėtį galima įgyvendinti kiekvieną kubitą pasukant y atitinkančia periodo dalimi:

$$|s_0\rangle = P(\pi y)\,|x_0\rangle,$$
$$|s_1\rangle = P\left(\frac{\pi y}{2}\right)|x_n\rangle,$$
$$\ldots$$
$$|s_n\rangle = P\left(\frac{\pi y}{2^n}\right)|x_n\rangle.$$



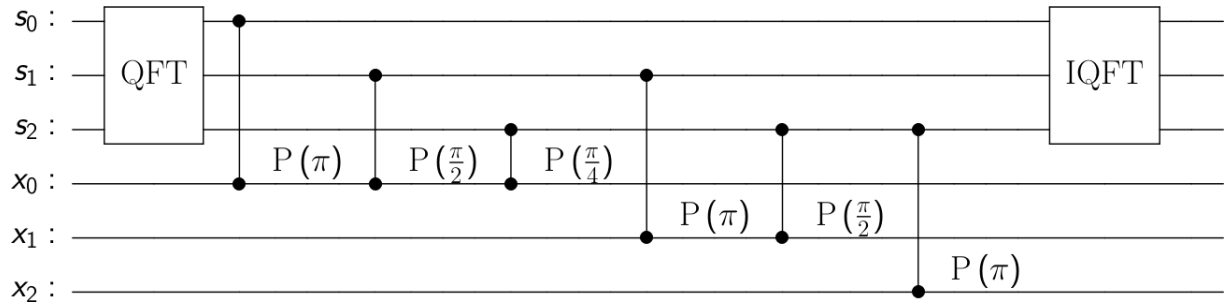
6 pav. Sudėties su 11 moduliu 8 grandinė.

Gauta sumos būsena $|\widetilde{s_n \ldots s_1} s_0\rangle$ pakeičia kintamąjį x, tačiau kubitų būsenos keičiamos nepriklausomai, todėl tokia sudėties kvantinių operatorių grandinė naudoja mažiau atminties nei klasikinio sumos algoritmo grandinė, įgyvendinta kvantiniais operatoriais.



7 pav. Dviejų kintamųjų sudėties moduliu 8 grandinė.

Kintamojo ir konstantos sudėties kvantinių operatorių grandinę galima praplėsti sudarant kintamojo ir kintamojo sudėties grandinę. Prie kintamojo $|\widetilde{y_n \ldots y_1} y_0\rangle$ galima pridėti kintamąjį $|x_n \ldots x_1 x_0\rangle$ kubitais $x_0, x1 \ldots x_n$ valdant konstantų $1, 2 \ldots 2^n$ sudėtį. Sudedant fazės posūkio operatoriai kubitams $y_{i<n}$ suteiktų visą ratą atitinkančius posūkius, todėl šie operatoriai praleidžiami.

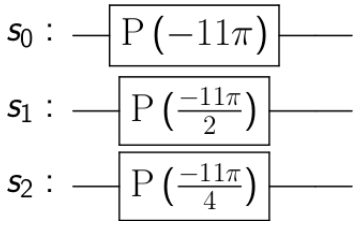


8 pav. Dviejų kintamųjų sudėties moduliu 8 grandinės naudojimas.

Sudėties grandinė dviems kintamiesiems kvantiniu kompiuteriu sudėti taikoma paruošiant klasikinius dvejetainius bitus atitinkančias kintamųjų kubitų būsenas, kvantine Furjė transformacija pakeičiant vieno kintamojo skaičiavimo sistemą, atliekant sudėtį ir atvirkštine kvantine Furjė transformacija sugrąžinant kintamųjų sumą į dvejetainę skaičiavimo sistemą. Tiek kvantinės Furjė transformacijos, tiek sudėties algoritmai veikia tiksliai, todėl idealiame kvantiniame kompiuteryje sumos būsena būtų stebima tikimybe 1.

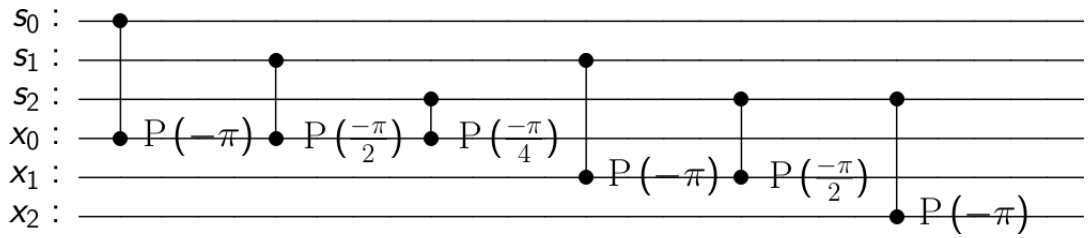
3.3. Atimtis

Kvantinių operatorių grandinėse atliekami veiksmai visada turi atvirkščius, nes unitariniai kvantiniai operatoriai privalo būti apverčiami. Atimtis yra sudėčiai atvirkščias veiksmas, todėl kvantinių operatorių grandines atimčiai galima sudaryti remiantis sudėties kvantinių operatorių grandinėmis.



9 pav. 11 atimties moduliu 8 grandinė.

Konstantos y atimtis iš kintamojo $|x_n \widetilde{\ldots x_1} x_0\rangle$ moduliu 2^{n+1} įgyvendinama pasukant kintamojo būsenos vektorius priešinga kryptimi.



10 pav. Dviejų kintamųjų atimties moduliu 8 grandinė.

Kintamojo $|x_n \ldots x_1 x_0\rangle$ atimtį iš kintamojo $|y_n \widetilde{\ldots y_1} y_0\rangle$ moduliu 2^{n+1} galima įgyvendinti dviejų kintamųjų sudėties kvantinių operatorių grandine atimant konstantas dvejeto laipsnius. Gauta grandinė kubitų būsenų vektorius pasuka taip, kaip pasuktų kintamųjų sudėties kvantinių operatorių grandinė, tačiau priešinga kryptimi.

3.4. Daugyba

Daugybos veiksmas susijęs su sudėtimi. Nors šiuo būdu retai skaičiuojama, daugybą galima užrašyti kaip

$$x \cdot y = \underbrace{x + x + \cdots + x}_{y \text{ kartų}}.$$

Jei y yra konstanta, daugybą galima atlikti pakartojant x sudėtį žinomą y kartų skaičių. Įgyvendinant kintamojo $|x_n \dots x_1 x_0\rangle$ ir konstantos y daugybą moduliu 2^{n+1} kvantinių operatorių grandine galima pasinaudoti fazės posūkio operatorių sudedamumo savybe

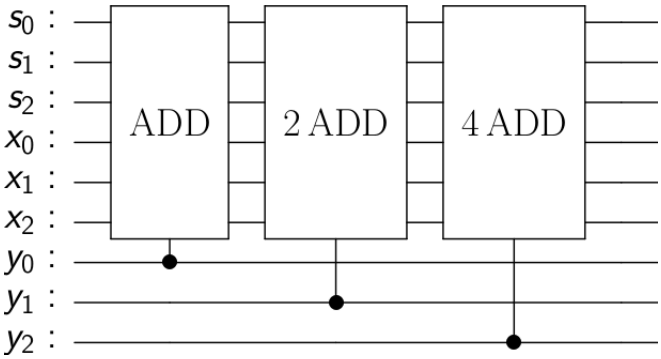
$$P(\theta)^y = P(\theta y)$$

ir naudoti dviejų kintamųjų $|\tilde{0}\rangle$ ir $|x_n \dots x_1 x_0\rangle$ sudėties grandinę y kartų didesniais fazių posūkiais.

Dviejų dvejetainių skaičių sandauga klasikiniuose skaičiavimuose skaičiuojama vis didesniais dvejeto laipsniais padaugintos sąlyginės sudėties — dvejetainės daugybos stulpeliu — algoritmu:

$$\begin{array}{rll} & x_n \dots x_1 x_0 & \\ \times & y_n \dots y_1 y_0 & \\ \hline & x_n \dots x_1 x_0, & \text{jei } y_0 = 1, \\ + & x_n \dots x_0, & \text{jei } y_1 = 1, \\ & \dots & \\ & 2^n \overline{x_n \dots x_0}, & \text{jei } y_n = 1. \end{array} \tag{47}$$

Tą patį algoritmą galima įgyvendinti kvantinių operatorių grandine atliekant kintamuoju $|y_n \dots y_1 y_0\rangle$ valdomą sąlyginę dvejeto laipsniais padaugintą $|x_n \dots x_1 x_0\rangle$ sudėtį su $|\tilde{0}\rangle$. 11 pav. pavaizduota dviejų kintamųjų daugybos grandinė, naudojanti sąlyginę kintamojo ir konstantos sandaugos sudėtį.

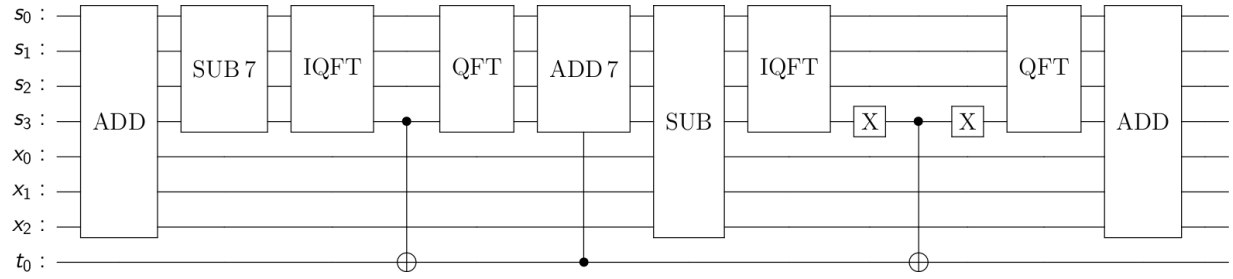


11 pav. Dviejų kintamųjų daugybos grandinė. Sandauga gaunama naudotos dviejų kintamųjų sudėties grandinės moduliu, šiuo atveju moduliu 8.

3.5. Perėjimas prie modulinės aritmetikos

Aptartos kvantinės operatorių grandinės skirtos sudėčiai, atimčiai ir daugybai moduliu 2^n, tačiau veiksmai baigtiniuose kūnuose GF(p) turi būti atlikti moduliu pirminiu skaičiumi p. Klasikiniuose skaičiavimuose natūraliųjų skaičių sudėtis, atimtis, daugyba ir dalyba su liekana n bitų kintamuosiuose vykdoma moduliu 2^n, nes n bitų kintamasis gali turėti 2^n skirtingų reikšmių. Klasikiniuose skaičiavimuose veiksmai už 2^n mažesniais moduliais vykdomi gautą reikšmę padalinant iš pasirinkto daliklio ir suskaičiuojant liekaną. Dalyba su liekana klasikiniuose kompiuteriuose įgyvendinama dalybos kampu algoritmu, tačiau dalybos kam-

pu algoritmas nėra pritaikytas apverčiamiems kvantiniams skaičiavimams, jo įgyvendinimui reikia daugelio kubitų. Kvantiniuose skaičiavimuose įprasta taikyti kitus modulinės aritmetikos būdus.

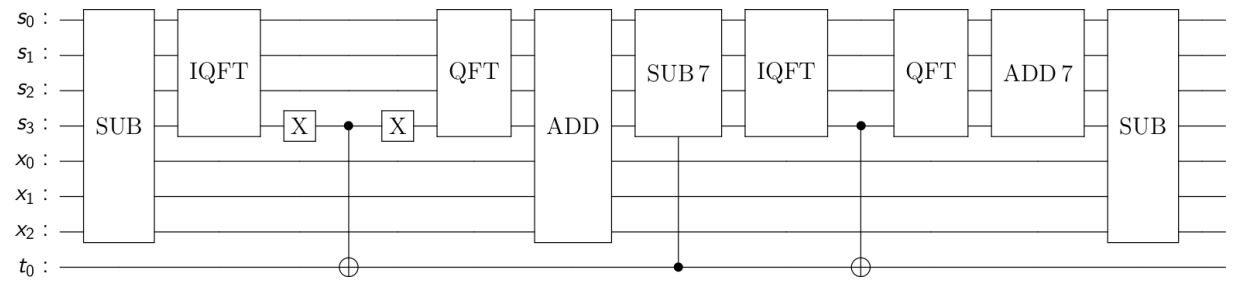


12 pav. Dviejų kintamųjų sudėties moduliu 7 grandinė.

Kvantinių operatorių grandinė sudėčiai pasirinktu moduliu sudaroma remiantis nelygybėmis

$$\begin{aligned} 0 \le x, y < 2^{n+1}, &\quad 0 < m < 2^{n+1}, \\ (x + y - m) \bmod 2^{n+2} < 2^{n+1}, &\quad \text{jei } x + y > m, \\ (x + y - m) \bmod 2^{n+2} \ge 2^{n+1}, &\quad \text{jei } x + y \le m, \\ x + y < m, &\quad \text{jei } (x + y) \bmod m - x \ge 0. \end{aligned}$$

Kintamasis $|\widetilde{y_n \dots y_1} y_0\rangle$ praplečiamas vienu kubitu iki $|0\widetilde{y_n \dots y_1} y_0\rangle$. Platesniame kvantiniame registre atliekama kintamųjų $|x_n \dots x_1 x_0\rangle$ ir $|0\widetilde{y_n \dots y_1} y_0\rangle$ sudėtis, tuomet atimamas pasirinktas daliklis m. Jei kintamųjų suma mažesnė nei m ir patenka į m liekanų aibę, sumos registras tampa didesnis nei 2^{n+1}, todėl sumos registro svariausias dvejetainės sistemos kubitas tampa lygus $|1\rangle$. Kintamųjų sumai esant didesnei nei m, sumos registre gaunama suma moduliu m, svariausias dvejetainės sistemos kubitas nepakinta. Perpildymo požymis išsaugomas pagalbiniame kubite. Perpildymui įvykus nereikalinga m atimtis panaikinama pridedant m. Pagalbinio kubito atlaisvinimui iš gautos sumos $(x + y) \bmod m$ atimamas x ir nelygybė $(x + y) \bmod m - x \ge 0$ patikrinama svariausiu dvejetainės sistemos kubitu kaip perpildymo požymiu. Neperpildžius galiojant nelygybei $x + y < m$ $|1\rangle$ lygus pagalbinis kubitas atlaisvinamas valdomu neigimu. Atlaisvinimo metu atlikti pagalbiniai veiksmai panaikinami jiems atvirkščiais veiksmais. 12 pav. pavaizduota šiuo būdu įgyvendinta sudėties moduliu 7 kvantinių operatorių grandinė.



13 pav. Dviejų kintamųjų atimties moduliu 7 grandinė.

Sudėties moduliu kvantinių operatorių grandines galima paversti atimties moduliu grandinėmis įprastu būdu apverčiant grandine įgyvendintą unitarinį operatorių. Apvertus 12 pav. pavaizduotą dviejų kintamųjų sudėties moduliu 7 grandinę gaunama 13 pav. pavaizduota dviejų kintamųjų atimties moduliu 7 grandinė.

Visos aptartos moduliu 2^n skaičiuojančios kvantinių operatorių grandinės paremtos sudėties moduliu 2^n grandine. Pakeitus sudėtį sudėtimi moduliu p grandinės gali būti paverstos baigtiniuose kūnuose GF(p) skaičiuojančiomis kvantinių operatorių grandinėmis. Pakeitus daliklį kintamojo ir konstantos sandaugos kvantinių operatorių grandinėje fazės posūkio operatoriai atskiriami kitais operatoriais, todėl daugyba remiantis $P(\theta)^y = P(\theta y)$ tampa negalima. Konstantos ir kintamojo sandauga baigtiniuose kūnuose įgyvendinama pakartota sudėtimi.

3.6. Dalyba

Baigtiniuose kūnuose GF(p) kiekvienam nenuliniam elementui a galima rasti atvirkščią elementą a^{-1}. Sandauga su atvirkščiu elementu baigtiniame kūne tolygi dalybos veiksmui. Kintamojo x dalybai dalikliu konstanta y kvantinių operatorių grandinę galima sukurti klasikiniais skaičiavimais išplėstiniu Euklido algoritmu suskaičiuotą y^{-1} sudauginant su x kintamojo ir konstantos sandaugos kvantinių operatorių grandine. Dviejų kintamųjų dalybą įgyvendinama sudėtingiau. Išplėstinis Euklido algoritmas nėra patogiai skaičiuojamas kvantiniais skaičiavimais dėl apverčiamumo būtinybės, tačiau apverčiamumu negalima pasinaudoti dalybai gauti: dviejų kintamųjų daugybos kvantinių operatorių grandinė atlieka veiksmą $0 + xy$, kuriam atvirkščias veiksmas $0 - xy$. Atvirkštinio skaičiaus radimą palengvina Oilerio teorema. Oilerio funkcija $\phi(m)$ apibrėžiama kaip

$$\phi(m) = \text{skaičius tokių natūraliųjų } k,\ 1 \leq k \leq m, \text{ kad } \gcd(m,k) = 1. \tag{48}$$

Oilerio teorema teigia, kad

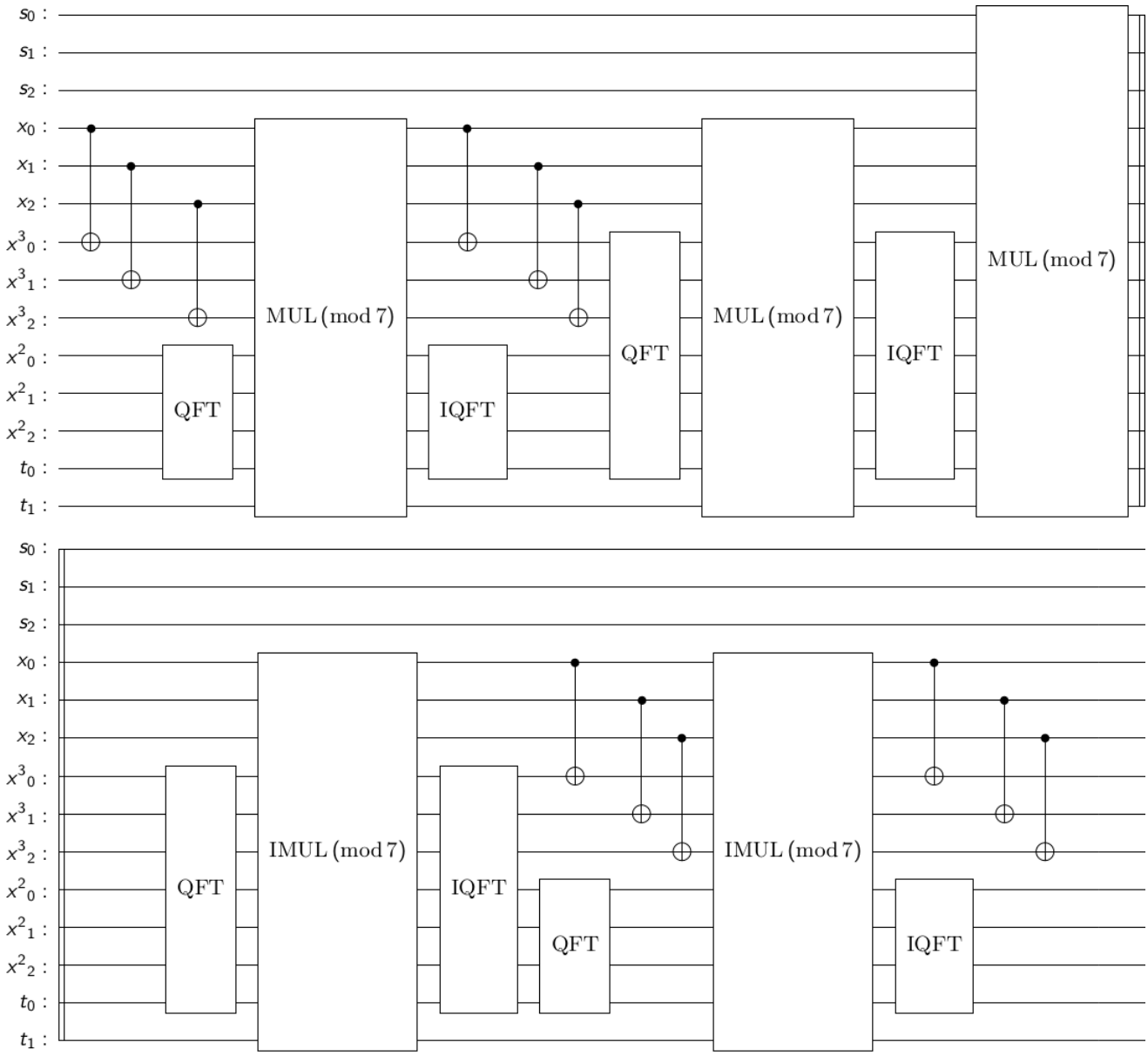
$$a^{\phi(m)} = 1 \bmod m, \quad a \neq 0. \tag{49}$$

Veiksmai baigtiniuose kūnuose atliekami moduliu pirminiu skaičiumi p. Pirminiam skaičiui p $\phi(p) = p - 1$. Tuomet

$$\begin{aligned} a^{\phi(p)} &= 1 \bmod p \quad | \cdot a^{-1}, \\ a^{\phi(p)-1} &= a^{-1} \bmod p, \\ a^{-1} &= a^{p-2} \bmod p. \end{aligned}$$

Kadangi p yra pastovus baigtiniam kūnui GF(p), y atvirkščias skaičius y^{-1} gali būti suskaičiuotas taikant dviejų kintamųjų sandaugos moduliu p kvantinių operatorių grandinę. Kėlimas laipsniu gali būti įgyvendintas įvairiais algoritmais, pavyzdžiui, kėlimo kvadratais algoritmu. 14 pav. pavaizduota GF(7) baigtiniame kūne atvirkštinį skaičių randanti kvantinių

operatorių grandinė $x^5 \equiv x^{-1} \pmod 7$ skaičiuoja seka x, x^2, x^3, x^5. Skaičiavimus baigus tarpinėms reikšmėms saugoti skirta atmintis atlaisvinama vykdant apverstą kvantinių operatorių grandinės dalį.



14 pav. Kintamajam x atvirkštinio skaičiaus $x^5 = x^{-1}$ radimo baigtiniame kūne GF(7) grandinė.

3.7. Tiesinės lygčių sistemos sprendimas GF(p)

Tiesinės lygčių sistemos plačiai taikomos įvairiose srityse pradedant fizika ir baigiant ekonomika. Tiesinių lygčių sistemų sudarymui ir sprendimui užtenka sudėties, atimties, daugybos ir dalybos veiksmų, todėl tiesinių lygčių sistemas galima sudaryti ir spręsti ir baigtiniuose kūnuose GF(p). Tiesinių lygčių sistemų sprendimas yra tinkamas įgyvendintų kvantinių skaičiavimų baigtiniuose kūnuose veikimo išbandymui.

Tiesinės lygčių sistemos klasikiniais skaičiavimais gali būti sprendžiamos Gauso metodu, leidimosi gradientu ar kitais sprendimo būdais. Klasikiniu kompiuteriu Gauso metodu n

kintamųjų n lygčių sistema sprendžiama $\mathcal{O}(n^3)$ laiko. Aptartomis kvantinių operatorių grandinėmis skaičiavimams baigtiniuose kūnuose įgyvendinti Gauso metodą nėra paprasta dėl naudojamo ir sunkiai suskaičiuojamo dalybos veiksmo. Baigtiniai kūnai turi baigtinį skaičių elementų, todėl lygčių sistemą baigtiniame kūne GF(p) klasikiniu kompiuteriu galima spręsti perrinkimu užtrunkant $\mathcal{O}(p^n)$ laiko. Kvantiniu kompiuteriu perrinkimas gali būti vykdomas trumpesniu $\mathcal{O}\left(\sqrt{2^{n\lceil \log_2 p \rceil}}\right)$ laiku pasitelkus Groverio paiešką.

Groverio paieškos algoritmas [Gro96] išskiria superpozicijos būseną pagal paieškos sąlygą nurodančią orakulo funkciją. Groverio paieškos pradinę sistemos būseną sudaro n kubitų lygiavertėje 2^n būsenų superpozicijoje. Uždaviniui pritaikyta orakulo funkcija išskiria ieškomą būseną paneigdama ieškomos būsenos amplitudę. Orakulo funkciją galima apibrėžti kaip unitarinį operatorių U išskiriantį būseną k, kurio elementus galima suskaičiuoti pagal

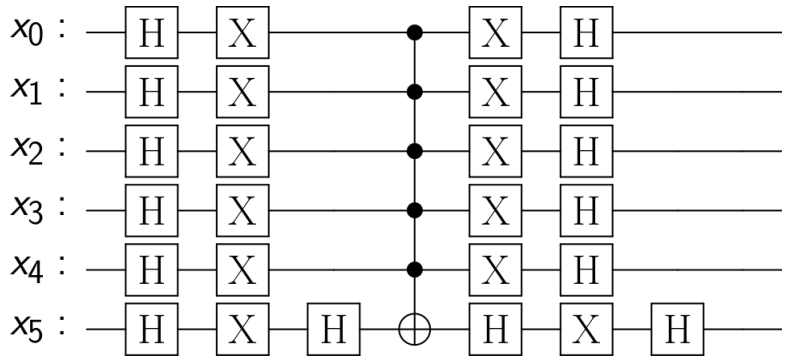
$$u_{ij} = \begin{cases} -1, & \text{jei } i = j \text{ ir } i = k, \\ 1, & \text{jei } i = j \text{ ir } i \neq k, \\ 0, & \text{jei kitaip.} \end{cases} \tag{50}$$

Groverio paieška vykdoma ciklais. Vieną Groverio paieškos ciklą sudaro ieškomos būsenos išskyrimas orakulo funkcija ir būsenų atskyrimas atspindint būsenas vidurkio atžvilgiu. Orakulo funkcija paneigia ieškomos būsenos amplitudę, todėl atspindint visų amplitudžių vidurkio atžvilgiu ieškomos būsenos amplitudė padidėja. Atspindžio vidurkio atžvilgiu unitarinis operatorius D išskaidomas į

$$D_{n\times n} = H^{\otimes n}(2|0^n\rangle\langle 0^n| - I)H^{\otimes n}. \tag{51}$$

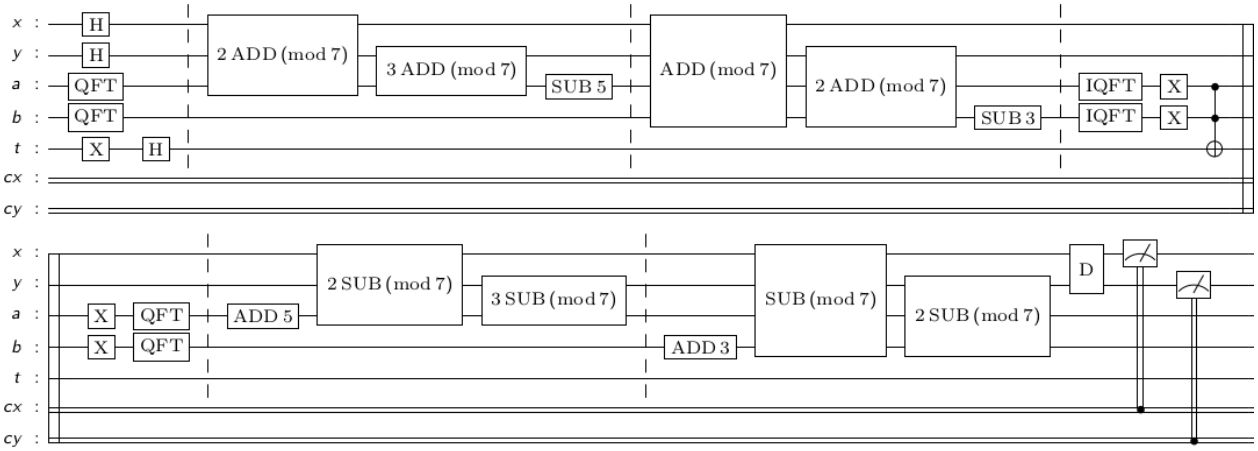
Groverio paieškos pradžioje visų būsenų amplitudės lygiavertėje superpozicijoje yra lygios $\frac{1}{\sqrt{2^n}}$. Kiekvieno Groverio paieškos amplitudės paneigimo ir atspindėjimo ciklo metu ieškomos būsenos amplitudė padidėja bent $\frac{2}{\sqrt{2^n}}$, todėl ieškomos būsenos amplitudė žymiai padidėja po $\sqrt{2^n}$ arba mažiau paieškos ciklų. Groverio paieškos algoritmą galima apibendrinti

$$\begin{aligned} |q_0\rangle &= H^{\otimes n}|0\rangle^{\otimes n}, \\ |q_i\rangle &= DU|q_{i-1}\rangle, \\ \text{matuojama būsena} \quad & |q_{\lfloor\sqrt{2^n}\rfloor}\rangle. \end{aligned}$$



15 pav. Atspindžio amplitudžių vidurkio atžvilgiu kvantinių operatorių grandinė, paieškos sritimi aprėpianti dviejų GF(7) kintamųjų verčių aibę.

Tiesinių lygčių sistemos, sudarytos iš n lygčių ir n GF(p) nežinomųjų sprendimui reikalinga $\lceil \log_2 p \rceil$ kubitų n kintamųjų būsenų paieška. Groverio paieškoje naudojamą atspindžio operatorių galima įgyvendinti kvantinių operatorių grandine pritaikant fazių atatrankos reiškinį būsenos fazei apsukti. 15 pav. pavaizduotas kvantinių operatorių grandine įgyvendintas šešių kubitų atspindžio operatorius D.



16 pav. Supaprastintai pavaizduota lygčių sistemą $\{2x + 3y = 5, x + 2y = 3\}$ baigtiniame kūne GF(7) sprendžianti kvantinių operatorių grandinė. Brėžinyje pavaizduotas tik vienas iš šešių Groverio paieškos ciklų.

Tiesinių lygčių sistemų sprendimui pasitelkiant Groverio paieškos algoritmą reikalinga lygybių teisingumą patikrinanti orakulo funkcija. Kiekvienai tiesinių lygčių sistemos

$$\begin{cases} c_{11}x_1 + c_{12}x_2 + \cdots + c_{1n}x_n = b_1 \\ c_{21}x_1 + c_{22}x_2 + \cdots + c_{2n}x_n = b_2 \\ \ldots \\ c_{n1}x_1 + c_{n2}x_2 + \cdots + c_{nn}x_n = b_n \end{cases}$$

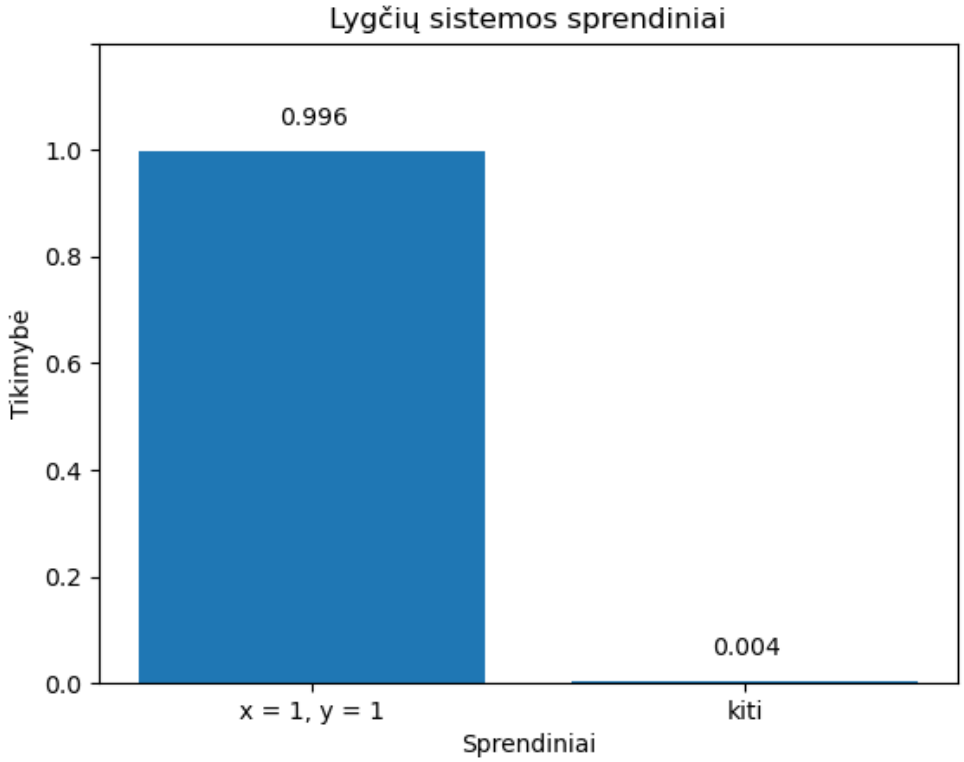
lygčiai sudaromos nuo nežinomųjų priklausančios sumos

$$
\begin{aligned}
&c_{11}x_1 + c_{12}x_2 + \cdots + c_{1n}x_n - b_1,\\
&c_{21}x_1 + c_{22}x_2 + \cdots + c_{2n}x_n - b_2,\\
&\ldots\\
&c_{n1}x_1 + c_{n2}x_2 + \cdots + c_{nn}x_n - b_n.
\end{aligned}
$$

Jei visos sumos lygios 0, nežinomųjų būsenos fazė apverčiama valdomu Paulio X operatoriumi veikiamos būsenos $|-\rangle$ sukelta fazių atatranka. Suskaičiuotos sumos panaikinamos paruošiant kitam Groverio paieškos ciklui, tuomet nežinomųjų būsena atspindima. Baigus Groverio paiešką nežinomieji matuojami sprendiniui gauti. 16 pav. supaprastinta kvantinių operatorių grandine pavaizduota sprendimo algoritmo pradžia ir pirmas Groverio paieškos ciklas bei matuojami kubitai tiesinių lygčių sistemos

$$
\begin{cases}
2x + 3y = 5\\
\ x + 2y = 2
\end{cases}
$$

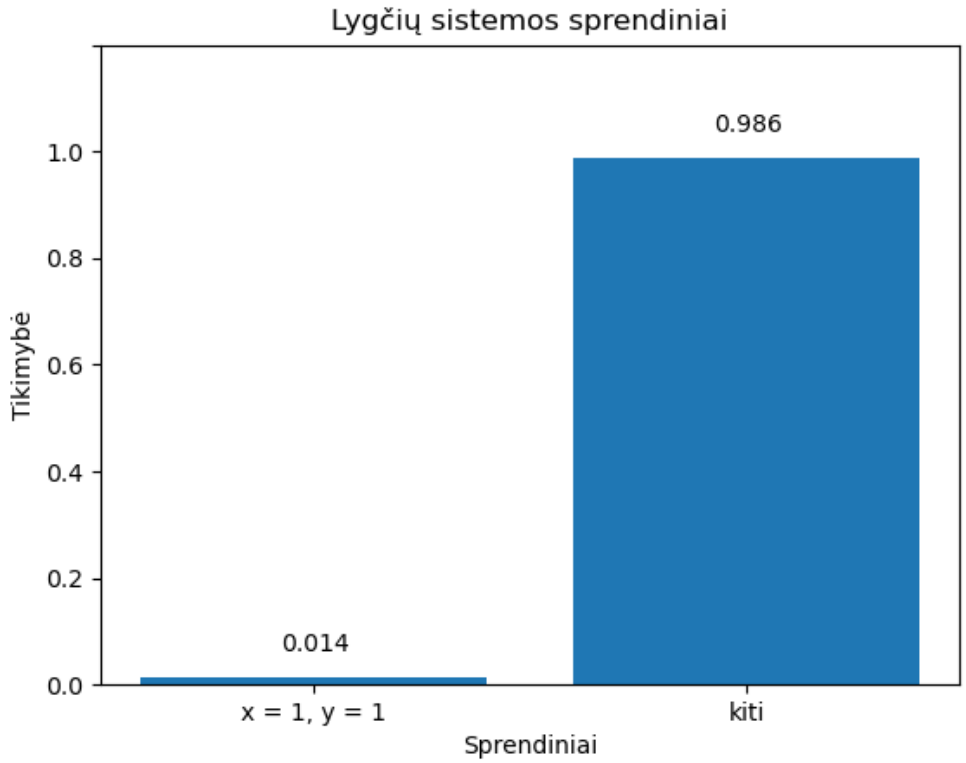
baigtiniame kūne GF(7) atveju.



17 pav. Kvantinių operatorių grandine rastų lygčių sistemos $\{2x + 3y = 5, x + 2y = 3\}$ baigtiniame kūne GF(7) sprendinių tikimybės, gautos vykdant grandinę „Qiskit“ simuliatoriumi. Teisingo lygties sprendinio $x = 1, y = 1$ tikimybė žymiai didesnė nei visų likusių x ir y derinių.

16 pav. pavaizduotą kvantinių operatorių grandinę šešiais Groverio paieškos ciklais įvykdžius „Qiskit“ kvantinių kompiuterių simuliatoriumi buvo gauta 17 pav. pavaizduota

grąžinto sprendinio tikimybių diagrama. Kvantiniame simuliatoriuje teisingas tiesinių lygčių sistemos sprendinys baigtiniame kūne GF(7) stebėtas žymiai dažniau nei visi likę neteisingi sprendiniai. Šis pavyzdys rodo, kad skaičiavimams baigtiniuose kūnuose sudarytos kvantinių operatorių grandinės geba atlikti skaičiavimus baigtiniuose kūnuose GF(p).



18 pav. Kvantinių operatorių grandine rastų lygčių sistemos $\{2x+3y=5, x+2y=3\}$ baigtiniame kūne GF(7) sprendinių tikimybės, gautos vykdant grandinę „IBMQ“ operatorių paklaidas modeliuojančiu simuliatoriumi. Teisingo lygties sprendinio $x=1, y=1$ tikimybė žymiai mažesnė nei visų likusių x ir y derinių dėl kvantinių operatorių veikimo paklaidų ir dekoherencijos.

16 pav. pavaizduota kvantinių operatorių grandinė negalėjo būti įvykdyta „IBMQ“ „ibmq_16_melbourne“ kvantiniu kompiuteriu dėl per didelio grandinės ilgio. Kvantinių operatorių grandinę įvykdžius kvantinių įrenginių paklaidas modeliuojančiu „IBMQ“ simuliatoriumi buvo gauta 18 pav. pavaizduota grąžinto sprendinio tikimybių diagrama. Kvantiniame simuliatoriuje įskaitant paklaidas teisingas tiesinių lygčių sistemos sprendinys baigtiniame kūne GF(7) stebėtas mažesne tikimybe nei visi likę neteisingi sprendiniai. Ilgesnėje grandinėje įsivyravus neidealaus kvantinio įrenginio paklaidoms ir aplinkos triukšmui būsenų tikimybės suvienodėja, tad vienintelis teisingas sprendinys iš 64 būsenų stebimas maždaug $\frac{1}{64}$ visų matavimų. Nors sudaryta kvantinių operatorių grandinė geba atlikti skaičiavimus baigtiniuose kūnuose GF(p) sprendžiant tiesines lygčių sistemas, šiuolaikinė kvantinė įranga nėra pakankamai pažengusi sudėtingesnėms kvantinių operatorių grandinėms vykdyti.

Rezultatai ir išvados

Šiame baigiamajame darbe buvo pristatyta darbe naudojama kvantinių kompiuterių teorijos dalis, aptartos tyrimo objekto — baigtinių kūnų GF(p) — savybės ir taikymo galimybės. Baigiamajame darbe buvo atlikti išsikelti uždaviniai:

1. kvantinių operatorių grandinėmis įgyvendinti sudėties, atimties, daugybos ir dalybos veiksmai baigtiniuose kūnuose GF(p):
   (a) aptarta ir įgyvendinta kvantinė Furjė transformacija ir jos atvirkštinė;
   (b) įgyvendinta kintamojo ir konstantos sudėtis Furjė skaičiavimo sistemoje;
   (c) įgyvendinta dviejų kintamųjų sudėtis;
   (d) įgyvendinta atimtis kaip sudėčiai atvirkščias veiksmas;
   (e) įgyvendinta kintamojo ir konstantos daugyba remiantis fazių posūkių sudedamumu;
   (f) įgyvendinta dviejų kintamųjų daugyba;
   (g) įgyvendinta sudėtis ir atimtis pasirinktu moduliu, reikalinga skaičiavimams GF(p);
   (h) įgyvendinta dviejų kintamųjų dalyba GF(p) remiantis Oilerio teorema;
2. naudojant įgyvendintas skaičiavimų baigtiniuose kūnuose grandines išspręsti tiesinių lygčių sistemą baigtiniame kūne GF(p):
   (a) aptartas Groverio paieškos algoritmas;
   (b) įgyvendinta tiesinės lygčių sistemos GF(7) orakulo funkcija;
   (c) dviejų kintamųjų tiesinių lygčių sistema GF(7) išspręsta Groverio paieška;
   (d) sprendimo kvantinių operatorių grandinė patikrinta kvantiniu simuliatoriumi;
3. patikrinti, kaip įgyvendinta lygčių sistemą sprendžianti kvantinių operatorių grandinė veikia tikrame kvantiniame įrenginyje:
   (a) tiesinių lygčių sistemos sprendimo kvantinių operatorių grandinė bandyta įvykdyti „IBMQ“ „ibmq_16_melbourne“ kvantiniu kompiuteriu;
   (b) sprendimo kvantinių operatorių grandinė įvykdyta „IBMQ“ paklaidas modeliuojančiu simuliatoriumi;
   (c) aptartos kvantinių operatorių grandinės paklaidos vykdant tikrame kvantiniame įrenginyje.

Veiksmai baigtiniuose kūnuose remiantis kvantine Furjė transformacija įgyvendinti aiškiomis, tačiau giliomis kvantinių operatorių grandinėmis. Kuo grandinė gilesnė, tuo joje labiau pasireiškia neidealių kvantinių įrenginių veikimo paklaidos. Vykdant kvantiniu simuliatoriumi sėkmingai veikianti kvantinių operatorių grandinė nebuvo tinkama skaičiavimui

tikrais šiuolaikiniais kvantiniais įrenginiais. Kvantiniams įrenginiams tobulėjant įmantrūs ir spartūs šiuolaikiniai teoriniai algoritmai taps įvykdomi.

Baigiamojo darbo metu buvo įgyvendinta tiesinių lygčių sistemą baigtiniame kūne Groverio paieškos algoritmu sprendžianti kvantinių operatorių grandinė. Įgyvendinta kvantinė grandinė sprendinį skaičiuoja $\mathcal{O}\left(\sqrt{2^{n\lceil \log_2 p \rceil}}\right)$ greičiu, tuo tarpu klasikinis Gauso algoritmas sprendinį geba skaičiuoti $\mathcal{O}(n^3)$ greičiu. Kvantinis HHL algoritmas įprastas tiesinių lygčių sistemas gali spręsti $\mathcal{O}\left(\frac{\log(n)s^2\kappa^2}{\epsilon}\right)$ greičiu. Jei HHL algoritmu būtų galima skaičiuoti baigtiniuose kūnuose, tiesinių lygčių sistemos baigtiniuose kūnuose galėtų būti sprendžiamos logaritminiu greičiu. Šį darbą būtų galima tęsti ieškant būdų HHL algoritmą pritaikyti tiesinių lygčių sistemoms baigtiniuose kūnuose spręsti.

Literatūra

[ABB+21] Abraham Asfaw, Luciano Bello, Yael Ben-Haim, Sergey Bravyi ir k.t. Learn Quantum Computation Using Qiskit, 2021. URL: http://community.qiskit.org/textbook. Tikrinta 2021-05-28.

[BBF03] Stephane Beauregard, Gilles Brassard ir Jose M. Fernandez. Quantum Arithmetic on Galois Fields, 2003. arXiv: 0301163 [quant-ph].

[Bea03] Stephane Beauregard. Circuit for Shor's algorithm using 2n+3 qubits, 2003. arXiv: 0205095v3 [quant-ph].

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search, 1996. arXiv: quant-ph/9605043 [quant-ph].

[YM08] Noson S. Yanofsky and Mirco A. Mannucci. *Quantum Computing for Computer Scientists*. Cambridge University Press, Cambridge, UK, 2008. 138–169 psl.

[JAA+18] Abhijith J., Adetokunbo Adedoyin, John Ambrosiano, Petr Anisimov ir k.t. Quantum Algorithm Implementations for Beginners, 2018. arXiv: 1804 . 03719 [cs.ET].

[KWA19] Daniel Koch, Laura Wessing ir Paul M. Alsing. Introduction to coding quantum algorithms: a tutorial series using qiskit, 2019. arXiv: 1903.04359 [quant-ph].

[RG17] Lidia Ruiz-Perez ir Juan Carlos Garcia-Escartin. Quantum arithmetic with the quantum Fourier transform. *Quantum Information Processing*, 16(6), 2017-04. ISSN: 1573-1332. DOI: 10.1007/s11128-017-1603-1. URL: http://dx.doi.org/10.1007/s11128-017-1603-1.

Priedas nr. 1
Programų išeities tekstai

Įgyvendintų programų išeities tekstai pasiekiami `https://github.com/maciulisleonardas/quantum-finite-fields` kaip „Python“ kalbos užrašinės.