ӘОЖ 530.145

ШОРДЫҢ КВАНТТЫҚ ФАКТОРИЗАЦИЯ АЛГОРИТМІ

Аманжолова Айслу Аманжолқызы
aisulu_2001.01@mail.ru
«Математика және компьютерлік ғылымдар»
білім бағдарламасының 2 курс магистранты
Х.Досмұхамедов атындағы Атырау университеті, Атырау қ, Қазақстан Республикасы
Ғылыми жетекшісі, ф.-м.ғ.к., профессор – **Шаждекеева Н.К.**

Аңдатпа

Шордың кванттық алгоритмі – бұл бүтін сандарды жай көбейткіштерге тиімді жіктеуге арналған кванттық есептеу әдісі. Ол дәстүрлі әдістермен салыстырғанда есептеу жылдамдығын едәуір арттырады және кванттық технологиялардың әлеуетін көрсетеді. Зерттеуде алгоритмнің жұмыс принциптері, қолдану салалары қарастырылады.

Кванттық есептеу – қазіргі заманғы ақпараттық технологиялардың ең қызықты және перспективалы, қарқынды дамып келе жатқан ғылыми бағыттарының бірі. Бұл салада соңғы жылдары көптеген жетістіктер мен жаңа бағыттар пайда болды, сондай-ақ классикалық есептеумен салыстырғанда кванттық есептеудің артықшылықтары айқындалды. Бұл саладағы жаңа жетістіктер мен ашылымдар ақпараттық технологиялардың дамуына ықпал етуде. Кванттық есептеу принциптері классикалық есептеу әдістерінен айтарлықтай ерекшеленеді.

Кванттық есептеу әдістерін зерттеу XX ғасырдың ортасында басталды. Ричард Фейнман мен Юрий Манин кванттық механика негізінде жұмыс істейтін есептеу жүйелерін қолдану идеяларын алғашқылардың бірі болып ұсынды. Кейінірек, 1994 жылы Питер Шор кванттық компьютерлердің дәстүрлі есептеуіш құрылғылармен шешуге қиын ірі сандарды көбейткіштерге жіктеу мәселесін тиімді шешуге қабілетті екенін көрсетті.[2]

Кванттық технологиялардың жедел дамуы ақпараттық қауіпсіздікке қатысты жаңа міндеттерді, әсіресе сандарды факторизациялау мәселесін шешу қажеттігін алға тартты. Осы саладағы маңызды жаңалықтардың бірі – Питер Шор 1994 жылы ұсынған кванттық факторизация алгоритмі. Бұл әдіс кванттық есептеулердің мүмкіндіктерін пайдалана отырып, үлкен құрама сандарды жай көбейткіштерге полиномиалдық уақыт ішінде тиімді түрде жіктеуге жол ашады. [1]

Шор алгоритмі факторизацияланатын санға байланысты функцияның периодын анықтауға негізделген. Осы периодты есептеу арқылы сандардың жай көбейткіштерін табуға болады. Бұл тәсіл, әсіресе криптография саласында маңызды рөл атқарады, себебі жай көбейткіштерге жіктеу – ақпараттық қауіпсіздіктің негізгі элементтерінің бірі.

Факторизация мәселесі

Үлкен сандарды факторизациялау – күрделілігі сандардың өлшемі артқан сайын экспоненциалды түрде өсетін есептеу міндеті. Яғни, разрядтар саны көбейген сайын, классикалық әдістермен бұл есепті шешу үшін айтарлықтай көп уақыт пен есептеу қуаты қажет болады. Мұндай өсу геометриялық прогрессияға сәйкес жүреді, сондықтан дәстүрлі компьютерлерде ірі сандарды жай көбейткіштерге жіктеу өте күрделі міндетке айналады.

Дегенмен, факторизациялау үшін бірнеше тиімді классикалық алгоритмдер қолданылады, олардың ішінде Шор алгоритмі ерекше орын алады. Осылайша, бұл алгоритм дәстүрлі факторизация әдістерімен салыстырғанда әлдеқайда жылдам жұмыс істейді. Алайда, қазіргі таңда кванттық компьютерлер әлі де даму кезеңінде тұр және кеңінен қолжетімді емес.

Факторизация мәселесі криптографияда ерекше маңызды рөл атқарады, өйткені сандарды жай көбейткіштерге жіктеудің күрделілігіне негізделген қауіпсіздік жүйелері кеңінен қолданылады. Мысалы, RSA шифрлау алгоритмі ірі құрама сандарды факторизациялаудың есептеу тұрғысынан қиын екендігіне сүйене отырып, мәліметтерді қорғау үшін қолданылады.

Кванттық факторизацияның классикалық әдістерден артықшылығы

Шордың кванттық алгоритмі жай көбейткіштерге жіктеу мәселесін шешуде классикалық алгоритмдермен салыстырғанда айтарлықтай артықшылықтары бар. Бұл алгоритм факторизация процесін экспоненциалды түрде жеделдетуге қабілетті. Яғни, кванттық компьютерде үлкен сандарды классикалық компьютерге қарағанда әлдеқайда жылдам факторизациялауға болады [4].

Алайда, Шор алгоритмін кванттық компьютерлерде жүзеге асыру белгілі бір қиындықтарға ие. Ол үшін жеткілікті түрде үлкен және тұрақты, көптеген кубиттері бар, қателік деңгейі төмен кванттық компьютер қажет. Сонымен қатар, кванттық күйлер мен операцияларды тиімді басқару және бақылау әдістерін әзірлеу қажет.

Шор кванттық факторизация алгоритмін сипаттау

Шор алгоритмі — кванттық есептеудің ең танымал алгоритмдерінің бірі, ол үлкен сандарды факторизациялауға арналған, яғни күрделі санды жай көбейткіштерге жіктеуге мүмкіндік беретін кванттық алгоритм. Оның негізгі принциптері:

1) Кванттық параллелизм: Алгоритм кванттық суперпозиция мен интерференцияны пайдалана отырып, факторизация процесін параллельді түрде жүзеге асырады.

2) Классикалық және кванттық кезеңдер: Алгоритм екі кезеңнен тұрады: кванттық кезең (суперпозиция мен өлшеу) және классикалық кезең (нәтижелерді өңдеу).

3) Қолдану: Шор алгоритмі криптографиялық жүйелердің (мысалы RSA) қауіпсіздігін бұзуға қабілетті, бұл оның практикалық маңыздылығын арттырады.

Шор алгоритмі сандарды факторизациялау үшін екі негізгі бөліктен тұрады – классикалық және кванттық. Классикалық бөлігі классикалық компьютерде орындалады және деректерді дайындау мен нәтижелерді талдауға арналған. Ол алгоритмнің кванттық бөлігінің кіріс деректерін алдын ала өңдеу мен шығыс деректерін түсіндіруде маңызды рөл атқарады.

Шор алгоритмінің кванттық бөлігі кванттық механиканың принциптерін – суперпозицияны (кубиттердің бір уақытта бірнеше күйлерде болу мүмкіндігі) және интерференцияны (әртүрлі кванттық күйлер ықтималдықтарының өзара әрекеттесуі) – факторизацияланатын санмен байланысты функцияның периодын тиімді анықтау үшін пайдаланады. Бұл принциптер кванттық компьютерге көптеген деректерді параллель түрде өңдеуге мүмкіндік береді және дұрыс жауаптардың ықтималдығын арттырады, нәтижесінде факторизация процесін айтарлықтай жылдамдатады.[3]

Шор алгоритмінің классикалық бөлімі

Факторизация алгоритмдерінің маңызды параметрі факторизацияланатын санның мөлшеріне байланысты тапсырманы орындау үшін қажетті ресурстардың өсу динамикасы болып табылады. Мысалы, кейбір үлкен N саны бізге белгісіз ($N = pq$) қарапайым p және q факторларынан тұрады деп елестетіп көрейік. Егер біз осы факторларды қарапайым шамадан тыс табу арқылы тапқымыз келсе, онда біз 2-ден $\sqrt{N}$-ге дейінгі барлық ықтимал факторларды сынап көруіміз керек, бұл жеткілікті үлкен N үшін іс жүзінде мүмкін емес операция. Бұл олардың жұмысында екі түрлі жай сандарды жасыруға мүмкіндік береді. Барлығы шығарманы көре алады, бірақ сандарды ешкім біле алмайды.

Шор алгоритміне тоқталайық: берілген N санын жай көбейткіштерге жіктеу қажет делік. Классикалық әдістерде бұл процесс экспоненциалды уақыт алады (мысалы, ең жылдам алгоритмдер $O\left(e^{(loglog\,N)^{1/3}}\right)$уақытында жұмыс істейді). Ал Шор алгоритмі полиномиалды уақыт ішінде (шамамен $O((log\ log\ N)^3)$ шешім табады.

Шор алгоритмінің орындалу кезеңдеріне тоқталайық:

1 – қадам: Кездейсоқ сан таңдау. Кездейсоқ a санын $(1 < a < N)$ таңдаймыз. ЕҮОБ$(a, N) \neq 1$ болса, онда ЕҮОБ$(a, N) - N$ санының көбейткіші, яғни шешім табылды.

2 – қадам:Кванттық периодты табу. Егер ЕҮОБ$(a, N) = 1$ болса, біз a -ның N бойынша (r) периодын табуымыз керек, мұнда:

$$a^r \equiv 1(mod\ N)$$

Классикалық әдіспен r табу қиындау, бірақ кванттық Фурье түрлендіруін (QFT) қолдана отырып, кванттық компьютер оны жылдам есептей алады.

3-қадам:Факторизацияны алу: Егер r – жұп сан болса, онда

$$N = \text{ЕҮОБ}(a^{r/2} - 1, N) \text{ немесе } N = \text{ЕҮОБ}(a^{r/2} + 1, N)$$

екенін тексереміз. Егер алынған ЕҮОБ саны N -ның көбейткіші болса, онда шешім табылды. [1]

$y < N$ санын алайық. ЕҮОБ $(y, N) = 1$ болатынын тексереміз.

Егер ЕҮОБ $(y, N) > 1$ болса, онда бізге ыңғайлы: біз N санының тривиалды емес бөлгішін табамыз. Сондықтан ЕҮОБ $(y, N) = 1$ деп есептейміз. Бұл жағдайда

$$y^r \equiv 1(N)$$

болатындай r натурал саны табылады.

Мысалы, $y^{\varphi(N)} \equiv 1(N)$, мұндағы $\varphi(N)$ – Эйлер функциясы, яғни N-нан кіші болатын сандар саны және N-мен өзара жай (Эйлер теоремасы).

Осындай ең кіші r саны N модулі бойынша y санының периоды деп аталады.

y санының N модулі бойынша периоды жұп $2s$ болсын. Онда

$y^{2s} - 1 = (y^s - 1)(y^s + 1)$ өрнегі N санына бөлінеді, бірақ $y^s - 1$ бөлінбейді N-ге. $y^s + 1$ бөлінбейді N-ге деп алайық. Онда

$$(y^s - 1)(y^s + 1) = kN = kpq$$

бұдан шығатыны $(y^s - 1)$ өрнегі p-ға, $(y^s + 1)$ өрнегі q-ға бөлінеді немесе керісінше.

Евклид алгоритмі көмегімен есептесек ЕҮОБ$(y^s \pm 1, N)$, онда біз тривиалды емес N санының бөлгішін табамыз, бұл тәсіліміз орындалу үшін, бірінші y санын дұрыс таңдау керек және N модулі бойынша y периодын есептей алу керек.

Мысалы: $N = 15$ болсын, $y = 13$ деп таңдап алайық және N модулі бойынша y периодын есептейміз.

$$13^2 = 169 \equiv 4(15)$$

$$13^3 = 4 \cdot 13 = 52 \equiv 7(15)$$

$$13^4 = 7 \cdot 13 = 91 \equiv 1(15)$$

15 модулі бойынша 13 периоды $r = 4$ болады. Бұл жұп сан.

$$y^4 - 1 = (y^2 - 1)(y^2 + 1)$$

$$13^4 - 1 = (13^2 - 1)(13^2 + 1) = 168 \cdot 170$$

Бұдан өзге, $13^2 + 1 = 170$ саны 15-ке бөлінбейді. Олай болса, $y = 13$ деп таңдауымыз сәтті болады.

$$\text{ЕҮОБ}\,(168{,}15) = 3 \text{ және ЕҮОБ}\,(170{,}15) = 5$$

есептеп, 15 санының екі жай көбейткішін таптық.

Лемма. N саны екі p мен q жай сандардың көбейтіндісі болсын, ал $S = \{y: 1 \le y < N,\ (y, N) = 1\}$.

Сонда, ең болмағанда $y \in S$ санының жартысының $2s$ жұп периоды болады және $(y^s + 1)$ бөлінбейді N-ге.

Бұл Лемма $y \in S$ санын қалай таңдасақ та, дұрыс таңдау кем дегенде $\frac{1}{2}$.

N санының көпшілігі үшін сәтті таңдау ықтималдығы көп. Бірақ, олар үшін бұл бағалау дәл болатын N бар болады, мысалы $N = 77$.

Бұл айтылған лемма y таңдау мәселесін анықтады деп есептесек, екінші мәселемен, яғни N модулі бойынша y периодын есептеумен айналысайық. Тізбектей y^2, y^3, y^4, ... - есептеу тіптен ұзақ, өйткені N модулі бойынша y периоды N-нен алынған Эйлер функциясы мәнінің жартысына жетуі мүмкін, яғни $\frac{(p-1)(q-1)}{2}$.

Шор алгоритмі – кванттық есептеулердің шынайы артықшылықтарын көрсететін алгоритмдердің бірі.

Қорытынды

Бұл мақалада Шор кванттық алгоритмінің жүзеге асырылуы қарастырылды. Жай көбейткіштерге жіктеу мәселесінің негізгі аспектілері мен кванттық факторизацияның классикалық әдістерден артықшылығы көрсетілді. Шор алгоритмі және оның жұмыс принциптері сипатталды.

Алгоритмді жүзеге асырудың күрделілігін бағалау көрсеткендей, оны тиімді қолдану үшін кванттық физика мен математиканы терең түсіну, сондай-ақ кванттық компьютерлерге немесе олардың эмуляторларына қолжетімділік қажет.

Шор алгоритмінің жүзеге асырылуы криптография мен ақпараттық қауіпсіздікке айтарлықтай әсер етеді. Бұл кванттық төзімді алгоритмдерді әзірлеу қажеттілігін тудырып, қазіргі қауіпсіздік әдістерін қайта қарастыруды талап етеді. Кванттық компьютерлердің дамуы мен Шор алгоритмінің жүзеге асырылуы кванттық есептеулер мен криптография саласындағы одан әрі зерттеулер мен жетілдірулерді қажет етеді.

Болашақта Шор кванттық факторизация алгоритміне байланысты қосымша зерттеулер мен әзірлемелер жүргізу жоспарлануда. Негізгі мақсаттардың бірі – кванттық компьютердегі кубиттер санын көбейту, бұл алгоритмді қолдану мүмкіндіктерін кеңейтеді. Сондай-ақ, кубиттер күйін дайындау және өлшеу процестерін оңтайландыру жоспарлануда, бұл есептеулердегі қателіктер ықтималдығын азайтуға және алгоритмнің тиімділігін арттыруға мүмкіндік береді. Сонымен қатар, Шор кванттық факторизация алгоритмінің әртүрлі салаларда қолданылу мүмкіндіктерін зерттеу де маңызды бағыттардың бірі болып табылады. Мысалы, бұл алгоритмді криптографияда жаңа шифрлау және дешифрлау әдістерін әзірлеу үшін пайдалану мүмкіндігін зерттеуге болады, олар кванттық компьютерлерді қолданатын шабуылдарға төзімді болады.

Қолданылған әдебиеттер тізімі:

1. Перри Райли Т. "Элементарное введение в квантовые вычисления" ИД Интеллект, 2018 г.

2. Душкин Р.В. Квантовые вычисления и функциональное программирование. / Р.В. Душкин 2014. — 318 с., Ил.

3. Сысоев С.С. Квантовые вычисления / С.С. Сысоев —2017. — 16 с., ил.

4. Нильсен М., Квантовые вычисления и квантовая информация / М. Нильсен , И. Чанг. — Пер.с англ— М:Мир, 2006 г.- 824с.