ЖУРНАЛ ФІЗИЧНИХ ДОСЛІДЖЕНЬ
т. 15, № 3 (2011) 3001(6 с.)

JOURNAL OF PHYSICAL STUDIES
v. 15, No. 3 (2011) 3001(6 p.)

КВАНТОВИЙ АЛҐОРИТМ ЕВОЛЮЦІЙНОГО АНАЛІЗУ ОДНОВИМІРНИХ КЛІТКОВИХ АВТОМАТІВ

Б. Павлишенко
Львівський національний університет імені Івана Франка
вул. Драгоманова, 50, 79005, Львів, Україна
(Отримано 4 лютого 2010 р.; в остаточному вигляді — 14 лютого 2011 р.)

У статті показано, що незворотну еволюцію класичного кліткового автомата можна реалізувати за допомогою квантового алґоритму при використанні додаткових квантових реґістрів анцил. Запропоновано алґоритм аналізу станів кліткового автомата, який базується на елементах алґоритму Ґровера — інверсії амплітуди шуканого стану та унітарного перетворення інверсії відносно середнього. Інверсія амплітуди шуканого стану здійснюється за допомогою квантового логічного елемента Тоффолі.
Ключові слова: квантовий комп'ютер, квантовий алґоритм, клітковий автомат.

PACS number(s): 03.67.Lx, 03.67.−a

ВСТУП

Одним із перспективних напрямків розвитку обчислювальних алґоритмів поряд із тюринговим програмуванням є використання кліткових автоматів. Клітковий автомат (КА) складається із системи комірок (кліток), які утворюють логічну ґратку [1]. Стан кожної комірки в деякий дискретний час характеризується деяким значенням змінної, яка є функцією станів локальних сусідніх комірок. Стан ґратки змінюється за законом, який визначається правилами переходів кліткового автомата. Зміна стану називається ітерацією. Системи, побудовані на машині Тюрінґа, складаються з незмінної активної частини, яка виконує алґоритмічні операції, та пасивної області даних. Кліткові автомати, на відміну від машин Тюрінґа, містять елементи, які одночасно відіграють як активну роль, виконуючи обчислювальні операції, так і пасивну роль змінних даних. Обчислювальна система на кліткових автоматах може оперувати власною структурою, змінюючи та розширюючи її. Цікавою властивістю кліткових автоматів є здатність при певних правилах переходів ґенерувати самовідтворювальні структури. Очевидно, що для деяких алґоритмів використання кліткових автоматів може бути набагато ефективнішим, ніж використання машини Тюрінґа внаслідок більшої кількості працюючих активних елементів. У структурі кліткових автоматів можна виділити множину кліток для вхідних та вихідних даних. Установлюючи наперед задані правила переходів, можна реалізувати ті чи інші алґоритми перетворення вхідних даних. Однак, це непросто внаслідок дуже складної поведінки кліткових автоматів навіть при простих правилах переходів. Як приклад, можна згадати гру "Життя", що запропонував Дж. Конвей, яка на двовимірній клітковій ґратці моделює еволюційний розвиток умовної популяції. Тому актуальним є вивчення еволюції кліткового автомата з метою добору правил переходів для заданого алґоритму.

Останнім часом активно розвивається теорія квантових обчислень. Розроблено ряд квантових алґоритмів, які дають суттєве прискорення розв'язку деяких задач унаслідок квантового паралелізму [2, 3]. Перспективним є використання квантових алґоритмів для аналізу еволюції кліткових автоматів з метою добору ефективних правил переходів. Квантові кліткові автомати (ККА) розглядають у багатьох роботах. У [4] описано ККА для універсальних квантових обчислень. У [5, 6] досліджено одномірні ККА. В [7] розглядається формалізм ККА ґратки кубітів. У [8, 9] досліджуються зворотні ККА. У [10,11] подано огляд досліджень ККА.

ПОСТАНОВКА ЗАДАЧІ

Мета роботи полягає в розробці квантових алґоритмів, які, використовуючи квантовий паралелізм, зможуть розрахувати при заданих правилах переходів усі еволюції кліткового автомата одночасно. Це дасть змогу дослідити, чи утворюються при цих правилах переходів кінцеві структури з наперед заданими характеристиками. В класичному випадку для цього потрібно провести послідовний розрахунок усіх можливих еволюцій КА, що може бути нездійсненним через експоненційно великий обсяг обчислень щодо логічних розмірів КА.

ОДНОВИМІРНІ КВАНТОВІ КЛІТКОВІ АВТОМАТИ

Ураховуючи складність багатомірних та багатостанових КА, розгляньмо такі одновимірні кліткові автомати, коли кожна клітка може перебувати лише у двох станах. Сусідні три клітки можуть перебувати у 8 різних станах, що утворює $2^8 = 256$ правил переходів клітки в новий стан на наступній ітерації. При чотирьох можливих станах таких правил може бути вже 2^{64} . Розгляньмо квантові логічні елементи, на основі яких можна побудувати одновимірний клітковий

автомат із вибраною схемою переходів. В основі квантових логічних елементів лежить поняття квантового біта — кубіта, який є вектором одиничної довжини у 2-вимірному комплексному векторному просторі з базисом $\{|0\rangle, |1\rangle\}$ [2, 3]. У класичному випадку n двостанових елементів утворюють $2n$-мірний простір. У квантових системах n кубітів утворюють простір вимірності 2^n. Розгляньмо клітку та її оточення з двох сусідів. Таку систему можна описати трьома кубітами з базисом

$$\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}. \quad (1)$$

Розгляньмо базові операції над кубітами. Оператор тотожного перетворення не змінює значення кубітів і в матричному записі має вигляд

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \quad (2)$$

Оператор заперечення X використовують для реалізації інверсії значень кубітів і його визначають так:

$$X = |0\rangle\langle 1| + |1\rangle\langle 0|. \quad (3)$$

У матричному зображенні оператор заперечення є таким:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \quad (4)$$

Одним із важливих елементів є 'контрольоване НЕ', яке здійснюється над двома кубітами і змінює значення другого кубіта на протилежне, якщо значення першого кубіта дорівнює 1. Цей логічний елемент можна визначити як

$$U_{\mathrm{CNOT}} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X, \quad (5)$$

а матриця оператора унітарного перетворення 'контрольоване НЕ' має вигляд

$$U_{\mathrm{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \quad (6)$$

Дію вентиля 'контрольоване НЕ' можна зобразити так:

$$U_{\mathrm{CNOT}} : |a, b\rangle \to |a, a \oplus b\rangle, \quad (7)$$

де $\oplus$ означає додавання за модулем 2. Ще одним важливим логічним елементом є вентиль Тоффолі, який діє на три кубіти і змінює значення третього кубіта на протилежне, якщо значення першого та другого кубітів дорівнює 1. Від логічного елемента 'контрольоване НЕ' вентиль Тоффолі відрізняється наявністю ще одного додаткового керуючого кубіта. Цей вентиль можна визначити як

$$T = |0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes U_{\mathrm{CNOT}}. \quad (8)$$

Перетворення Тоффолі можна зобразити так:

$$T : |a, b, c\rangle \to |a, b, c \oplus ab\rangle. \quad (9)$$

Вентиль Тоффолі є універсальним квантовим логічним елементом, на основі якого можна побудувати оборотну квантову машину Тюрінґа [2, 3].

Розгляньмо можливість реалізації синхронного кліткового автомата на квантових логічних елементах. Для визначеності розгляньмо одне із правил переходів у клітковому автоматі. Наприклад, клітка набуває значення 0, якщо обоє сусідів мають однакові значення, а в інших випадках клітка матиме значення 1. Таке правило можна записати у вигляді

$$x'[i] := x[i-1] \oplus x[i+1]. \quad (10)$$

У класичному клітковому автоматі така еволюція незворотна. Розгляньмо можливість реалізації цієї еволюції для квантового кліткового автомата при використанні додаткових реґістрів анцил. Якщо зберігати в цих реґістрах результати попередніх ітерацій, то можна досягнути зворотності та унітарності еволюції квантового кліткового автомата. Розгляньмо оператор реалізації правила (10), який діє на три кубіти — два сусідні $|x_{i-1}\rangle, |x_{i+1}\rangle$, та анцилу $|a_i\rangle$ з допоміжного реґістра:

$$C = (X \otimes X \otimes I) \cdot T \cdot (X \otimes X \otimes I) \cdot T \cdot (I \otimes I \otimes X). \quad (11)$$

На початку ітерації всі допоміжні анцили перебувають у стані

$$|0, 0, \ldots, 0\rangle_n \quad (12)$$

Послідовність унітарних перетворень для двох сусідніх кубітів $|x_{i-1}\rangle, |x_{i+1}\rangle$ та анцили $|a_i\rangle$ можна записати у вигляді

$$\begin{aligned} &C_i : I \otimes I \otimes X|x_{i-1}, x_{i+1}, 0\rangle \to T|x_{i-1}, x_{i+1}, 1\rangle \to |x_{i-1}, x_{i+1}, 1 \oplus x_{i-1}x_{i+1}\rangle \\ &\to X \otimes X \otimes I|x_{i-1}, x_{i+1}, 1 \oplus x_{i-1}x_{i+1}\rangle \to |\neg x_{i-1}, \neg x_{i+1}, 1 \oplus x_{i-1}x_{i+1}\rangle \\ &\to T|\neg x_{i-1}, \neg x_{i+1}, 1 \oplus x_{i-1}x_{i+1}\rangle \to |\neg x_{i-1}, \neg x_{i+1}, 1 \oplus x_{i-1}x_{i+1} \oplus \neg x_{i-1}\neg x_{i+1}\rangle \\ &\to X \otimes X \otimes I|\neg x_{i-1}, \neg x_{i+1}, 1 \oplus x_{i-1}x_{i+1} \oplus \neg x_{i-1}\neg x_{i+1}\rangle \to |x_{i-1}, x_{i+1}, x_i^{t+1}\rangle. \end{aligned} \quad (13)$$

Дію оператора C_i на можливі значення кубітів можна зобразити так:

$$
\begin{aligned}
&C_i : |0\rangle_{i-1,t}|0\rangle_{i+1,t}|0\rangle_{a,t+1} \to |0\rangle_{i-1,t}|0\rangle_{i+1,t}|0\rangle_{a,t+1}\\
&C_i : |1\rangle_{i-1,t}|1\rangle_{i+1,t}|0\rangle_{a,t+1} \to |1\rangle_{i-1,t}|1\rangle_{i+1,t}|0\rangle_{a,t+1}\\
&C_i : |1\rangle_{i-1,t}|0\rangle_{i+1,t}|0\rangle_{a,t+1} \to |1\rangle_{i-1,t}|0\rangle_{i+1,t}|1\rangle_{a,t+1}\\
&C_i : |0\rangle_{i-1,t}|1\rangle_{i+1,t}|0\rangle_{a,t+1} \to |0\rangle_{i-1,t}|1\rangle_{i+1,t}|1\rangle_{a,t+1}.
\end{aligned} \tag{14}
$$

Кубіт $|0\rangle_{a,t+1}$ належить до додаткового регістра анцил, який відображатиме стан кліткового автомата в наступний момент часу $t+1$. Під час унітарного перетворення C_i задіяними є лише кубіти $|x\rangle_{i-1,t}$, $|x\rangle_{i+1,t}$, $|0\rangle_{a,t+1}$, а щодо інших кубітів регістра автомата та анцил здійснюється перетворення тотожності I. На рис.1 наведено квантову схему реалізації правил переходів для КА (10)–(14)

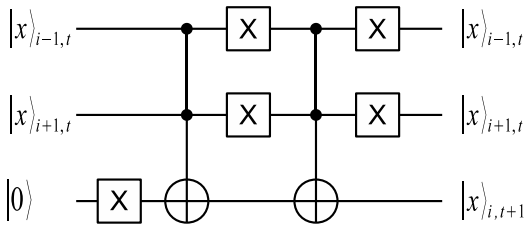

Рис. 1. Квантова схема реалізації правил переходів для КА.

Для однієї ітерації кліткового автомата необхідно провести унітарні перетворення C_i для всіх n кубітів регістру. J-у ітерацію кліткового автомата можна здійснити за допомогою такого оператора:

$$A_j = C_n \otimes \dots C_2 \otimes C_1. \tag{15}$$

Зобразимо першу ітерацію кліткового автомата з додатковим регістром анцил

$$A_1 : |x\rangle_0|0\rangle_1^{\otimes n} \to |x\rangle_0|f(x)\rangle_1, \tag{16}$$

де $|x\rangle = |x_1, x_2 \dots x_n\rangle$ — початковий стан кліткового автомата, $f(x)$ — деяка функція, що відображає правила переходів (10)–(14). На наступній ітерації додається ще один регістр анцил, і її можна зобразити так:

$$A_2 : |x\rangle_0|f(x)\rangle_1|0\rangle_2^{\otimes n} \to |x\rangle_0|f(x)\rangle_1|f(f(x))\rangle_2. \tag{17}$$

Еволюцію кліткового автомата після m ітерацій можна описати так:

$$A_m \dots A_2 A_1 : |x\rangle_0|0\rangle_1^{\otimes n} \dots |0\rangle_m^{\otimes n} \to |x\rangle_0|f(x)\rangle_1 \dots |f^{(m)}(x)\rangle_m. \tag{18}$$

Далі реалізуємо ітерацію, обернену до ітерації, що описується оператором A_{m-1}, таку, що

$$A_{m-1}(A_{m-1})^{-1} = I. \tag{19}$$

Дію такого оператора на сукупніть регістрів кубітів після m ітерацій (18) можна записати так:

$$(A_{m-1})^{-1} : |x\rangle_0|f(x)\rangle_1 \dots |f^{(m-1)}(x)\rangle_{m-1}|f^{(m)}(x)\rangle_m \to |x\rangle_0|f(x)\rangle_1 \dots |0\rangle_{m-1}^{\otimes n}|f^{(m)}(x)\rangle_m. \tag{20}$$

Для сукупності обернених перетворень отримаємо

$$(A_1)^{-1} \dots (A_{m-2})^{-1}(A_{m-1})^{-1} : |x\rangle_0|f(x)\rangle_1 \dots |f^{(m-1)}(x)\rangle_{m-1}|f^{(m)}(x)\rangle_m \to |x\rangle_0|0\rangle_1^{\otimes n} \dots |0\rangle_{m-1}^{\otimes n}|f^{(m)}(x)\rangle_m. \tag{21}$$

Унаслідок дії операторів зворотних еволюцій регістри додаткових анцил, які використовували як допоміжні для еволюції кліткового автомата, перебуватимуть в початковому стані й можуть бути вилучені із подальшого розгляду. Загальну еволюцію кліткового автомата можна описати таким оператором:

$$U_{CA} = (A_1)^{-1} \dots (A_{m-2})^{-1}(A_{m-1})^{-1} A_m A_{m-1} \dots A_1. \tag{22}$$

Вилучивши з розгляду додаткові регістри анцил, які перебувають у початковому стані, остаточну еволюцію квантового кліткового автомата можна описати так:

$$U_{CA} : |x\rangle|0\rangle^{\otimes n} \to |x\rangle|f^{(m)}(x)\rangle. \tag{23}$$

Розгляньмо послідовні кроки реалізації квантового кліткового автомата:

1. На початковому етапі регістр кубітів переведемо в нульовий стан

$$|x_1, x_2, \dots x_n\rangle_n \to |0_1, 0_2, \dots 0_n\rangle_n. \tag{24}$$

2. До кожного кубіта регістра застосуємо однокубітне перетворення Адамара, яке у спінорному

базисі зображається матрицею

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \qquad (25)$$

У результаті отримаємо

$$H^{\otimes n}|0_1, 0_2, \dots 0_n\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{x=1}^{x=2^n} |x\rangle, \qquad (26)$$

де $|x\rangle$ позначає номер базисного стану квантового регістра $|x_1, x_2, \dots x_n\rangle_n$. Перетворення Адамара приводить початковий стан (24) до суперпозиції всіх можливих станів із однаковою амплітудою.

3. Реалізуємо унітарне перетворення (23):

$$|\Psi_{CA}\rangle = U_{CA}\left(H^{\otimes n}|0\rangle^{\otimes n}\right)|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x=1}^{2^n} |x\rangle|f^{(m)}(x)\rangle. \qquad (27)$$

У суперпозицію $|\Psi_{CA}\rangle$ включено 2^n результатів еволюцій для кожного з 2^n початкових станів кліткового автомата вимірності n. Отже, протягом однієї квантової еволюції кліткового автомата реалізуються всі можливі еволюції для початкових станів при заданих правилах переходів.

АНАЛІЗ ЕВОЛЮЦІЇ КВАНТОВОГО КЛІТКОВОГО АВТОМАТА

Еволюція квантового кліткового автомата для заданих початкових станів однозначно задається правилами переходів. Щоб дослідити ці правила, необхідно проаналізувати еволюції для 2^n початкових станів кліткового автомата.

Розгляньмо можливість виявлення складних нетривіальних структур в еволюції КА при заданих правилах переходів. Така задача може виникати, наприклад, при пошуку правил ґенерації самовідтворювальних структур. Тобто виникає питання — чи може існувати деякий кінцевий стан,

$$|q\rangle = |e_1, e_2, \dots e_n\rangle, \qquad (28)$$

при заданих правилах переходу та деякій початковій комбінації. Амплітуда такого стану може бути $\sim \frac{1}{\sqrt{2^n}}$, якщо він трапляється лише один раз. Виявлення такого стану простим вимірюванням вимагає (2^n) спроб, що еквівалентно класичному випадку.

Розгляньмо можливість підсилити амплітуду шуканого стану, використовуючи ідеї алґоритму Ґровера, який використовують для пошуку у квантовій базі даних [15–17]. Відмінність цієї задачі від алґоритму Ґровера полягає в тому, що тут не шукаємо невідомого стану, який відповідає умові квантового оракула. Цей стан відомий і потрібно тільки дати відповідь, що він існує. Використаймо допоміжний кубіт, що керуватиметься n-мірним елементом Тоффолі, у якому керуючими кубітами виступають n кубітів кліткового автомата вихідного регістра результатів. Такий логічний елемент можна описати унітарною матрицею

$$T = \begin{pmatrix} 1 & \dots & \dots & 0 \\ \dots & \dots & \dots & \dots \\ \dots & \dots & 0 & 1 \\ 0 & \dots & 1 & 0 \end{pmatrix}. \qquad (29)$$

Розгляньмо деякий унітарний оператор, який є тензорним добутком однокубітних операторів

$$S_T = \bigotimes_{i=1}^{n} S_i, \qquad (30)$$

де

$$S_i = \begin{cases} I, & \text{якщо } e_i = 1 \\ X, & \text{якщо } e_i = 0 \end{cases}. \qquad (31)$$

Оператор S_T переводить шуканий стан $|e_1, e_2, \dots e_n\rangle$ у стан $|1_1, 1_2, \dots 1_n\rangle$. Це необхідно для того, щоб за допомогою перетворення Тоффолі (29) реалізувати інверсію керованого допоміжного кубіта $|z\rangle$ для шуканих станів. Подіємо на допоміжний $|z\rangle$ кубіт у приготованому стані $|1\rangle$ оператором Адамара

$$|z\rangle = H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \qquad (32)$$

Розгляньмо оператор

$$U_T = (I^{\otimes n} \otimes S_T \otimes I)(I^{\otimes n} \otimes T_n)(I^{\otimes n} \otimes S_T \otimes I). \qquad (33)$$

Подіємо цим оператором на систему регістрів кубітів у початковому та кінцевому станах системи $\frac{1}{\sqrt{2^n}} \sum_{x=1}^{x=2^n} |x\rangle|f^{(m)}(x)\rangle|z\rangle$. Перша справа група операторів, виділених дужками, реалізує перехід у стан $|1_1, 1_2, \dots 1_n\rangle$ шуканих кінцевих станів КА, друга група реалізує інверсію керованого кубіта для шуканих станів, третя — повертає змінені першою групою стани у стан перед застосуванням оператора (33). Допоміжний керований кубіт $|z\rangle$ після дії оператора (33) перебуває в стані (32). Унаслідок дії оператора (33) отримаємо

$$U_T\left(\frac{1}{\sqrt{2^n}} \sum_{x=1}^{x=2^n} |x\rangle|f^{(m)}(x)\rangle|z\rangle\right) = \frac{1}{\sqrt{2^n}}\left(\sum_{x \notin X_q} |x\rangle|f^{(m)}(x)\rangle - \sum_{x \in X_q} |x\rangle|q\rangle\right) \otimes |z\rangle, \qquad (34)$$

де X_q — множина початкових станів $|x\rangle$, які внаслідок еволюції кліткового автомата приводять до шуканого стану $|q\rangle$ після m ітерацій КА. Кубіт $|z\rangle$ у новому базисі не змінить свого значення, а в суперпозиції станів відбудеться інверсія знака амплітуди стану підсистеми $\sum_{x \in X_q} |x\rangle|q\rangle$. Це зумовлено тим, що перед дією оператора (34) кубіт був переведений у новий базисний стан (32), а інверсія стану в цьому базисі рівнозначна інверсії знака амплітуди підсистеми $\sum_{x \in X_q} |x\rangle|q\rangle$.

Розгляньмо оператор U_{CA}^{-1}, обернений до оператора (22), який описує еволюцію кліткового автомата, і для якого виконується умова

$$U_{CA}U_{CA}^{-1} = I. \tag{35}$$

Подіємо на систему (34) оператором U_{CA}^{-1}

$$U_{CA}^{-1}U_T\left(\frac{1}{\sqrt{2^n}}\sum_{x=1}^{x=2^n}|x\rangle|f^{(m)}(x)\rangle|z\rangle\right) \tag{36}$$

$$= \frac{1}{\sqrt{2^n}}\left(\sum_{x\notin X_q}|x\rangle - \sum_{x\in X_q}|x\rangle\right)\otimes|0_1,0_2,\dots 0_n\rangle_n\otimes|z\rangle.$$

У результаті дії оператора U_{CA}^{-1} отримаємо суперпозицію початкових станів однаковими амплітудами. Регістр анцил перебуває в початковому стані і може бути вилучений із подальшого розгляду. Для початкових станів, що приводять до шуканих кінцевих станів кліткових автоматів, значення амплітуд будуть від'ємними.

Для підсилення амплітуд станів $\sum_{x\in X_q}|x\rangle|q\rangle$ застосуймо оператор інверсії алґоритму Ґровера

$$U_G = 2|\Psi_c\rangle\langle\Psi_c| - I, \tag{37}$$

де

$$|\Psi_c\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}}\sum_{i=0}^{i=2^n-1}|i\rangle. \tag{38}$$

У геометричній інтерпретації оператор U_G здійснює в Гільбертовому просторі дзеркальне відображення деякого вектора щодо осі, яка визначається вектором $|\Psi_c\rangle$.

Оператор інверсії можна представити сукупністю однокубітних операторів Адамара та операторів інверсії стану кубіта щодо базисного вектора $|0\rangle$

$$U_G = H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n}. \tag{39}$$

Оператор (37) також називають оператором інверсії щодо середнього [15,17], оскільки його можна розглянути у вигляді

$$U_G : \sum_i a_i|i\rangle \to \sum_i (2A - a_i)|i\rangle, \tag{40}$$

де A — середнє значення амплітуд a_i.

Якщо шуканий стан $\sum_{x\in X_q}|x\rangle|q\rangle$ реалізується лише з однієї початкової комбінації кліткового автомата, то його амплітуда буде

$$\beta = \frac{1}{\sqrt{2^n}}. \tag{41}$$

Можна показати, що, реалізуючи ітерацію

$$U_G U_{CA}^{-1}U_T U_{CA}, \tag{42}$$

отримаємо підсилення амплітуди втричі, що аналогічно до реалізації ітерації інверсії в алґоритмі Ґровера пошуку у квантовій базі даних [15–17]. На рис. (2) наведено квантову схему реалізації унітарного перетворення (42)

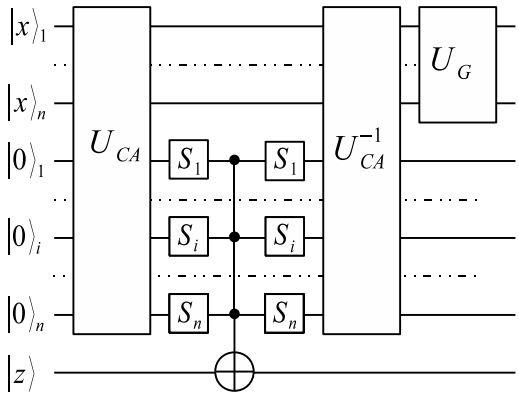

Рис. 2. Квантова схема реалізації унітарного перетворення $U_G U_{CA}^{-1}U_T U_{CA}$.

Розгляньмо кількість ітерацій, необхідних для достатнього підсилення амплітуди шуканого стану. Якщо лише один початковий стан $|x\rangle$ кліткового автомата приводить до шуканого кінцевого стану $|q\rangle$, то, використовуючи міркування, аналогічні до алґоритму Ґровера [15–17], можна знайти оптимальну кількість ітерацій унітарного перетворення (42)

$$k \approx \frac{\pi}{4}\sqrt{N}, N = 2^n. \tag{43}$$

Із цього результату випливає, що складність запропонованого алґоритму є $O(\sqrt{N})$, що в порівнянні зі складністю аналогічного класичного алґоритму $O(N)$ означає поліноміальне прискорення. Якщо маємо l таких початкових станів, які в результаті еволюції кліткового автомата приводять до шуканого кінцевого стану, то згідно з [15,17] отримаємо

$$k \approx \frac{\pi}{4}\sqrt{\frac{N}{l}}. \tag{44}$$

Якщо l є невідомим, тоді необхідно провести серію експериментів, для яких

$$L = 1, 2, 4, 8 \dots . \tag{45}$$

Можна показати, що для такої серії розрахунків складність обчислень буде також $O(\sqrt{N})$.

ВИСНОВОК

Реалізація одновимірних кліткових автоматів на квантових логічних елементах дає змогу побудувати квантові алґоритми аналізу правил переходів кліткових автоматів, які дають поліноміальне прискорення порівняно із класичними алґоритмами внаслідок реалізації квантового паралелізму. Показано, що незворотну еволюцію класичного кліткового автомата можна реалізувати за допомогою квантового алґоритму при використанні додаткових квантових реґістрів

анцил. Запропонований алґоритм аналізу станів кліткового автомата базується на елементах алґоритму Ґровера — інверсії амплітуди шуканого стану та унітарного перетворення інверсії відносно середнього. Інверсія амплітуди шуканого стану здійснюється за допомогою квантового логічного елемента Тоффолі.

ПОДЯКИ

Я щиро дякую професорові Володимирові Ткачукові та асистентові Юрію Криницькому за обговорення отриманих результатів, критичні зауваження та цінні поради.

[1] S. Wolfram, Physica D **10**, 1 (1984).
[2] Т. Крохмальський, Журн. фіз. досл. **8**, 1 (2004).
[3] А. Китаев, А. Шень, М. Вялий, *Классические и квантовые вычисления*, (МЦНМО, Москва, 1999).
[4] K. G. H. Vollbrecht, J. I. Cirac, Phys. Rev. A **73**, 012324 (2006).
[5] P. Arrighi, R. Fargetton, Z. Wang, arXiv:0704.3961v3 (2008).
[6] P. Arrighi, V. Nesme, R. Werner, arXiv:0711.3517v1 (2007)
[7] C. A. Perez-Delgado, arXiv:0709.0006v1 (2007).
[8] B. Schumacher, R. F. Werner, arXiv:quant-ph/0405174v1, (2004).
[9] Dirk-M. Schlingemann, H. Vogts, R. F. Werner, arXiv: 0804.4447v1 (2008).
[10] K. Wiesner, *Quantum Cellular Automata*, arXiv: 0808.0679v1 (2008).
[11] B. Aoun, M. Tarifi, *Introduction to Quantum Cellular Automata*, arXiv:quant-ph/0401123v1 (2004)
[12] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[13] C. Zalka, Phys. Rev. A **60**, 2746 (1999).
[14] C. Lavor, L. R. U. Manssur, R. Portugal, arXiv: quant-ph/0301079v1 (2003).
[15] L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[16] C. Zalka, Phys. Rev. A **60**, 2746 (1999).
[17] C. Lavor, L. R. U. Manssur, R. Portugal, arXiv:quant-ph/0301079v1 (2003).

QUANTUM ALGORITHM OF EVOLUTIONARY ANALYSIS OF ONE DIMENSIONAL CELLULAR AUTOMATA

B. Pavlyshenko
Ivan Franko National University of Lviv, Faculty of Electronics,
50, Drahomanov St., Lviv, 79005 Ukraine
e-mail: pavlsh@yahoo.com

It is shown that irreversible classical cellular automata can be performed by quantum algorithm using additional ancilla registers. An algorithm for cellular automata states analysis has been proposed. This algorithm is based on the elements of Grover's algorithm — the inversion of amplitude of searched states and unitary transform of inversion about the average. The inversion of searched states amplitudes can be performed by the quantum Toffoli gate.