Dar vienas ypatingas kvantinis algoritmas – kaip rasti informaciją nesutvarkytoje duomenų aibėje?

R. Čiegis

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

Birželio 17 d., 2025, Vilnius

Šio seminaro tikslas yra pratęsti susipažinimą su kvantiniu pasauliu.

Taip, jis gali būti keistas, prieštaraujantis mūsų intuicijai.

Bet kai šiek tiek geriau šį pasaulį pažįstame, tai pamatome, kad jame galioja pagrindinė taisyklė – jis pažinus ir valdomas (tiesa, dėsniai gali mums pasirodyti keistoki, o kodėl jie turėtų būti žmonėms lengvai suprantami?).

Turime kvantinę būseną

$$|\psi\rangle = \sum_{x=0}^{N-1} \alpha_x |x\rangle ,$$

$$a_x \geq 0, \quad 0 \leq x < N.$$

Turime kvantinę būseną

$$|\psi\rangle = \sum_{x=0}^{N-1} \alpha_x |x\rangle ,$$

$$a_x \geq 0, \quad 0 \leq x < N.$$

Kai atliekame matavimą, tai su tikimybe $|\alpha_x|^2$ gauname rezultatą, atitinkantį x-ąją bazinių vektorių būseną.

Turime kvantinę būseną

$$|\psi\rangle = \sum_{x=0}^{N-1} \alpha_x |x\rangle ,$$

$$a_x \geq 0, \quad 0 \leq x < N.$$

Kai atliekame matavimą, tai su tikimybe $|\alpha_x|^2$ gauname rezultatą, atitinkantį x-ąją bazinių vektorių būseną.

Sakykime, kad norime išmatuoti k-tąją būseną.
Lov Grover 1996 pasiūlė idėją, kuri yra gana akivaizdi, paprasta, bet tikrai talentinga.

Turime kvantinę būseną

$$|\psi\rangle = \sum_{x=0}^{N-1} \alpha_x |x\rangle ,$$

$$a_x \geq 0, \quad 0 \leq x < N.$$

Kai atliekame matavimą, tai su tikimybe $|\alpha_x|^2$ gauname rezultatą, atitinkantį x-ąją bazinių vektorių būseną.

Sakykime, kad norime išmatuoti k-tąją būseną.
Lov Grover 1996 pasiūlė idėją, kuri yra gana akivaizdi, paprasta, bet tikrai talentinga.

Prieš atliekant matavimą reikia modifikuoti būsenų vektoriaus koeficientus taip, kad reikalingą būseną atitinkantis koeficientas taptų esmingai didžiausias $|\alpha_k|^2 \approx 1$.

Turime kvantinę būseną

$$|\psi\rangle = \sum_{x=0}^{N-1} \alpha_x |x\rangle ,$$

$$a_x \geq 0, \quad 0 \leq x < N.$$

Kai atliekame matavimą, tai su tikimybe $|\alpha_x|^2$ gauname rezultatą, atitinkantį x-ąją bazinių vektorių būseną.

Sakykime, kad norime išmatuoti k-tąją būseną.
Lov Grover 1996 pasiūlė idėją, kuri yra gana akivaizdi, paprasta, bet tikrai talentinga.

Prieš atliekant matavimą reikia modifikuoti būsenų vektoriaus koeficientus taip, kad reikalingą būseną atitinkantis koeficientas taptų esmingai didžiausias $|\alpha_k|^2 \approx 1$.

Tokią idėją Grover pritaikė kvantinio paieškos algoritmo sudarymui. Tai ir bus mūsų seminaro tikslas.

Šiandien sieksiu parodyti, kad ir kvantinių skaičiavimų atveju svarbiausias darbas yra sudaryti veiksmingus algoritmus ir juos pagrįsti.

Šiandien sieksiu parodyti, kad ir kvantinių skaičiavimų atveju svarbiausias darbas yra sudaryti veiksmingus algoritmus ir juos pagrįsti.

Kvantinių algoritmų realizavimas irgi yra svarbus etapas, bet tai galima efektyviai atlikti naudojant pvz. Qiskit įrankius.

Kvantinis informacijos paieškos algoritmas

- Turime sąrašą argumento reikšmių $X = \{0, 1, \ldots, 2^n - 1\}$. Pažymėkime $N = 2^n$.

Kvantinis informacijos paieškos algoritmas

- Turime sąrašą argumento reikšmių $X = \{0, 1, \ldots, 2^n - 1\}$. Pažymėkime $N = 2^n$.
- Taip pat turime funkciją $f(x) \in \{0, 1\}, \quad x \in X$.

  Reikia rasti tokius $x \in X_1 \subset X$, kai $f(x) = 1$.

Kvantinis informacijos paieškos algoritmas

- Turime sąrašą argumento reikšmių $X = \{0, 1, \ldots, 2^n - 1\}$. Pažymėkime $N = 2^n$.
- Taip pat turime funkciją $f(x) \in \{0, 1\}, \quad x \in X$.

  Reikia rasti tokius $x \in X_1 \subset X$, kai $f(x) = 1$.

Kvantinis informacijos paieškos algoritmas

- Turime sąrašą argumento reikšmių $X = \{0, 1, \ldots, 2^n - 1\}$. Pažymėkime $N = 2^n$.
- Taip pat turime funkciją $f(x) \in \{0, 1\}, \quad x \in X$.

  Reikia rasti tokius $x \in X_1 \subset X$, kai $f(x) = 1$.

  Funkcija f dar vadinama *orakulu* (*Eng. oracle*), *ji apibrėžia vieną ar kelias "pažymėtas" bazines būsenas.*

Kvantinis informacijos paieškos algoritmas

- Turime sąrašą argumento reikšmių $X = \{0, 1, \ldots, 2^n - 1\}$. Pažymėkime $N = 2^n$.
- Taip pat turime funkciją $f(x) \in \{0, 1\}, \quad x \in X$.

  Reikia rasti tokius $x \in X_1 \subset X$, kai $f(x) = 1$.

  Funkcija f dar vadinama *orakulu* (*Eng. oracle), ji apibrėžia vieną ar kelias "pažymėtas" bazines būsenas.*
- Nesutvarkytose aibėse paieškos algoritmų sudėtingumas yra $\mathcal{O}(N)$.

Nagrinėkime tokį svarbų kriptografijoje orakulo atvejį.

Populiarios simetrinės šifravimo sistemos DES (Data Encryption Standard) saugumas yra grindžiamas rakto K saugumu. Šio rakto ilgis yra 2^{56} bitai.

Nagrinėkime tokį svarbų kriptografijoje orakulo atvejį.

Populiarios simetrinės šifravimo sistemos DES (Data Encryption Standard) saugumas yra grindžiamas rakto K saugumu. Šio rakto ilgis yra 2^{56} bitai.

Sakykime, kad per 10 sekundžių galime patikrinti 2^{25} rakto variantus (tai gana tikslus šiuolaikinių asmeninių kompiuterių skaičiavimo pajėgumo įvertis).

Nagrinėkime tokį svarbų kriptografijoje orakulo atvejį.

Populiarios simetrinės šifravimo sistemos DES (Data Encryption Standard) saugumas yra grindžiamas rakto K saugumu. Šio rakto ilgis yra 2^{56} bitai.

Sakykime, kad per 10 sekundžių galime patikrinti 2^{25} rakto variantus (tai gana tikslus šiuolaikinių asmeninių kompiuterių skaičiavimo pajėgumo įvertis).

Tada visų variantų patikrinimas užtruks 10×2^{31} sekundes, taigi ilgiau nei 700 metų.

Kvantinio Groverio algoritmo sudėtingumas yra $\mathcal{O}(\sqrt{N})$ (tuo įsitikinsime šiame seminare).

Kvantinio Groverio algoritmo sudėtingumas yra $\mathcal{O}(\sqrt{N})$ (tuo įsitikinsime šiame seminare).

Tarkime, kad mūsų kvantinio kompiuterio skaičiavimo greitis yra toks pat, kaip ir standartinio kompiuterio.

Tada rakto paieškai reikės atlikti tik 2^{28} algoritmo ciklus ir tai užtruks tik 80 sekundžių.

Kvantinis orakulo funkcijos f skaičiavimo operatorius

Tarkime, kad žinome klasikinį f skaičiavimo algoritmą.

Kvantinis orakulo funkcijos f skaičiavimo operatorius

Tarkime, kad žinome klasikinį f skaičiavimo algoritmą.

Priminsime, kaip tada sukonstruojame kvantinį šios funkcijos skaičiavimo operatorių

$$U_f(x,\phi): \quad |x,\phi\rangle \quad \rightarrow \quad |x,\phi \oplus f(x)\rangle\,,$$

čia $|x,f(x)\rangle = |x\rangle \otimes |f(x)\rangle$,

o $|\phi\rangle$ yra mūsų pasirinktas papildomas kubitas.

Groverio algoritmo bendroji schema

- Generuojame visų n kubitų superpoziciją Hilberto vektorinėje erdvėje (tokią operaciją jau daug kartų atlikome ankstesniuose seminaruose):

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

Groverio algoritmo bendroji schema

- Generuojame visų n kubitų superpoziciją Hilberto vektorinėje erdvėje (tokią operaciją jau daug kartų atlikome ankstesniuose seminaruose):

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

- Apskaičiuojame operatoriaus U_f vaizdą – tai tik vienas kvantinio algoritmo veiksmas

$$U_f : \quad |\psi, 0\rangle \quad \rightarrow \quad \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x, f(x)\rangle \, .$$

$$U_f : \quad |\psi, 0\rangle \quad \rightarrow \quad \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x, f(x)\rangle \, .$$

$$U_f : \quad |\psi, 0\rangle \quad \rightarrow \quad \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x, f(x)\rangle \, .$$

Pasirinkome pagalbinį kubitą $|\phi\rangle = |0\rangle$, tai nėra galutinis mūsų pasirinkimas, bet jis padės lengviau suprasti paieškos algoritmą.

$$U_f : \quad |\psi, 0\rangle \quad \to \quad \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x, f(x)\rangle \, .$$

Pasirinkome pagalbinį kubitą $|\phi\rangle = |0\rangle$, tai nėra galutinis mūsų pasirinkimas, bet jis padės lengviau suprasti paieškos algoritmą.

Jau žinome f reikšmes visose būsenose, taigi suradome ir mus dominančius taškus $x \in X_1$.

$$U_f : \quad |\psi, 0\rangle \quad \to \quad \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x, f(x)\rangle \, .$$

Pasirinkome pagalbinį kubitą $|\phi\rangle = |0\rangle$, tai nėra galutinis mūsų pasirinkimas, bet jis padės lengviau suprasti paieškos algoritmą.

Jau žinome f reikšmes visose būsenose, taigi suradome ir mus dominančius taškus $x \in X_1$.

Bet, jeigu dabar atliksime matavimą, tai sužinosime $f(x)$ reikšmę atsitiktinai parinktame taške (kodėl?) ir neteksime informacijos apie $f(x)$ reikšmes visuose kituose taškuose.

Pasiruošimas matavimo operacijai

Turime kvantinę būseną

$$|\psi\rangle = \sum_{x=0}^{N-1} \alpha_x |x\rangle ,$$

$$a_x \geq 0, \quad 0 \leq x < N.$$

Pakeičiame amplitudžių ženklus:

$$\alpha_x = \begin{cases} \alpha_x, & \text{jeigu } f(x) = 0, \\ -\alpha_x, & \text{jeigu } f(x) = 1. \end{cases}$$

Tokią operaciją atliekantį kvantinį operatorių žymėkime

$$Z_f : \quad |x\rangle \quad \rightarrow \quad (-1)^{f(x)} |x\rangle .$$

Atliekame inversijos transformaciją vidurkio atžvilgiu.

Čia pateikiame matematinį transformacijos apibrėžimą, panaudojant paprastus atvaizdžius.

Skaičiuojame vidurkį

$$A = \frac{1}{N} \sum_{x=0}^{N-1} \alpha_x$$

ir atliekame transformaciją

$$\alpha_x := 2A - \alpha_x, \quad x = 0, \ldots, N-1.$$

Kaip pavyzdį nagrinėkime pirmosios Groverio algoritmo iteracijos vykdymą.

Tarkime, kad $f(x_k) = 1$, o visuose kituose taškuose $f(x_j) = 0$.

Taip pat tarkime, kad pradiniu momentu visi koeficientai yra teigiami $\alpha_x > 0$ ir vienodi.

Atlikus vieną iteraciją $\alpha_k \approx 3\alpha_x$, $x \neq k$.

Atlikus vieną iteraciją $\alpha_k \approx 3\alpha_x$, $x \neq k$.

Po antros iteracijos koeficientas α_k dar padidėja kitų koeficientų atžvilgiu $\alpha_k \approx 5\alpha_x$, $x \neq k$.

Atlikus vieną iteraciją $\alpha_k \approx 3\alpha_x$, $x \neq k$.

Po antros iteracijos koeficientas α_k dar padidėja kitų koeficientų atžvilgiu $\alpha_k \approx 5\alpha_x$, $x \neq k$.

Atlikus $\frac{\pi}{8}\sqrt{N}$ iteracijų $\alpha_k^2 \approx \sum_{j \neq k} \alpha_j^2$.

Po $\frac{\pi}{4}\sqrt{N}$ iteracijų $\alpha_k^2 \approx 1 - \frac{1}{N}$.

Atlikus vieną iteraciją $\alpha_k \approx 3\alpha_x$, $x \neq k$.

Po antros iteracijos koeficientas α_k dar padidėja kitų koeficientų atžvilgiu $\alpha_k \approx 5\alpha_x$, $x \neq k$.

Atlikus $\frac{\pi}{8}\sqrt{N}$ iteracijų $\alpha_k^2 \approx \sum_{j \neq k} \alpha_j^2$.

Po $\frac{\pi}{4}\sqrt{N}$ iteracijų $\alpha_k^2 \approx 1 - \frac{1}{N}$.

Toliau didinant iteracijų skaičių koeficientų pasiskirstymas vėl artėja prie pradinio tolygaus pasiskirstymo.

Nagrinėkime pavyzdį: $n = 6$, $N = 64$. Tada gauname tokias tikimybes, kad išmatuosime reikalingą kubitą

$$\begin{aligned}
\text{it} = 0 \quad & p = 0.015625, \\
\text{it} = 1 \quad & p = 0.134827, \\
\text{it} = 2 \quad & p = 0.343895, \\
\text{it} = 3 \quad & p = 0.59138, \\
\text{it} = 6 \quad & p = 0.996586, \\
\text{it} = 12 \quad & p = 7.05e - 05.
\end{aligned}$$

Atlikę t Groverio algoritmo iteracijų, matuojame paskutinio kubito reikšmę. Jeigu gauname vienetą, tai turime Hilberto poerdvį

$$\frac{1}{\sqrt{2^k}} \sum_{i=1}^{k} |x_i, 1\rangle .$$

Išmatavę likusius kubitus gauname vieną iš ieškomų sprendinių $x_i \in X_1$.

Jeigu matuodami paskutinį kubitą gauname nulinę reikšmę, tai kartojame skaičiavimus.

Jau sužinojote visus pagrindinius Groverio algoritmo žingsnius.

Jau sužinojote visus pagrindinius Groverio algoritmo žingsnius.

Tikiu, kad tokios informacijos Jums visgi neužtenka. Norite sužinoti ne tik, kas bus, bet ir kodėl.

Jau sužinojote visus pagrindinius Groverio algoritmo žingsnius.

Tikiu, kad tokios informacijos Jums visgi neužtenka. Norite sužinoti ne tik, kas bus, bet ir kodėl.

Dabar atliksime ir pilnesnę matematinę analizę, aiškinančią šio algoritmo veikimą.

Matematika čia nėra sudėtinga, nors ji ir skirta kvantinės mechanikos procesų aptarimui.

Jau sužinojote visus pagrindinius Groverio algoritmo žingsnius.

Tikiu, kad tokios informacijos Jums visgi neužtenka. Norite sužinoti ne tik, kas bus, bet ir kodėl.

Dabar atliksime ir pilnesnę matematinę analizę, aiškinančią šio algoritmo veikimą.

Matematika čia nėra sudėtinga, nors ji ir skirta kvantinės mechanikos procesų aptarimui.

Labai svarbus lieka ir klausimas, kaip bendruoju atveju, kai gali egzistuoti ir daugiau nei viena "pažymėta" būsena, parenkame optimalų iteracijų skaičių.

Matome, kad reikalinga išsamesnė TEORIJA, pagrindžianti Groverio algoritmą.

Ženklų pakeitimo transformacija

Pateiksime universalų ir efektyvų būdą, kaip atlikti šią transformaciją. Tai pirmoji dalis bendro Groverio algoritmo.

Ženklų pakeitimo transformacija

Pateiksime universalų ir efektyvų būdą, kaip atlikti šią transformaciją. Tai pirmoji dalis bendro Groverio algoritmo.

Imkime tokį kontrolinį kubitą, jį naudosime skaičiuodami orakulo operatorių:

$$|\phi\rangle = H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Pažymėkime X_0 aibę būsenų $x \in X$, kur $f(x) = 0$, ir X_1 aibę, kur $f(x) = 1$.

Skaičiuokime funkcijos vaizdą

$$U_f(|\psi,\phi\rangle) = \sum_{x=0}^{N-1} \alpha_x U_f\,|x,\phi\rangle = \sum_{x\in X_0} \alpha_x U_f\,|x,\phi\rangle + \sum_{x\in X_1} \alpha_x U_f\,|x,\phi\rangle$$

$$= \frac{1}{\sqrt{2}}\Big(\sum_{x\in X_0} \alpha_x\,|x,0\oplus 0\rangle - \sum_{x\in X_0} \alpha_x\,|x,1\oplus 0\rangle + \sum_{x\in X_1} \alpha_x\,|x,0\oplus 1\rangle$$

$$- \sum_{x\in X_1} \alpha_x\,|x,1\oplus 1\rangle\Big) = \sum_{x\in X_0} \alpha_x\,|x,\phi\rangle + \sum_{x\in X_1} (-\alpha_x)\,|x,\phi\rangle\,.$$

Skaičiuokime funkcijos vaizdą

$$U_f(|\psi,\phi\rangle) = \sum_{x=0}^{N-1} \alpha_x U_f |x,\phi\rangle = \sum_{x\in X_0} \alpha_x U_f |x,\phi\rangle + \sum_{x\in X_1} \alpha_x U_f |x,\phi\rangle$$

$$= \frac{1}{\sqrt{2}}\Big(\sum_{x\in X_0} \alpha_x |x, 0\oplus 0\rangle - \sum_{x\in X_0} \alpha_x |x, 1\oplus 0\rangle + \sum_{x\in X_1} \alpha_x |x, 0\oplus 1\rangle$$

$$- \sum_{x\in X_1} \alpha_x |x, 1\oplus 1\rangle \Big) = \sum_{x\in X_0} \alpha_x |x,\phi\rangle + \sum_{x\in X_1} (-\alpha_x) |x,\phi\rangle .$$

Panaudodami operatorių Z_f galime taupiai užrašyti šį rezultatą:

$$Z_f |\psi\rangle = \sum_{x\in X_0} \alpha_x |x\rangle - \sum_{x\in X_1} \alpha_x |x\rangle .$$

Inversijos transformacija

Dabar aptarsime, kaip galima atlikti inversijos transformaciją:

Inversijos transformacija

Dabar aptarsime, kaip galima atlikti inversijos transformaciją:

$$D: \quad \sum_{x=0}^{N-1} \alpha_x |x\rangle \quad \rightarrow \quad \sum_{x=0}^{N-1} (2A - \alpha_x) |x\rangle ,$$

$$A = \frac{1}{N} \sum_{x=0}^{N-1} \alpha_x .$$

Inversijos transformacija

Dabar aptarsime, kaip galima atlikti inversijos transformaciją:

$$D: \quad \sum_{x=0}^{N-1} \alpha_x |x\rangle \quad \to \quad \sum_{x=0}^{N-1} (2A - \alpha_x) |x\rangle ,$$

$$A = \frac{1}{N} \sum_{x=0}^{N-1} \alpha_x .$$

Tai atlieka operatorius (kol kas tai tik matematinis apibrėžimas)

$$D = \begin{pmatrix} \frac{2}{N} - 1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} - 1 & \cdots & \frac{2}{N} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} - 1 \end{pmatrix} .$$

Inversijos transformacija

Dabar aptarsime, kaip galima atlikti inversijos transformaciją:

$$D: \quad \sum_{x=0}^{N-1} \alpha_x |x\rangle \quad \to \quad \sum_{x=0}^{N-1} (2A - \alpha_x) |x\rangle ,$$

$$A = \frac{1}{N} \sum_{x=0}^{N-1} \alpha_x .$$

Tai atlieka operatorius (kol kas tai tik matematinis apibrėžimas)

$$D = \begin{pmatrix} \frac{2}{N} - 1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} - 1 & \cdots & \frac{2}{N} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} - 1 \end{pmatrix} .$$

Nesunku patikrinti, kad D yra unitarusis:

$$D = D^\dagger, \quad DD = I .$$

Taip pat apibrėžiame dar vieną panašų operatorių, kuris irgi pakeičia kvantinių bazinių būsenų amplitudžių ženklus

$$Z_{OR}: \quad |x\rangle \rightarrow \begin{cases} |x\rangle, & x = 0^n, \\ -|x\rangle, & x \neq 0^n. \end{cases}$$

Nesunku patikrinti, kad Z_{OR} yra diagonalinis ir irgi unitarusis.

Taip pat apibrėžiame dar vieną panašų operatorių, kuris irgi pakeičia kvantinių bazinių būsenų amplitudžių ženklus

$$Z_{OR}: \quad |x\rangle \rightarrow \begin{cases} |x\rangle, & x = 0^n, \\ -|x\rangle, & x \neq 0^n. \end{cases}$$

Nesunku patikrinti, kad Z_{OR} yra diagonalinis ir irgi unitarusis.

Transformaciją D realizuojame taip:

$$D = H^{\otimes n} \, Z_{OR} \, H^{\otimes n}, \quad n = \log N.$$

Tada Groverio operatorių G užrašome taip:

$$G = H^{\otimes n} \, Z_{OR} \, H^{\otimes n} \, Z_f .$$

Tada Groverio operatorių G užrašome taip:

$$G = H^{\otimes n} Z_{OR} H^{\otimes n} Z_f.$$

Parodysime, kad šis operatorius veikia tik dvimatį visų kvantinių bazinių būsenų rinkinį ir todėl gali būti aprašytas 2×2 dydžio matrica (tai ir yra pagrindinė informacija, leidžianti ištirti Groverio algoritmo savybes).

Tada Groverio operatorių G užrašome taip:

$$G = H^{\otimes n} Z_{OR} H^{\otimes n} Z_f .$$

Parodysime, kad šis operatorius veikia tik dvimatį visų kvantinių bazinių būsenų rinkinį ir todėl gali būti aprašytas 2×2 dydžio matrica (tai ir yra pagrindinė informacija, leidžianti ištirti Groverio algoritmo savybes).

Apibrėžiame dvi nepriklausomas kvantinių būsenų superpozicijas

$$|\psi_0\rangle = \frac{1}{\sqrt{|X_0|}} \sum_{x \in X_0} |x\rangle , \quad |\psi_1\rangle = \frac{1}{\sqrt{|X_1|}} \sum_{x \in X_1} |x\rangle .$$

Tada gauname jau minėtą dviejų vektorinių struktūrų tiesinę kombinaciją:

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle = \sqrt{\frac{|X_0|}{N}}\, |\psi_0\rangle + \sqrt{\frac{|X_1|}{N}}\, |\psi_1\rangle\,.$$

Tada gauname jau minėtą dviejų vektorinių struktūrų tiesinę kombinaciją:

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle = \sqrt{\frac{|X_0|}{N}}\, |\psi_0\rangle + \sqrt{\frac{|X_1|}{N}}\, |\psi_1\rangle \,.$$

Pirmasis rezultatas yra trivialus

$$Z_f\, |\psi_0\rangle = |\psi_0\rangle \,, \quad Z_f\, |\psi_1\rangle = -\,|\psi_1\rangle \,.$$

Operatorių Z_{OR} galime išreikšti ir taip (patikrinte patys, tai labai paprastas pratimas):

$$Z_{OR} = 2\left|0^n\right\rangle\left\langle 0^n\right| - I.$$

Operatorių Z_{OR} galime išreikšti ir taip (patikrinte patys, tai labai paprastas pratimas):

$$Z_{OR} = 2\,|0^n\rangle\,\langle 0^n| - I.$$

Tada transformaciją vidurkio atžvilgiu galime užrašyti:

$$H^{\otimes n}\,Z_{OR}\,H^{\otimes n} = 2\,|\psi\rangle\,\langle\psi| - I,$$

Operatorių Z_{OR} galime išreikšti ir taip (patikrinte patys, tai labai paprastas pratimas):

$$Z_{OR} = 2\left|0^n\right\rangle\left\langle 0^n\right| - I.$$

Tada transformaciją vidurkio atžvilgiu galime užrašyti:

$$H^{\otimes n}\, Z_{OR}\, H^{\otimes n} = 2\left|\psi\right\rangle\left\langle\psi\right| - I,$$

o Groverio transformaciją

$$G = \left(2\left|\psi\right\rangle\left\langle\psi\right| - I\right) Z_f.$$

Atlikę nesudėtingus algebros skaičiavimus, gauname

$$G\left|\psi_0\right\rangle = \frac{|X_0| - |X_1|}{N}\left|\psi_0\right\rangle + \frac{2\sqrt{|X_0| \cdot |X_1|}}{N}\left|\psi_1\right\rangle,$$

$$G\left|\psi_1\right\rangle = -\frac{2\sqrt{|X_0| \cdot |X_1|}}{N}\left|\psi_0\right\rangle + \frac{|X_0| - |X_1|}{N}\left|\psi_1\right\rangle.$$

Šį operatorių atitinkanti 2×2 dydžio matrica M yra apibrėžiama taip

$$m_{ij} = \left\langle\psi_i\right| G\left|\psi_j\right\rangle, \quad 0 \leq i, j \leq 1,$$

ji yra tokia

$$M = \begin{pmatrix} \frac{|X_0|-|X_1|}{N} & -\frac{2\sqrt{|X_0|\cdot|X_1|}}{N} \\ \frac{2\sqrt{|X_0|\cdot|X_1|}}{N} & \frac{|X_0|-|X_1|}{N} \end{pmatrix}.$$

Nagrinėdami kvantinių unitariųjų transformacijų geometrines interpretacijas matome, kad jos apibrėžia posūkius, taip yra ir M atveju:

$$M = \begin{pmatrix} \sqrt{\frac{|X_0|}{N}} & -\sqrt{\frac{|X_1|}{N}} \\ \sqrt{\frac{|X_1|}{N}} & \sqrt{\frac{|X_0|}{N}} \end{pmatrix}^2 = \begin{pmatrix} \cos(2\theta) & -\sin(2\theta) \\ \sin(2\theta) & \cos(2\theta) \end{pmatrix},$$

čia

$$\theta = \sin^{-1}\left(\sqrt{\frac{|X_1|}{N}}\right).$$

Nagrinėdami kvantinių unitariųjų transformacijų geometrines interpretacijas matome, kad jos apibrėžia posūkius, taip yra ir M atveju:

$$M = \begin{pmatrix} \sqrt{\frac{|X_0|}{N}} & -\sqrt{\frac{|X_1|}{N}} \\ \sqrt{\frac{|X_1|}{N}} & \sqrt{\frac{|X_0|}{N}} \end{pmatrix}^2 = \begin{pmatrix} \cos(2\theta) & -\sin(2\theta) \\ \sin(2\theta) & \cos(2\theta) \end{pmatrix},$$

čia

$$\theta = \sin^{-1}\left(\sqrt{\frac{|X_1|}{N}}\right).$$

Pradinę būseną turime tokią

$$|\psi\rangle = \cos(\theta)\,|\psi_0\rangle + \sin(\theta)\,|\psi_1\rangle\,.$$

Tada viena Groverio iteracija pasuka šį vektorių kampu (2θ):

$$G\,|\psi\rangle = \cos(3\theta)\,|\psi_0\rangle + \sin(3\theta)\,|\psi_1\rangle\,.$$

Atlikus dvi iteracijas gauname kvantinę būseną

$$G^2 |\psi\rangle = \cos(5\theta) |\psi_0\rangle + \sin(5\theta) |\psi_1\rangle ,$$

o po t iteracijų:

$$G^t |\psi\rangle = \cos((2t+1)\theta) |\psi_0\rangle + \sin((2t+1)\theta) |\psi_1\rangle .$$

Atlikus dvi iteracijas gauname kvantinę būseną

$$G^2 |\psi\rangle = \cos(5\theta) |\psi_0\rangle + \sin(5\theta) |\psi_1\rangle ,$$

o po t iteracijų:

$$G^t |\psi\rangle = \cos((2t+1)\theta) |\psi_0\rangle + \sin((2t+1)\theta) |\psi_1\rangle .$$

Patikrinkime, kad jeigu turime kvantinę būseną

$$|\psi\rangle = \alpha |\psi_0\rangle + \beta |\psi_1\rangle = \frac{\alpha}{\sqrt{|X_0|}} \sum_{x \in X_0} |x\rangle + \frac{\beta}{\sqrt{|X_1|}} \sum_{x \in X_1} |x\rangle$$

tai tikimybė išmatuoti kurią nors būseną $x \in X_1$ yra lygi $|\beta|^2$.

Atlikus dvi iteracijas gauname kvantinę būseną

$$G^2 |\psi\rangle = \cos(5\theta) |\psi_0\rangle + \sin(5\theta) |\psi_1\rangle ,$$

o po t iteracijų:

$$G^t |\psi\rangle = \cos((2t+1)\theta) |\psi_0\rangle + \sin((2t+1)\theta) |\psi_1\rangle .$$

Patikrinkime, kad jeigu turime kvantinę būseną

$$|\psi\rangle = \alpha |\psi_0\rangle + \beta |\psi_1\rangle = \frac{\alpha}{\sqrt{|X_0|}} \sum_{x \in X_0} |x\rangle + \frac{\beta}{\sqrt{|X_1|}} \sum_{x \in X_1} |x\rangle$$

tai tikimybė išmatuoti kurią nors būseną $x \in X_1$ yra lygi $|\beta|^2$. Pagal apibrėžimą, tikimybė išmatuoti kažkurią konkrečią būseną $x \in X_1$ yra lygi $|\beta|^2/|X_1|$, o tokių būsenų skaičius $|X_1|$.

Groverio artinys po t iteracijų yra toks:

$$G^t |\psi\rangle = \cos((2t+1)\theta) |\psi_0\rangle + \sin((2t+1)\theta) |\psi_1\rangle .$$

taigi tikimybė išmatuoti kurią nors būseną $x \in X_1$ yra lygi

$$\sin^2 ((2t+1)\theta).$$

Groverio artinys po t iteracijų yra toks:

$$G^t |\psi\rangle = \cos((2t+1)\theta) |\psi_0\rangle + \sin((2t+1)\theta) |\psi_1\rangle .$$

taigi tikimybė išmatuoti kurią nors būseną $x \in X_1$ yra lygi

$$\sin^2 ((2t+1)\theta).$$

Norint, kad ši tikimybė būtų maksimali, o iteracijų skaičius būtų minimalus, reikia imti tokį iteracijų skaičių (natūralusis skaičius), kuris yra artimiausias

$$(2t+1)\theta = \frac{\pi}{2} \quad \rightarrow \quad t = \frac{\pi}{4\theta} - \frac{1}{2} \quad \rightarrow \quad t = \lfloor \frac{\pi}{4\theta} \rfloor .$$

Groverio artinys po t iteracijų yra toks:

$$G^t |\psi\rangle = \cos((2t+1)\theta) |\psi_0\rangle + \sin((2t+1)\theta) |\psi_1\rangle .$$

taigi tikimybė išmatuoti kurią nors būseną $x \in X_1$ yra lygi

$$\sin^2 ((2t+1)\theta).$$

Norint, kad ši tikimybė būtų maksimali, o iteracijų skaičius būtų minimalus, reikia imti tokį iteracijų skaičių (natūralusis skaičius), kuris yra artimiausias

$$(2t+1)\theta = \frac{\pi}{2} \quad \rightarrow \quad t = \frac{\pi}{4\theta} - \frac{1}{2} \quad \rightarrow \quad t = \lfloor \frac{\pi}{4\theta} \rfloor .$$

Jei turime tik vieną elementą aibėje X_1, tai

$$\theta = \sin^{-1}\left(\sqrt{\frac{1}{N}}\right) \approx \sqrt{\frac{1}{N}} \quad \rightarrow \quad t \approx \frac{\pi}{4}\sqrt{N}.$$

Jei turime s potencialių sprendinių, tai

$$\theta = \sin^{-1}\left(\sqrt{\frac{s}{N}}\right) \quad \rightarrow \quad t = \frac{\pi}{4\theta}, \quad t \approx \frac{\pi}{4}\sqrt{\frac{N}{s}}.$$

Jei turime s potencialių sprendinių, tai

$$\theta = \sin^{-1}\left(\sqrt{\frac{s}{N}}\right) \quad \rightarrow \quad t = \frac{\pi}{4\theta}, \quad t \approx \frac{\pi}{4}\sqrt{\frac{N}{s}}.$$

O kokią strategiją galime rekomenduoti iteracijų skaičiaus t parinkimui, jei neturime informacijos apie s ?