РЕЦЕНЗИЯ

на дисертационен труд на тема:

„КВАНТОВИ АЛГОРИТМИ "

с автор **Христо Светленов Тончев**,

за придобиване на образователната и научна степен „доктор"
по професионално направление 4.1.Физически науки,
Научна специалност 01.03.19 Физика на атомите и молекулите

Рецензент: доц. д-р Лъчезар Стоянов Георгиев,
Институт за ядрени изследвания и ядрена енергетика, Българска академия на науките

1. Общи данни за дисертанта.

Авторът на дисертацията е завършил висше образование като магистър през 2008 г. във Физическия факултет на СУ "Климент Охридски" със специалност физика и професионална квалификация „Теоретична и математическа физика". През 2012 г. е зачислен е като редовен докторант във Физическия факултет на СУ "Климент Охридски" с научен ръководител проф. дфн Николай Витанов. Положил е всички необходими изпити.

Авторефератът към дисертацията отразява вярно съдържанието на дисертацията, като отчита адекватно поставените цели и задачи, съдържанието на работата, получените резултати и научните приноси.

2. Актуалност на разработвания в дисертационния труд проблем в научно и научно-приложно отношение.

Алгоритмите за квантови компютри са от една страна най-важната част на квантовата информатика, тъй като показват какви задачи и до каква степен могат да се решават на един квантов компютър, а от друга – точно те демонстрират изчислителното превъзходство на квантовите компютри в сравнение с класическите им предшественици. Публикуването на алгоритъма на П. Шор през 1994 г., за факторизиране на големи числа на прости множители, който се оказва експоненциално по-бърз от всички известни класически алгоритми за факторизиране, доведе до неочаквано възраждане на интереса към квантовата теория, включително от страна на всякакви военни и разузнавателни служби, както и на компютърни и софтуерни гиганти като Майкорсóфт и Гугъл, и предизвика невиждан разцвет на квантовата информатика. Благодарение на някой специфични особености на квантовите системи, като квантово

сплитане и квантов паралелизъм, квантовите алгоритми обещават намирането на значително по-бързи и по-ефективни решения и на други сложни математически задачи като определяне на реда на модулно експоненциране, проблема за скритата подгрупа, определяне на периоди на функции, дискретни логаритми, бързо квантово търсене, както и квантова симулация на реални физически системи.

Без съмнение, изучаването на съществуващите алгоритми за квантови компютри, тяхното усъвършенстване и разработването на нови квантови алгоритми е изключително актуална научна тематика, която изисква солидни познания свързани с най-силните физически и математически резултати получени в рамките на квантовата теория през 20 век.

3. Познава ли дисертантът състоянието на проблема?

Дисертантът познава добре широката научна област на квантовите компютри и квантовите алгоритми. Запознат е с особеностите при разлагането на много-кюдитните квантови операции на дву-кюдитни контролирани гейтове. Усвоил е сложния математичен апарат на дискретната Фурие трансформация, алгоритъма за измерване на фазата на унитарен оператор и алгоритъма на Шор за факторизиране на цели числа на прости множители. Резултатите представени в образователната част на дисертацията, естествено не са нови, но са важни и са усвоени с разбиране, като са илюстрирани с интересни примери.

В допълнение към стандартния учебен материал по квантови компютри и алгоритми дисертантът е усвоил и по-специфични умения свързани с декомпозицията на произволна d- мерна квантова операция чрез Хаусхолдерови отражения и фазов гейт – това е използвано по същество в значителна част от дисертацията.

Целите и задачите поставени в дисертационния труд са продиктувани от стремежа да бъдат ускорени, опростени и направени по-ефективни известните алгоритми за квантови компютри.

4. Анализ на избраната методика

Използването на системи с d нива (кюдити) е обещаващо обобщение на системите с две нива (кюбити). От една страна кюдитите, макар да не представляват принципно различие в сравнение с кюбитите, предоставят по-бързи и по-ефективни изчислителни възможности за квантовите компютри. От друга страна, в природата съществуват много квантови системи с повече от две (почти изродени) дискретни квантови състояния, които естествено могат да бъдат описани чрез кюдити. Не на последно място, в много от примерите за построяване на реален квантов компютър, увеличаването на броя на кубитите е технологически ограничено и единствената възможност за повишаване на изчислителната мощ на квантовия компютър е чрез увеличаване на размерността на Хилбертовото пространство отговарящо на единичния квантов регистър, т.е, чрез използване на кутрити (квантови системи с три нива) и в общия случай – на кюдити.

В дисертацията и в публикациите върху които тя е изградена е показано, че за обобщаване на квантовия алгоритъм на Гровер за търсене в индексирано множество, за работа върху кюдити, не е задължително да се използва дискретната Фурие трансформация както това е демонстрирано по-рано, за реализацията на която са необходими много повече условия върху физическото взаимодействие между кюдитите и много повече конструктивни стъпки. Вместо това е достатъчно да бъде построена унитарна матрица, която да трансформира много-кюдитното състояние $|0,0,\ldots,0\rangle$ в равно-теглова суперпозиция на всички състояния от изчислителния базис.

В допълнение към това е направено обобщение на алгоритъма за пресмятане на фазата и квантов брояч за определяне на броя на решенията на алгоритъма на Гровер с кюдити. При тази реализация само таргет-регистъра е изграден от кюдити, докато контролния регистър е изпълнен само от кубити, тъй като за изпълнение на контролирани квантови операции са достатъчни само две състояния. Направени са числени симулации, при които таргет-регистъра е изграден от кютрити и е показано, че ефективността на брояча с кютрити се повишава, а в същото време се повишава и вероятността за намиране на броя на решенията на задачата за квантово търсене.

Получените резултати в дисертацията показват, че използването на кютрити и в общия случай на кюдити в квантовия алгоритъм на Гровер и в квантовия брояч на решенията му повишава значително ефективността на алгоритъма и вероятността за намиране на броя на решенията.

Друг успешен подход към ускоряване на алгоритмите за търсене от гледна точка на методиката е използването на случайни (недетерминистични) подходи от типа на произволно придвижване (random walk). В дисертацията са използвани две разновидности на квантово случайно придвижване, в които времето се променя дискретно или непрекъснато. Както класическите така и квантовите методи за случайно придвижване могат да решават определени задачи за търсене по-ефективно и по-бързо от конкурентните детерминистични класически или квантови методи.

5. Обобщена характеристика на дисертационния труд

Дисертацията е посветена на обобщаването, за реализация чрез кюдити, на основни квантови алгоритми използвани в квантовите компютри, формулирани първоначално за кюбити.

Дисертацията е в обем от 144 страници, съдържа 76 фигури, структурирани като Увод, четири глави, списък на използваните литературни източници съдържащ 91 публикации и Заключение. В Увода и в Глава 1 са представени основните положения на квантовите компютри и квантовите алгоритми и има подчертано образователен характер, показващ, че дисертантът е усвоил основните понятия и методологията на научната тематика. Останалите Глави представят оригинални теоретични научни изследвания с фундаментален характер. В Глава 2 е разгледан алгоритъмът на Гровер за квантово търсене в номерирано множество от обекти, използващ кюдити, като са предложени два реални аналога на матрицата на Адамар използвана в случая на кюбити, както и една комплексна унитарна матрица. В Глава 3, след представяне на известните резултати за кюбити, е разгледан квантовият алгоритъм за определяне на

фазата, реализиран върху кюдити, както и построяването на квантов брояч за алгоритъма на Гровер с кюдити. Представените симулации използващи кютрити показват значително увеличаване на ефективността в сравнение с кюбитите както и повишаване на вероятността за намиране на решение на задачата за квантово търсене. В Глава 4, като допълнение към алгоритъма на Гровер е изследван алгоритъма за квантовото търсене с произволно преместване върху хиперкуб, с използване на асиметрични монети. Представена е числена симулация на този алгоритъм и е направено сравнение на алгоритъма за квантовото търсене с произволно преместване върху хиперкуб с квантовия алгоритъм за търсене на Гровер.

6. Научни или научно-приложните приноси на дисертационния труд

За обобщението на алгоритъма на Гровер за търсене върху база данни индексирана с кюдити са въведени две нови реални, унитарни и симетрични матрици H_1 и H_2, които са аналог на матрицата на Адамар за кюбити. Предимството на тези матрици при реализацията на алгоритъма е, че не се налага намирането на обратната матрица, което е неизбежно при използването на Фурие трансформацията. За тези два случая е направена компютърна симулация на действието на алгоритъма на Гровер с кютрити при различен брой кютрити и различен елемент на търсене. Показано е как се променя вероятността за намиране на търсения елемент при пространство на търсене от 3 кютрита в зависимост от броя итерации в алгоритъма на Гровер.

Построен е квантов алгоритъм за определяне на фазата и квантов брояч върху кюдити, като в контролния регистър са използвани кюбити докато в таргет регистъра са използвани кютрити. Това дава възможност да се направи CNOT гейт, необходим за алгоритъма за определянето на фазата. Този алгоритъм от своя страна е необходим за конструирането на квантов брояч за алгоритъма на Гровер върху кюдити. Представени са числени симулации на алгоритъма на квантовия брояч с кюбити и кютрити при различна големина на регистрите и различен брой на елементите на търсене. Симулирани са предложените комплексни и реални аналози на гейта на Адамар (F^{-1}, F, H_1 и H_2) . Демонстрирано, че заедно с експоненциалното нарастване на размера на таргет-регистъра, вероятността за намиране на броя решения при използване на кютрити, респективно с кюдити, се увеличава значително.

Друг важен принос в дисертацията е представеният квантов алгоритъм за търсене с произволно преместване с дискретно време, използващ асиметрични монети, при които вероятността за преминаване на съседен възел е несиметрична. Тази модификация на алгоритъма за квантово случайно преместване е оптимизирана за търсене върху възлите на хирперкуб, който представлява граф с 2^n на брой възли и n на брой ръбове между тях. Предложен е нов метод за разделяне на хиперкуб на две части, чрез използване на асиметрични монети, получени от Хаусхолдеров оператор, при което не променя оператора на смесване. Показано е, че разделянето чрез подходящи асиметрични монети, може да доведе до удвояване на вероятността за намиране на решение. Предложени са четири различени нови монети, които дават най-добри резултати, като за всяка от тях са предложени нови квантови вериги на алгоритъма за търсене с произволно преместване върху хипиркуб. Направени са числени симулации на квантово търсене с произволно преместване при използването на новите монети, резултатите от които са представени графично. Направено е сравнение на алгоритъма за квантовото търсене с произволно преместване върху хиперкуб с квантовия

алгоритъм за търсене на Гровер като са анализирани предимствата и недостатъците на всеки от тези алгоритми за търсене.

7. Преценка на публикациите по дисертационния труд

Дисертационният труд се основава на 3 публикации в реферирани международни списания, от които 2 в списание с импакт-фактор - Phys. Rev. A. Забелязани са 5 цитирания на резултатите представени в дисертацията. Това напълно удовлетворява изискванията на Закона за развитие на академичния състав в Република България, Правилника за неговото прилагане, както и на Правилника за условията и реда за придобиване на научни степени и заемане на академични длъжности в СУ „Св. Климент Охридски" и на Препоръчителните изисквания към кандидатите за придобиване на научни степени и заемане на академични във Физическия факултет на СУ „Св. Климент Охридски".

8. До каква степен приносите в дисертационният труд са личен принос на дисертанта?

Считам, че дисертантът има значителен принос към резултатите представени в дисертацията. В публикацията „Time-efficient implementation of quantum search with qudits, Physical Review A 85, 062321 (2012)" неговият принос вероятно не е водещ, но в публикацията „Quantum phase estimation and quantum counting with qudits, Phys. Rev. A 94, 042307" той е първи съавтор и приемам, че приносът му е равностоен. Без съмнение остава третата публикация „Alternative coins for quantum random walk search optimized for a hypercube, Journal of Quantum Information Science - 5, 6-15 (2015)", в която той е единствен автор.

9. Критични бележки

1. Обща забележка – формулите нямат номера, както е дисертацията така и в автореферата. Това оставя изложението без вътрешни връзки и прави дискусията на резултатите неудобна;

2. В увода са използвани съкращения на английски език, като DTRWA, CTRWA, SKW, DTRWS и CTRWS, без да са дадени техните пълни значения на английски език – дадени са само преводите им на български език. Това затруднява проследяването на съкращенията в литературата, както и изложението на материала в дисертацията;

3. В Глава 1.1 и 1.2 е направен обзор на най-важните едно-кюбитови и мулти-кюбитови гейтове (квантови операции). Показана е универсалната конструкция

на контролиран дву-кюбитен унитарен гейт чрез едно-кюбитови гейтове. В Глава 1.5 е показано, че всяка кюдитна операция може да се разложи чрез ротации или Хаусхолдерови отражения. Тук трябва да се отбележи, че гейтовете на Хадамар H, диагоналният $\pi/8$ гейт T и дву-кюбитовият CNOT образуват универсален дискретен набор от квантови гейтове, с които може да се апроксимира произволен много-кюбитов гейт. Макар тази информация да се съдържа в текста на дисертацията, не е заявено достатъчно ясно кои точно са дискретните набори от универсални квантови гейтове, с които ще се работи за реализация на квантовите алгоритми чрез кюдити. Например, в Глава 1.5 е споменат общият резултат, че всяка много-кюдитна операция може да се реализира чрез дву-кюдитни операции (като CNOT) и едно-кюдитни гейтове, обаче не е указано явно как (и дали) могат да се разложат последните с помощта на $d \times d$ матрици (аналогични на H и T в кюбитовия случай) за $d > 3$. Това е важно не толкова от алгоритмична гледна точка, колкото заради технологичните ограничения при физическата реализация на квантовите компютри;

4. На стр. 25 се казва „Кюдита е система с d нива, т.е., кюдита има d чисти състояния …“. Освен пропуснатия пълен член трябва да се отбележи, че в квантовата теория суперпозицията от чисти вектори на състояния е отново вектор на чисто състояние в същото Хилбертово пространство. В този случай употребата на понятието „чисти“ състояния е неподходяща, тъй като то е резервирано за квантови състояния описвани с матрица на плътността, която е идемпотентна. Би било по-добре да се замени например с „базисни“ състояния;

5. Според мен, неточно е преведено на български език понятието „Кералност“ в Глава 4. По-точно би било да се преведе като „киралност“. Макар, че английската дума „chirality” има гръцки произход, а в медицината се използва главно българският превод „хиралност“ (както например в думата „хирург“), понятието „киралност“ е въведено във физиката от Лорд Келвин със следната дефиниция: „*Наричам всяка геометрична фигура, или група от точки, кирална и казвам, че има киралност, ако нейният образ в идеално плоско огледало не съвпада със самата нея.*“

10. Лични впечатления

Личните ми впечатления са главно от предварителното обсъждане на дисертационния труд проведено през месец юни 2017 г. Докторантът демонстрира добро познаване на тематиката на дисертацията, и показва творчески подход към изследване на поставените проблеми.

11. Заключение

Въз основа на гореизложеното считам, че представеният дисертационен труд напълно отговаря на изискванията на Закона за развитие на академичния състав в Република България, Правилника за неговото прилагане, както и на Правилника за условията и реда за придобиване на научни степени и заемане на академични длъжности в СУ „Св. Климент Охридски" и на Препоръчителните изисквания към кандидатите за придобиване на научни степени и заемане на академични във Физическия факултет на СУ „Св. Климент Охридски".

Забелязаните граматически неточности и направените корекции са незначителни и второстепенни и по никакъв начин не намаляват високата научна стойност и доброто техническо представяне на съдържанието на дисертацията.

Във връзка с това, напълно убедено препоръчвам на Уважаемото Научно жури да присъди на Христо Светленов Тончев образователната и научна степен „Доктор" по професионално направление 4.1.Физически науки (Физика на атомите и молекулите).

София, 15.09.2017 г.

Рецензент:

/доц. Л. Георгиев/