ДОСЛІДЖЕННЯ АЛГОРИТМІВ КВАНТОВИХ ОБЧИСЛЕНЬ

НТУУ «КПІ» ННК «ІПСА»
кафедра СП-САПР
Бочко Олексій Олександрович

АКТУАЛЬНІСТЬ РОБОТИ

- Квантові комп’ютери та алгоритми є новим перспективним напрямком сучасних інформаційних технологій.
- алгоритм Гровера для пошуку даних в неструктурованій БД дає квадратичне прискорення розв ́язку, що є актуальним при великих значеннях N(кількість елементів в БД).
- Квантовий алгоритм Шора дає можливість обчислити прості множники великих чисел за практично прийнятний час і зламати шифри RSA-криптосистем.

ЗАДАЧІ, ЩО ВИКОНУВАЛИСЯ

- Проведено аналіз передумов створення, принципів роботи та досягнутих на даний момент результаті в сфері побудови обчислювальних машин, що працюють з використанням квантової логіки.
- Розробка програмної моделі роботи квантових алгоритмів Гровера та Шора в середовищі MATLAB.
- Експериментальне дослідження розроблених моделей.
- Перевірка коректності роботи розроблених моделей.

ІСТОРІЯ ВИНИКНЕННЯ КВАНТОВИХ КОМП'ЮТЕРІВ

Р. Фейнман – в роботі «Моделювання фізики на компютерах» привернув увагу науковців до «квантових обчислень»

ІСТОРІЯ ВИНИКНЕННЯ КВАНТОВИХ КОМП'ЮТЕРІВ

1994р. Пітер Шор – запропонува квантовий алгоритм швидкої факторизації цілих чисел

ІСТОРІЯ ВИНИКНЕННЯ КВАНТОВИХ КОМП'ЮТЕРІВ

- 1996 р. Лов Гровер – квантовий алгоритм швидкого пошуку в неупорядкованій базі даних.

ПРИНЦИП РОБОТИ КВАНТОВОГО КОМП'ЮТЕРА

Основним елементом квантового комп'ютера є регістр із L кубітів.

Основні етапи роботи:

- Ініціалізація
- Виконання операцій
- Зчитування результату

КУБІТИ

- Основною відмінністю квантового біта - кубіта від класичного біта є те, що кубіт крім станів 0 і1 може також знаходитись в суперпозиції цих станів.
- Стан кубіта опсується вектором двох компонент:

$$\psi = a_0 |0\rangle + a_1 |1\rangle$$

$$|a_0|^2 + |a_1|^2 = 1$$

ОСНОВИ КВАНТОВИХ ОБЧИСЛЕНЬ

- Квантові гейти є аналогами булевських операцій AND, OR, NOT тощо
- Квантовий гейт що діє на n кубіт це унітарний $\mathbf{U} : \mathbb{C}^{2n} \rightarrow \mathbb{C}^{2n}$
- Приклад: гейт NOT

$$\mathbf{NOT} = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

ОСНОВИ КВАНТОВИХ ОБЧИСЛЕНЬ

- Квантові гейти є аналогами булевських операцій AND, OR, NOT тощо
- Квантовий гейт що діє на n кубіт це унітарний $\mathbf{U} : \mathbb{C}^{2n} \rightarrow \mathbb{C}^{2n}$
- Приклад: гейт NOT

$$\mathbf{NOT} = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

АЛГОРИТМ ГРОВЕРА

f(x) = 1

- S(0), S(1) . . . S(x) . . . S(N −1), N = 2^L для L кубитов

- 1. Рівноймовірносна суперпозиція. Амплитуды станів 1/sqrt(N)
- Вентель Адамара

$$|S\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} |y\rangle$$

- 2. Поворот фазы нужного состояния.

$$R|S(x)\rangle = -|S(x)\rangle$$

$$R|S(w)\rangle = |S(w)\rangle, w \neq x$$

- 3. Перетворення диффузії
- $D = 2P - I$, S(w) -

> - S(w) + 2*A,

- P – проекційна матриця с p = 1/N A – середня амплитуда

АЛГОРИТМ ГРОВЕРА

Основний цикл:

1. Initialize the system to the state

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle$$

2. Perform the following "Grover iteration" *r(N)* times. The function *r(N)*, which is asymptotically $O(N^{1/2})$, is described below.
    1. Apply the operator U_ω.
    2. Apply the operator U_s.
3. Perform the measurement Ω. The measurement result will be λ_ω with probability approaching 1 for N>>1. From λ_ω, ω may be obtained.

ПРИКЛАД АЛГОРИТМА ГРОВЕРА

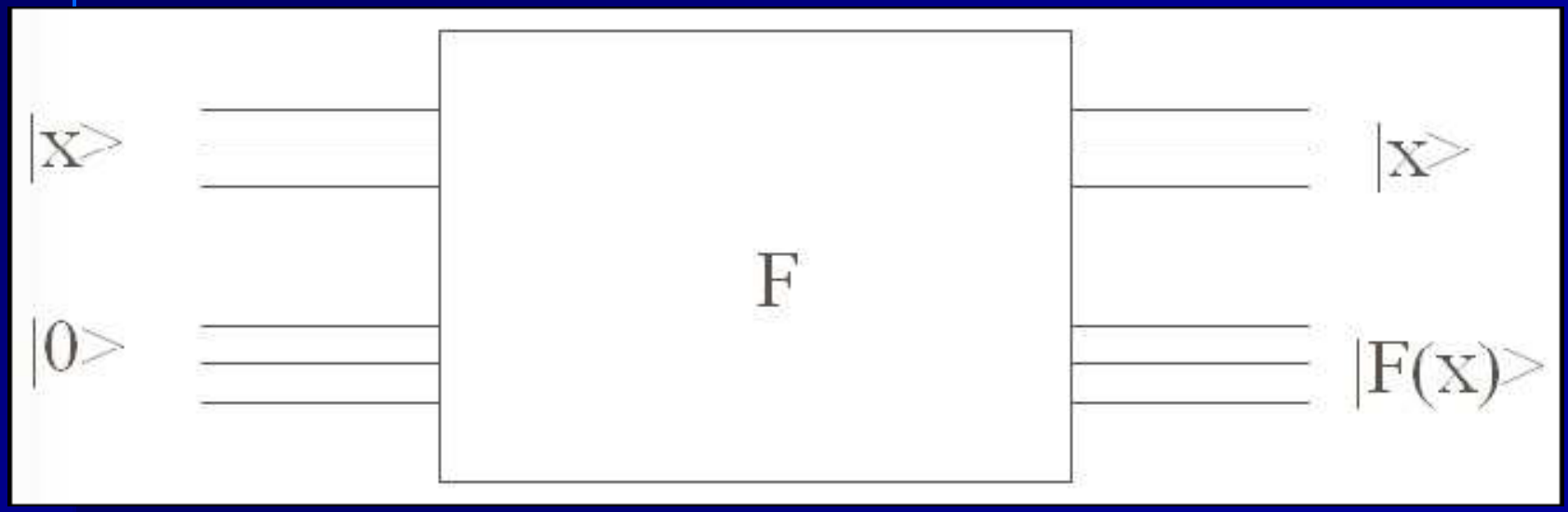
- L = 2 кубіта
- S(0), S(1), S(2), S(3), N = 4. Пусть |10⟩ - решение уравнения

- 1. Рівноймовірнісна суперпозиція. Амплітуди станів 1/2
- (½, ½, ½, ½)
- 2. Поворот фази станів |10⟩.
- (½, ½, -½, ½)
- 3. Перетворення дифузіїS(w) -> - S(w) + 2*A
- -(½, ½, -½, ½) + 2*(¼, ¼, ¼, ¼) = (0, 0, 1, 0)

:

АЛГОРИТМ ШОРА

- Ключова ідея – квантовий паралелізм



$$\sum_x |x\rangle|0\rangle \rightarrow \sum_x |x|\, f(x)\rangle\rangle$$

АЛГОРИТМ ШОРА

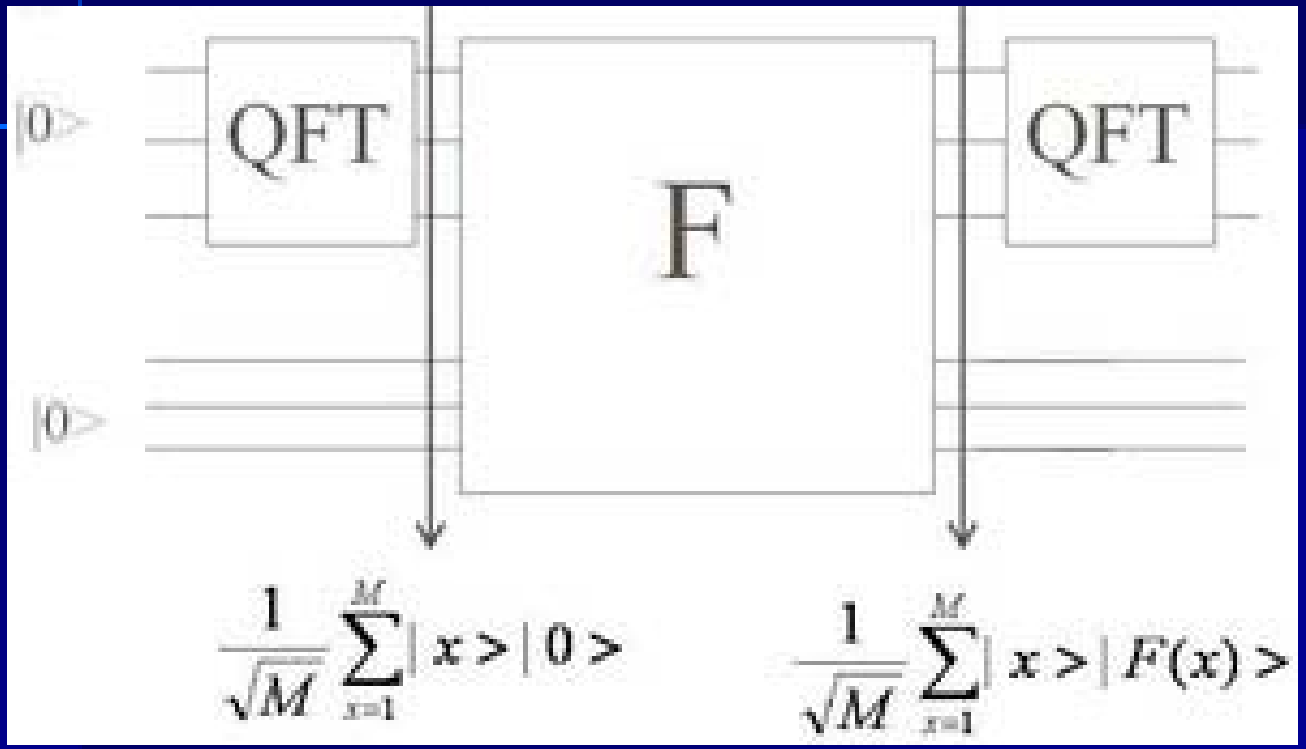
ОСНОВНІ КРОКИ:

1. Обрати випадковий залишок a по модулю N
2. Перевірити НСД(a, N)=1
3. Знайти порядок r залишка a по модулю N
4. Якщо r парний то обчислити НСД ($a^{r/2}$- 1, N)

Означення: минимальне r таке що $a^r \equiv 1 \pmod N$ называєтья порядком a по модулю N

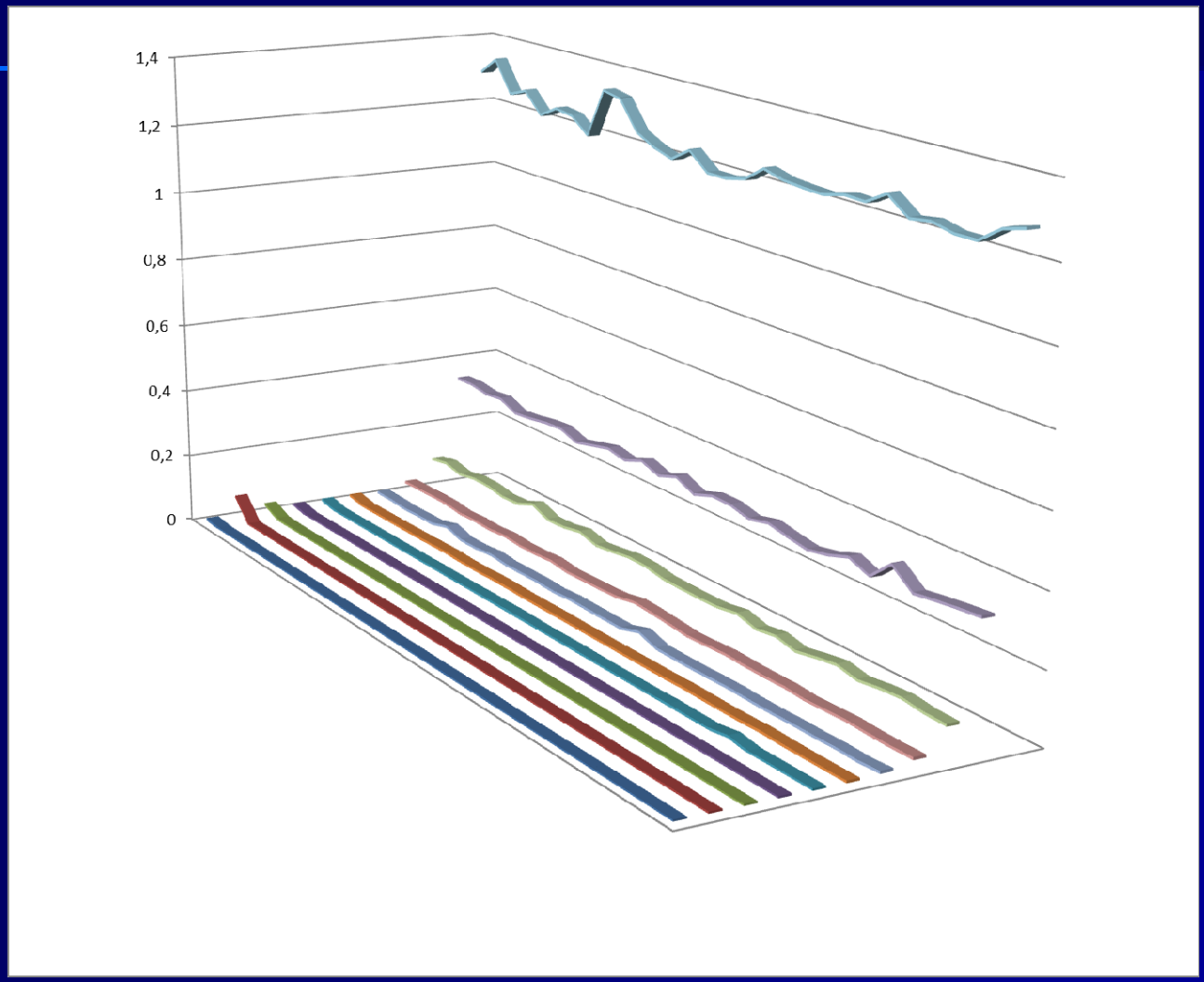
Порядок є періодом функції $f(x)=a^x \pmod N$

АЛГОРИТМ ШОРА



$$\mathbf{U}_{FT}\left|x\right\rangle = \frac{1}{\sqrt{\omega}}\sum_{k=0}^{\omega-1} e^{2\pi i k x/\omega}\left|k\right\rangle$$

РЕЗУЛЬТАТИ МОДЕЛЮВАННЯ АЛГОРИТМА ГРОВЕРА



РЕЗУЛЬТАТИ МОДЕЛЮВАННЯ АЛГОРИТМА ШОРА

>> shor(15, 3)
p = 3
q = 5
Elapsed time is 0.006218 seconds.
>> shor(35, 3)
p = 7
q = 5
Elapsed time is 0.003555 seconds.
>> shor(91, 23)
p = 7
q = 13
Elapsed time is 0.004315 seconds.
>> shor(221, 3)
p = 13
q = 17
Elapsed time is 0.003399 seconds.

ВИСНОВКИ

1. Обидва алгоритми змодельовано

ВИСНОВКИ

1. Обидва алгоритми змодельовано.
2. Переваг у часі роботи алгоритма Гровера не отримано

ВИСНОВКИ

1. Обидва алгоритми змодельовано.
2. Переваг у часі роботи алгоритма Гровера не отримано
3. Максимальним числом яке факторизує модель алгоритма Шора є 221

ВИСНОВКИ

1. Обидва алгоритми змодельовано.
2. Переваг у часі роботи алгоритма Гровера не отримано
3. Максимальним числом яке факторизує модель алгоритма Шора є 221
4. Алгоритми мають бути реалізовані на працюючих квантових компютерах з регістрами 1000 і більше кубіт.

ДЯКУЮ ЗА УВАГУ!