

ივანე ჯავახიშვილის სახელობის თბილისის
სახელმწიფო უნივერსიტეტი

ნანა აბრამიანი

ინფორმაციის წარმოდგენა ქვანტურ კომპიუტერში
(დამუშავება და ძებნა)

სამაგისტრო ნაშრომი შესრულებულია საინფორმაციო ტექნოლოგიების
მაგისტრის აკადემიური ხარისხის მოსაპოვებლად

ხელმძღვანელი: გელა ბესიაშვილი

ტექნიკურ მეცნიერებათა კანდიდატი

ასისტენტ-პროფესორი

თბილისი

2013

სარჩევი

ანოტაცია.....	3
შესავალი.....	5
თავი 1. ქვანტური კომპიუტერები.....	7
1.1 ქვანტური კომპიუტერი.....	7
1.2 ქვანტური კომპიუტერის სტრუქტურა.....	8
1.3 ქვანტური კომპიუტერის პრაქტიკული გამოყენება.....	9
1.4 ქვანტური კომპიუტერის შექმნის პრობლემები.....	11
1.5 ქვანტური კომპიუტერის პერსპექტივები.....	13
1.6 ქვანტური ინტერნეტი.....	14
თავი 2. ქვანტური და კლასიკური კომპიუტერების შედარება.....	15
2.1 რით არის უკეთესი ქვანტური კომპიუტერი კლასიკურზე.....	15
2.2 ქვანტური ინფორმაცია.....	16
2.3 ქვანტური ტელეპორტაცია.....	17
თავი 3. ქვანტური კომპიუტერის კომპონენტები.....	18
3.1 ქვანტური ქუბიტი.....	18
3.2 ქვანტური რეგისტრი.....	22
3.3 ქვანტური გეიტები.....	25
თავი 4. ქვანტური გამოთვლები.....	28
4.1 ქვანტური გამოთვლების გამოჩენა.....	28
4.2 ქვანტური გამოთვლების იდეა.....	29
თავი 5. ქვანტური ალგორითმი.....	31
5.1 გროვერის ძებნის ქვანტური ალგორითმი.....	31
5.2 ძებნის ქვანტური ალგორითმის საშუალებებით მათემატიკური პრობლემების გადაჭრა.....	35
5.3 ლოგიკური ფუნქციის ნულის პოვნა.....	35
5.4 მაგალითები.....	37
თავი 6. ქვანტური კონცეპტი.....	43
6.1 ქვანტური კონცეპტის გამოკვლევა.....	43
6.2 კონცეპტის ფორმირება.....	44
დასკვნა.....	46
გამოყენებული ლიტერატურა:.....	47

ანოტაცია

თანამედროვე სამყაროში ყველაფერი ინფორმაციულ ტექნოლოგიებზეა დაფუძნებული. კომპიუტერი არის უნივერსალური ინსტრუმენტი, რომელიც გამოიყენება ყველა სფეროში. მის გარეშე არ აქვს აზრი მეცნიერებას, საბანკო საქმეს, სწავლას, კომუნიკაციის საშუალებებს და ა.შ.

თანამედროვე სამყარო არის ინფორმაციის უსასრულო სიმრავლე, ნულებისა და ერთიანების ნაკადი, რომლებიც გადაიცემა რადიოარხებით, სატელეფონო ქსელით. დღეს შესაძლებელია ეკონტაქტო ადამიანს, რომელიც იმყოფება ათასობით კილომეტრით ჩვენსგან შორს, ორ წამში შესაძლებელია ურთულესი გამოთვლების ჩატარება და ა.შ. ამ ყველაფერს და სხვა შესაძლებლობების უსასრულო სიმრავლეს განსაზღვრავს კომპიუტერი და ინფორმაციული ქსელები.

ისტორიული ანალიზი გვაჩვენებს, რომ ინფორმაციული ტექნოლოგიები იზრდება ექსპონენციალურად დიდი სიჩქარით და დღეს უკვე მსჯელობა მიდის ქვანტური კომპიუტერის შექმნაზე. ამჟამად ბევრი სამეცნიერო ნაშრომია გამოქვეყნებული ქვანტურ კომპიუტერებზე, მასში ინფორმაციის დამუშავებაზე, ქვანტური ალგორითმების წარმოდგენაზე და ა.შ. ეს ყველაფერი განაპირობა იმ ფაქტმა, რომ რთული ამოცანების ამოხსნას კლასიკური კომპიუტერი ვეღარ უმკლავდება. მომხმარებელს გააჩნია ბევრი მოთხოვნა და ამიტომ მეცნიერებმა დაიწყეს ფიქრი ბევრად უფრო მძლავრი მანქანის შექმნაზე.

დღესდღეობით ეს თემა ძალიან აქტუალურია, ძალიან ბევრი კითხვა ჩნდება მის ირგვლივ და ჩვენს მიერ ზემოაღნიშნული ფაქტორები მეტყველებენ თემის აქტუალობაზე და ნაშრომი ეძღვნება ამ აქტუალურ საკითხებს.

ნაშრომის მიზანია ნათლად და თვალსაჩინოდ აღწეროს ქვანტური კომპიუტერები, მასში ინფორმაციის წარმოდგენა და ქვანტური მეთოდებისა და მოდელირების საშუალებით წარმოადგინოს რთული ამოცანები კლასიკურ კომპიუტერზე.

ნაშრომი განიხილავს ორ ძირითად მიმართულებას. პირველი არის გროვერის ალგორითმი, რომელიც ახორციელებს ძებნას მონაცემთა ბაზაში, ხოლო მეორე მიმართულება ეხება ქვანტური მეთოდოლოგიის გამოყენებას ცოდნის ბაზებში. როგორც ცნობილია, ცოდნის ბაზებში ინფორმაციის ძებნის ერთ-ერთი საშუალებაა კონცეპტუალური ძებნის ამოცანა (ძებნა ქვანტური კონცეპტების საშუალებით).

Information in quantum computers (working up and searching)

In the modern world everything is based on informational technologies. The computer is a universal instrument, that is used in every field. Without it there's nothing in science, banking, studying communication and so on.

Modern world is endless multiplicity of information, zero and uniform flow, that is transmitted on radiochannels, telephone network. Today you can contact the person, who is thousands of kilometres away. It's possible to the most difficult calculations and so on. All of these and another possibility is an infinite set of computers and information networks.

Historical analysis shows, that informational technologies grow in exponentially great speed, and today developing quantum computers is being discussed. Now many scientific work is published about quantum computers, information processing, quantum algorithms performance in it and so on.

This is all due to the fact, that a classical computer can no longer cope solve complex problems. Many customers have requested that's why scientists began thinking to create a much more powerful car.

This task is very actual today, there are many question about it, and these abovementioned factors speak about items actuality and work is devoted to the discussion of these issues .

The aim of the work is clearly and visibly describe quantum computers, it is to provide information an quantum methods and modeling of complex task through a classical computer.

There work discusses two main directions. He first is the Grover search algorithm, which performs the database while the second one deals with the application of quantum methodology for knowledge bases. As it's known in search of information in knowledge bases one way conceptual search task.

შესავალი

1990-ან წლებში გამოჩნდა მეცნიერების ახალი სფერო - ქვანტური თეორია და ქვანტური გამოთვლები. ქვანტური ლოგიკის მუშაობის შესაძლებლობა პირველმა შეიმუშავა მათემატიკოსმა ი. ფონ ნეიმანმა. მაგრამ იმ დროს ჯერ არ იყო შექმნილი ჩვეულებრივი კლასიკური კომპიუტერებიც კი. კლასიკური კომპიუტერის გამოჩენის შემდეგ კი მეცნიერები ცდილობდნენ ახალი ელემენტების შემუშავებას მათთვის. კომპიუტერების გავრცელების შემდეგ მეცნიერები, რომლებიც დაკავებულნი იყვნენ ქვანტური ობიექტების შესწავლით, მივიდნენ იმ დასკვნამდე, რომ პრაქტიკულად შეუძლებელია პირდაპირ გათვალისწინებული ევოლუციური სისტემის მდგომარეობა, რომელიც შედგება რამდენიმე ათეული ნაწილაკისაგან. ეს აიხსნება იმით, რომ რთული სისტემის მთლიანი აღწერისათვის საჭიროა კომპიუტერის მეხსიერებაში შევინახოთ ცვლადების, ე.წ. ქვანტური ამპლიტუდების, ექსპონენციალურად დიდი რაოდენობა. შეიქმნა პარადოქსალური სიტუაცია: ვიცით ევოლუციის განტოლება, ნაწილაკების ურთიერთქმედების ზუსტი პოტენციალები, სისტემის საწყისი მდგომარეობა, მაგრამ პრაქტიკულად შეუძლებელია მომავლის გამოთვლა. ამ სიტუაციას მიაქცია ყურადღება იუ.ი. მანინმა 1980 წელს, რომ აუცილებელია ქვანტური გამოთვლითი მოწყობილობების თეორიის შემუშავება. 1980-იან წლებში ეს პრობლემა შეისწავლა ამერიკელმა ფიზიკოსმა პ.ბენევემა, რომელმაც აჩვენა, რომ ქვანტურ სისტემას შეუძლია განახორციელოს გამოთვლები. ასევე, ინგლისელმა მეცნიერმა დ.დოიჩმა თეორიულად შეიმუშავა უნივერსალური ქვანტური კომპიუტერი. მაგრამ დიდხანს იყო გაურკვეველი ის, რომ შეიძლებოდა თუ არა ქვანტური კომპიუტერის გამოთვლითი სიმძლავრე გამოყენებული ყოფილიყო პრაქტიკული ამოცანების ამოხსნის გაუმჯობესებისათვის. 1994 წელს ამერიკელმა მათემატიკოსმა პ.შორმა შემოგვთავაზა ქვანტური ალგორითმი.

პირველი კლასიკური კომპიუტერი არ გამოირჩეოდა ბევრი ღირებულებებით, მაგრამ დღითიდღე იხვეწებოდა და დღესდღეობით კომპიუტერი პრაქტიკულად ყველა სახლშია, მაგრამ ადამიანის მოთხოვნები გამოთვლით ტექნიკასთან უფრო და უფრო რთულდება, ითხოვს რთული ამოცანების ამოხსნას, რომლებსაც კლასიკური კომპიუტერი ვერ უმკლავდება ან მოითხოვს შესრულების ძალიან დიდ დროს და ახლა ადამიანი ელოდება ბევრად უფრო სხვას და სწრაფს. კლასიკურმა კომპიუტერმა ამოწურა თავის შესაძლებლობები და ყველა სიახლის მოლოდინშია, ხოლო ტერმინმა „ქვანტური“ კომპიუტერი დააინტერესა საზოგადოება და სწორედ ამიტომ არის თემა აქტუალური.

დღესდღეობით ქვანტურ კომპიუტერზე მუშაობა ხდება რამოდენიმე მსხვილ კორპორაციებში, როგორიცაა მაგალითად, IBM, AT&T, Microsoft, Intel. შეიძლება სრულფასოვანი გამოთვლით მანქანის შექმნასთან ჯერ კიდე შორს ვართ, მაგრამ ქვანტური მექანიკის პრინციპები წარმატებით გამოიყენება და მუშაობს თანამედროვე ელექტრონიკაში. ანუ რეგულარულად მიმდინარეობს სემინარები, ხშირად ხდება სამეცნიერო პუბლიკაციების გამოცემა, იქმნება გამოთვლითი მოწყობილობების ნიმუშები.

როგორც უკვე აღვნიშნე ნაშრომი განიხილავს ორ მიმართულებას, მაგრამ სანამ გადავალთ ინფორმაციის დამუშავებაზე და ძებნაზე მანამდე უნდა განვიხილოთ ქვანტური კომპიუტერის სტრუქტურა, მისი კომპონენტები, ვნახოთ როგორ ხდება მასში გამოთვლები. ამიტომ რამოდენიმე თავს დავუთმობ ამ საკითხების გარკვევას.

თავი 1. ქვანტური კომპიუტერები

1.1 ქვანტური კომპიუტერი

ქვანტური კომპიუტერი არის გამოთვლითი მოწყობილობა, რომელიც მუშაობის დროს ქვანტური ალგორითმების სასუალებით იყენებს ქვანტო-მექანიკურ ეფექტებს, ისეთებს, როგორიცაა ქვანტური პარალელიზმი და ქვანტური არეულობა.

ქვანტური პარალელიზმი მდგომარეობს იმაში, რომ მონაცემები გამოთვლის პროცესში წარმოადგენენ ქვანტურ ინფორმაციას, რომელიც პროცესის დამთავრების შემდეგ გარდაიქმნება კლასიკურში ქვანტური რეგისტრის საბოლოო მდგომარეობის გაზომვის შედეგად. ერთი ქვანტური ოპერაციის გამოყენებისას ქვანტური მდგომარეობის სუპერპოზიციის კოეფიციენტის მრავალი რიცხვი, რომლებიც ვირტუალურ ფორმაში შეიცავენ კლასიკურ ინფორმაციას, გარდაიქმნება ერთდროულად. ქვანტური სუპერპოზიცია კი შეიძლება წარმოვიდგინოთ როგორც ორი დისკრეტული სიდიდის გაერთიანებული მდგომარეობა, რომელიც გაზომვისას გვამღევს ერთ-ერთს.

ქვანტური კომპიუტერი გამოთვლებისთვის იყენებს არა კლასიკურ ალგორითმებს, არამედ ქვანტური ბუნების ბევრად უფრო რთულ პროცესებს, რომლებსაც უწოდებენ ქვანტურ ალგორითმებს. ეს ალგორითმები იყენებენ ქვანტო-მექანიკურ ეფექტებს: ქვანტურ არეულობას და ქვანტურ პარალელიზმს.

ქვანტურ კომპიუტერს შეუძლია დაშიფროს შეტყობინებები, რომლებიც დაშიფრულია RSA ასიმეტრიული კრიფტოგრაფიული ალგორითმის საშუალებით. დღემდე ეს ალგორითმი ითვლება შედარებით უფრო სანდოდ, რადგან კლასიკური კომპიუტერის რიცხვების დაყოფის ეფექტური საშუალება მარტივ მამრავლებად დღესდღეობით არ არის ცნობილი. მაგალითად, რომ მივიღოთ წვდომა საკრედიტო ბარათთან საჭიროა ორ მამრავლიანი რიცხვი ასობით ციფრიანი სიგრძით. ყველაზე ჩქარი თანამედროვე კომპიუტერისთვის ამ ამოცანის შესრულება მოითხოვდა დიდ დროს. შორის ალგორითმის საშუალებით ეს ამოცანა ხდება შესრულებადი, თუ გვექნება გამართული ქვანტური კომპიუტერი.

რომ გავიგოთ რისთვისაა საჭირო ქვანტური კომპიუტერი, უნდა წარმოვიდგინოთ მისი მოქმედების პრინციპი. კლასიკური კომპიუტერი მუშაობს ნულებისა და ერთიანების თანმიმდევრული ოპერაციების ჩატარების ხარჯზე, ხოლო ქვანტური კომპიუტერი იყენებს

ზეგამტარუნარიანი ლენტის რგოლებს. დენი რგოლებში მიედინება სხვადასხვა მიმართულებებით, ამიტომ ასეთი რგოლების ჯაჭვს შეუძლია ერთდროულად რეალიზაცია გაუკეთოს ნულებისა და ერთიანების ბევრად უფრო ბევრ ოპერაციას. ზუსტად ეს დიდი სიმძლავრე არის ქვანტური კომპიუტერის ძირითადი ღირებულება.

შეგვიძლია გამოვყოთ ქვანტური კომპიუტერების ორი ტიპი. ორივე ტიპი დაფუძნებულია ქვანტურ მოვლენებზე, ოღონდ სხვადასხვა რიგის:

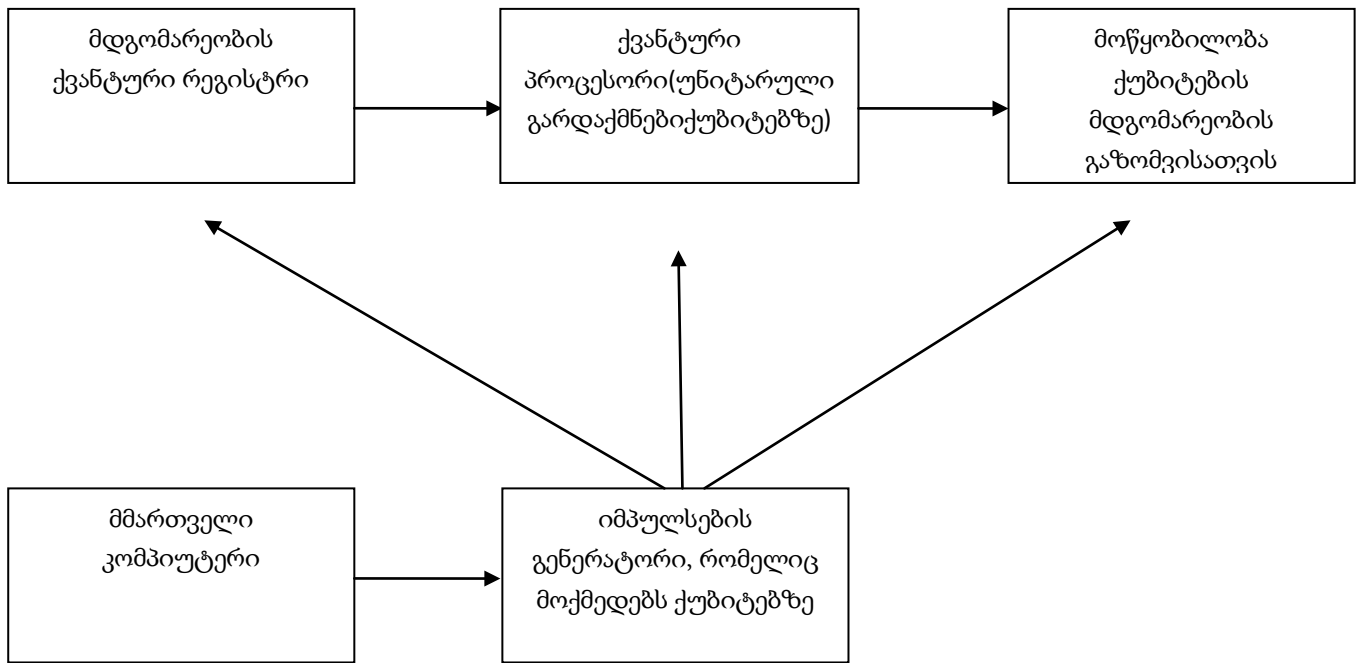
- ❖ კომპიუტერები, რომლის საფუძველს წარმოადგენენ მაგნიტური ნაკადის ქვანტირება.
- ❖ მეორე ტიპია ე.წ. ქვანტური კოგერენტული კომპიუტერები. საჭიროებს გამოსაყენებელი ქუბიტების ტალღური ფუნქციის კოგერენტულობის მხარდაჭერას გამოთვლის დროს თავიდან ბოლომდე. შედეგად, რამოდენიმე ამოცანისთვის ასეთი კომპიუტერების გამოთვლითი სიმძლავრე პროპორციულია 2^N -ის, სადაც N არის კომპიუტერში ქუბიტების რიცხვი. სწორედ ეს ტიპი გვაქვს მხედველობაში, როდესაც ვსაუბრობთ ქვანტურ კომპიუტერებზე.

1.2 ქვანტური კომპიუტერის სტრუქტურა

განვიხილოთ ქვანტური კომპიუტერის გამოთვლების რეალიზაციის მარტივი მაგალითი. დავუშვათ, რომ გვაქვს L ქუბიტების სისტემა და თითოეული მათგანი იდეალურად იზოლირებულია გარე სამყაროსგან. დროის ნებისმიერ მომენტში შეგვიძლია ავირჩიოთ ნებისმიერი ორი ქუბიტი და ვიმოქმედოთ მასზე უნიტარული მატრიცით 4×4 -ზე ზომით. ასეთი მოქმედებების თანმიმდევრობა არის ქვანტური კომპიუტერის პროგრამა.

გამოთვლებისათვის რომ გამოვიყენოთ ქვანტური სქემა, უნდა შეგვეძლოს შესასვლელი მონაცემების შეტანა, ჩავატაროთ გამოთვლები და დავითვალოთ შედეგი. ამიტომ ნებისმიერი ქვანტური კომპიუტერის პრინციპიალური სქემა უნდა შეიცავდეს შემდეგ ფუნქციონალურ ბლოკებს: ქვანტურ რეგისტრს მონაცემების შესატანად, ქვანტურ პროცესორს მონაცემთა გარდაქმნისათვის და მონაცემთა გადათვლის მოწყობილობას.

ქვანტური კომპიუტერის სქემატური სტრუქტურა შემდეგნაირია:



ქვანტურ კომპიუტერში გარდაქმნების რეალიზაციის შემდეგ სუპერპოზიციის ახალი ფუნქცია წარმოადგენს გამოთვლების შედეგს ქვანტურ პროცესორში. რჩება მხოლოდ მიღებული მნიშვნელობების დათვლა, რისთვისაც ხდება ქვანტური სისტემის მნიშვნელობის გაზომვა. შედეგად წარმოიქმნება ნულებისა და ერთიანების თანმიმდევრობა და ქვანტურ კომპიუტერს შეუძლია რაღაც ალბათობებით მოგვცეს ნებისმიერი პასუხი. ამასთან, გამოთვლების ქვანტური სქემა ითვლება სწორად, თუ სწორი პასუხი მიიღება ალბათობით, რომელიც საკმარისად ახლოსაა ერთიანთან. გამოთვლების რამოდენიმეჯერ გამეორებისას და იმ პასუხის არჩევა, რომელიც გვხვდება ხშირად, შეგვიძლია შევამციროთ შეცდომის ალბათობა მცირე სიდიდემდე.

1.3 ქვანტური კომპიუტერის პრაქტიკული გამოყენება

ქვანტური კომპიუტერის პროტოტიპები არსებობენ დღეს. მართალია ჯერ ექსპერიმენტალურად აწყობენ მხოლოდ მცირე რეგისტრებს, რომლებიც შედგებიან რამოდენიმე ქვანტური ბიტისგან. ჯგუფმა, რომელსაც ხელმძღვანელობდა ამერიკელი ფიზიკოსი ი.ჩანგი, გამოაცხადა 5-ბიტის ქვანტური კომპიუტერის აწყობა. ეს არის დიდი მიღწევა. თუმცა, სამწუხაროდ, არსებული ქვანტურ სისტემებს ჯერ არ შეუძლიათ საიმედო გამოთვლების

ჩატარება. მაგრამ ეფექტური ქვანტური კომპიუტერის შექმნას არ კრძალავს ფიზიკა. საჭიროა მხოლოდ ტექნოლოგიური სირთულეების გარდაქმნა.

არსებობს ქვანტური კომპიუტერების ბევრი შესაძლო მოდელი. პირველი ქვანტური კომპიუტერი, რომელიც შექმნილი იყო პრაქტიკაზე, არის იმპულსური ბირთვული მაგნიტურ-რეზონანსული სპექტომეტრი მაღალი გაფართოებით, მაგრამ როგორც ქვანტური კომპიუტერი არ განიხილება. როდესაც გამოჩნდა ქვანტური კომპიუტერის კონცეფცია, მაშინ მეცნიერები მიხვდნენ, რომ ბირთვული მაგნიტურ-რეზონანსული სპექტომეტრი წარმოადგენს ქვანტური კომპიუტერის ვარიანტს.

ბირთვულ მაგნიტურ-რეზონანსულ სპექტომეტრში განსახილველი მოლეკულის ბირთვის სპინები წარმოქმნიან ქუბიტებს. თითოეულ ბირთვს აქვს რეზონანსის თავისი სიხშირე მოცემულ მაგნიტურ ველში. ბირთვული მაგნიტურ-რეზონანსული სპექტომეტრის მთავარ უპირატესობას წარმოადგენს ის, რომ მასში შეიძლება გამოვიყენოთ ერთნაირი მოლეკულების დიდი რაოდენობა. ამასთან, თითოეული მოლეკულა წარმოადგენს ქვანტურ სისტემას.

ამ მომენტში ყველაზე დიდი ქვანტური კომპიუტერი შედგება 7 ქუბიტისგან. ეს საკმარისია იმისათვის, რომ რეალიზებული იქნას შორის ალგორითმი და დავყოთ რიცხვი 15 მარტივ მამრავლებად 3-ზე და 5-ზე.

არსებობს რამოდენიმე იდეა და მოსაზრება იმაზე, თუ როგორ საიმედო და ადვილად სამართავი ქვანტური ბიტი. რუსი მეცნიერი მ.ვ.ფეიგელმანი გვთავაზობს შემდეგს: ავაწყოთ ქვანტური რეგისტრები მინიატურული ზეგამტარი რგოლებისგან. ყოველი რგოლი შეასრულებს ქუბიტის როლს, ხოლო 0 და 1 მდგომარეობებს შეესაბამება რგოლში დენის მიმართულება - საათის ისრის მიმართულებით და პირიქით. ასეთი ქუბიტების გადართვა შეიძლება მაგნიტური ველით.

ქვანტური კომპიუტერების პრაქტიკული რეალიზაციისთვის ფიზიკოსები იყენებენ სხვადასხვა სახის ეგზოტიკურ ობიექტებს და მოვლენებს. ქვანტური კომპიუტერების შექმნაზე აქტიურად მუშაობს კომპანია D-Wave Systems, რომელმაც 2007 წლის თებერვალში შექმნა 16 ქუბიტისანი ქვანტური კომპიუტერი. ახლა ეს კომპანია აგრძელებს ქვანტური კომპიუტერის განვითარებას.

- 2007 წლის ნოემბერში კომპანიამ კონფერენციაზე წარმოადგინა 28 -ქუბიტისანი კომპიუტერის მუშაობა.

- 2008 წლის დეკემბერში კომპანიამ ორგანიზება გაუკეთა გამოთვლების დახარისხების პროექტს.
- 2011 წლის მაისში წარმოდგენილია D-Wave One კომპიუტერი, რომელიც შექმნილია 128-ქუბიტის პროცესორის ბაზაზე.

ქვანტური კომპიუტერის აგება რეალური ფიზიკური მოწყობილობის სახით წარმოადგენს XXI საუკუნის ფიზიკის ფუნდამენტალურ ამოცანას. დღეს აგებულია ქვანტური კომპიუტერების მხოლოდ შემოსაზღვრული ვარიანტები (10 ქუბიტის საზღვრებში).

1.4 ქვანტური კომპიუტერის შექმნის პრობლემები

დღესდღეობით ქვანტური კომპიუტერი არის მოწყობილობა, რომელიც არსებობს მხოლოდ თეორიაში, აზროვნებით ექსპერიმენტში. ყველა ნაშრომი, რაც დღეს გამოქვეყნებულია, არის მხოლოდ თეორიული. ქვანტური კომპიუტერი არის n ქუბიტის სიმრავლე, რომლისთვისაც პრაქტიკულად განსაზღვრულია შემდეგი ოპერაციები:

- ❖ ყოველი ქუბიტი შეიძლება მოვამზადოთ რაღაც ცნობილ მდგომარეობაში $|0\rangle$;
- ❖ ყოველი ქუბიტი შეიძლება გაზომილ იქნას ბაზისში $\{|0\rangle, |1\rangle\}$;
- ❖ უნივერსალური ქვანტური გეითი შეიძლება გამოყენებულ იქნას ნებისმიერი ქვესიმრავლესთვის, რომელიც შედგება ფიქსირებული ქუბიტების რიცხვისგან;
- ❖ ქუბიტების მდგომარეობა არ იცვლება ზემოაღნიშნული გარდაქმნების შედეგად;

ანუ შეიძლება ვთქვათ, რომ ქვანტური კომპიუტერი არის სისტემა, რომელშიც ხდება ფაზური გარდაქმნა მაკროსამყაროდან მიკროსამყაროში.

ძირითადი პრობლემები, რომლებიც დაკავშირებულია ქვანტური კომპიუტერების შექმნასთან და გამოყენებასთან:

- ❖ საჭიროა გამოთვლების მაღალი სიზუსტის უზრუნველყოფა;
- ❖ გარე ზემოქმედებამ შეიძლება გაანადგუროს ქვანტური სისტემა ან შეიტანოს მასში დამახინჯებები;

ქვანტური კომპიუტერების ნებისმიერი ფიზიკური რეალიზაცია იქნება მიახლოებითი. ჩვენ არ შეგვიძლია შევქმნათ მოწყობილობა, რომელიც მოგვცემს ფაზისური სივრცის ნებისმიერ ვექტორს. ნებისმიერი მოწყობილობის მუშაობა გაუქნდება შემთხვევითი შეცდომებით. ამიტომ ჩნდება კითხვა შეიძლება თუ არა საიმედო ქვანტურ ელემენტებზე გამოთვლების ჩატარება. ასეთი ამოცანა იხსნება მარტივად, მაგალითად, დამატებითი ბიტების დახმარებით.

ფიზიკურ სისტემა ქვანტური კომპიუტერის შექმნისათვის ითხოვს შემდეგი 5 მოთხოვნის შესრულებას:

- ❖ სისტემა უნდა შედგებოდეს ნაწილაკების ზუსტი რიცხვისგან;
- ❖ უნდა იყოს სისტემის ცნობილ საწყის მდგომარეობაში მოყვანის შესაძლებლობა;
- ❖ იზოლაციის დონე გარე გარემოსგან უნდა აიყოს ძალიან მაღალი;
- ❖ უნდა შეგვეძლოს სისტემის მდგომარეობის შეცვლა ფაზისური სივრცის უნიტარული გარდაქმნების მიმდევრობის მოცემით;
- ❖ უნდა გვქონდეს სისტემის მდგომარეობის „ძლიერი გამოთვლების“ შესრულების შესაძლებლობა;

ამ ხუთი ამოცანისგან ყველაზე რთული ითვლება მესამე და მეოთხე. მათ ზუსტ ამოხსნაზეა დამოკიდებული ოპერაციების შესრულების სიზუსტე. მეხუთეც არ არის ადვილი, რადგან ცალკეული ნაწილაკის მდგომარეობის გაზომვა არ არის ადვილი.

ქვანტური კომპიუტერის რეალიზაციისას უნდა შესრულდეს შემდეგი მოთხოვნები:

- ❖ ფიზიკური სისტემა, რომელიც წარმოადგენს ფართომასშტაბურ ქვანტურ კომპიუტერს, უნდა შეიცავდეს კარგად გარჩევადი ქუბიტების საკმარისად დიდ რიცხვს $L < 10^3$ შესაბამისი ქვანტური ოპერაციების შესრულებისათვის;
- ❖ საჭიროა უზრუნველყოთ ქვანტური მდგომარეობების სუპერპოზიციის ეფექტების განადგურების მაქსიმალური ზეგავლენა. ქვანტური მდგომარეობების სუპერპოზიციის განადგურების დრო 104-ჯერ უნდა აღემატებოდეს ძირითადი ქვანტური ოპერაციების შესრულების დროს;
- ❖ საჭიროა უზრუნველყოთ გაზომვა გასასვლელზე ქვანტური სისტემის მდგომარეობის საკმარისად მაღალი საიმედოობით. ქვანტური მდგომარეობის საბოლოო გაზომვა წარმოადგენს ქვანტური გამოთვლების ერთ-ერთ მთავარ პრობლემას;

1.5 ქვანტური კომპიუტერის პერსპექტივები

ქვანტური კომპიუტერების პერსპექტიულობა მდგომარეობს იმაში, რომ ქვანტურ კომპიუტერებს შეუძლიათ ამოხსნან მთელი რიგი ამოცანებისა, რომლებიც დღესდღეობით არის რთული და ძნელად დასამუშავებელი. მათ კი მათი ამოხსნა შეუძლიათ ადვილად. კერძოდ კი, უფრო პერსპექტიული სფერო არის ქვანტური კრიპტოგრაფიის შექმნა.

ქვანტური კრიპტოგრაფია იძახის შემდეგს: გადაცემული შეტყობინების გატაცება მაშინვე ხდება ცნობილი. ეს ნიშნავს, რომ შპიონაჟის ფაქტის შეუმჩნეველობა არ შეიძლება. გატაცებული შეტყობინება, რომელიც დაშიფრულია ქვანტური კომპიუტერის მიერ, კარგავს თავის სტრუქტურას და ხდება გაუგებარი მიმღებისათვის.

ქვანტურ კომპიუტერს აქვს გამოყენების კიდევ ერთი სფერო, რომლის უდიდესი მნიშვნელობაც დღეს უკვე ცნობილია. ქვანტური კომპიუტერის გიგანტური გამომთვლელი ძალა საშუალებას გვაძლევს დავაკისროთ მანქანას ყველაზე მრავალფეროვანი ინტელექტუალური შემოქმედება. მანქანას შეუძლია არამარტო შეაგროვოს, შეინახოს და დაამუშაოს ინფორმაცია, არამედ შეასრულოს ოპერაციები მასზე, რომელიც არ არის ხელმისაწვდომი ყველაზე მძლავრი თანამედროვე კომპიუტერებისათვის. ეს ნიშნავს, რომ ქვანტური კომპიუტერები მოგვცემენ საშუალებას შევქმნათ ახალი თაობის ექსპერტული სისტემები. ექსპერტული სისტემა არის კომპიუტერის სისტემა, რომელიც იყენებს ერთი ან რამოდენიმე ექსპერტის ცოდნას ფორმალიზებული სახით, ასევე ამონახსნის მიღების ლოგიკას. ეს სისტემა განკუთვნილია ამონახსნის მიღებისათვის რთულ პირობებში, როდესაც არ გვყოფნის დრო, გამოცდილება, ცოდნა, ინფორმაცია. შეტანილ მოთხოვნაზე მანქანა გვაძლევს კვალიფიცირებულ კონსულტაციას ან მინიშნებას.

ექსპერტული სისტემების პირველი მოდელები შექმნეს 1970 წლების შუაში: სისტემა MYCIN გამოიყენებოდა მედიცინაში დაავადებების დიაგნოსტიკისათვის, DENDRAL - ნიადაგის ქიმიური შემადგენლობის ანალიზისათვის. ექსპერტული სისტემის მეხსიერებაში შეიძლება ინახებოდეს შესაძლო ტექნიკური ინფორმაციების დიდი რაოდენობა: მატერიის პარამეტრები, მანქანის პარამეტრები, სტანდარტების პარამეტრები და ა.შ. ასე ინახება ამონახსნის მიღების ალგორითმები, შედგენილი ყველაზე საუკეთესო სპეციალისტების მიერ. ექსპერტულ სისტემაში შეგვაქვს მოთხოვნა მანქანის კონსტრუირებაზე განსაზღვრული ფუნქციებით. ექსპერტული სისტემა ასრულებს მანქანის შემუშავებასა და კონსტრუირებას და გვაძლევს მზა ნახაზებს,

რომლის მიხედვითაც შეგვიძლია მანქანის აწყობა. მსგავსი ექსპერტული სისტემის შედგენა ქვანტური კომპიუტერების საფუძველზე გამოიწვევს დიდ გადატრიალებას ტექნიკაში.

ახლა კი შევეცადოთ წარმოვიდგინოთ როგორი იქნება მომავალში ქვანტური კომპიუტერი. ეს იქნება დიდი კომპიუტერი, რომელიც შეიცავს ათასობით მმართველ ელემენტს, რომლებიც მოქმედებენ ლოკალურად ყოველ ქუბიტზე. ჩნდება კითხვა: თუ როგორ განხორციელდება ეს ზემოქმედება? უფრო ეს მოხდება ელექტრონული იმპულსების საშუალებით. შესაძლებელია ასევე სინათლის ნაკადის ოპტიკური მართვით, რომელიც ფოკუსირებულია ქუბიტებზე. მაგრამ ამ შემთხვევაში ძნელი იქნება მოვერიდოთ მეზობელი ქუბიტების ზემოქმედებას. რაც შეეხება ელექტრონულ მეთოდებს, ისინი ფართოდ გამოიყენება მიკროელექტრონიკაში კლასიკური ლოგიკური ელემენტების მართვისთვის. ამიტომ მათი გამოყენება არის უფრო პერსპექტიული ქვანტური კომპიუტერების შექმნისთვის.

ამის შედეგად შესაძლებელია, რომ ქვანტური კომპიუტერი შეიქმნება მიკროელექტრონული ტექნოლოგიის ტრადიციული მეთოდების გამოყენებით და შეიცავს მმართველი ელექტროდების სიმრავლეს, რომელიც გვახსენებს თანამედროვე მიკროპროცესორს.

ქვანტური კომპიუტერები არ ამოხსნიან პრინციპიალურად ამოუხსნელ კლასიკურ ამოცანებს, ისინი უბრალოდ გააუმჯობესებენ გამოთვლებს. ამასთან, შესაძლებელი იქნება ქვანტური კავშირი - დიდ მანძილზე ქუბიტების გადაცემა, რაც მიგვიყვანს ქვანტური ინტერნეტის შექმნასთან.

1.6 ქვანტური ინტერნეტი

მომავალში შესაძლებელია, რომ შეიქმნას თავისებური ქსელი, ანუ თანამედროვე ინტერნეტის ანალოგი, რომელშიც გამოიყენება ისეთი მოვლენა, როგორიცაა ქვანტური ტელეპორტაცია. მისი აზრი მდგომარეობს იმაში, რომ თუ გვაქვს ორი „შერეული“ ნაწილაკი, რომლებიც გაფანტულები არიან სივრცეში, მაშინ ერთი მათგანის გაზომვით მივიღებთ მეორე ნაწილაკის წამიერ გაზომვას. მისი რეალიზაცია ხდება დაახლოებით ასე:

გვაქვს ორი „შერეული“ ქუბიტი და ვთქვათ, ერთი იმყოფება თბილისში - A, ხოლო მეორე ნიუ იორკში - B. გაგზავნი, რომელიც იმყოფება ჩვენი ქვეყნის დედაქალაქში, „ახვევს“ A ქუბიტს ინფორმაციის კიდევ ერთ ქუბიტთან. შემდეგ გაგზავნი ახდენს გაზომვებს ამ სისტემაზე. ამ დროს ნიუ-იორკში მდებარე ქუბიტი გადადის ახალ მდგომარეობაში. ფიზიკოსები ამას

უწოდებენ „კოლაფსირებას“. სიტყვა „კოლაფსი“ ნიშნავს ჩქარ შეკუმშვას. მოცემულ შემთხვევაში B ქუბიტი მდგომარეობების პოტენციალური სიმრავლიდან გადადის რომელიმე ერთში. ამ დროს ხდება ინფორმაციის ქვანტური ნაწილის გადატანა. მაგრამ გაგზავნილი ინფორმაციის აღდგენა შეუძლებელია, რადგან მიმღებისთვის B ქუბიტი ჯერ კიდევ იმყოფება მდგომარეობების სიმრავლეში. ამ დროს გამგზავნი აგზავნის კლასიკური არხით თავისი გაზომვების შედეგს (მხოლოდ 2 ბიტ ინფორმაციას).

თავი 2. ქვანტური და კლასიკური კომპიუტერების შედარება

2.1 რით არის უკეთესი ქვანტური კომპიუტერი კლასიკურზე

გამოთვლითი მანქანების ძირითადი ნაწილი მუშაობს შემდეგი სქემის მიხედვით: მეხსიერების n ბიტი ინახავს მდგომარეობას და დროის ყოველი ტაქტი იცვლება პროცესორით. ქვანტურ შემთხვევაში n ქუბიტების სისტემა იმყოფება მდგომარეობაში, რომელიც წარმოადგენს ყველა ბაზისური მდგომარეობის სუპერპოზიციას, ამიტომ სისტემის ცვლილება ეხება ყველა 2^n ბაზისურ მდგომარეობებს ერთდროულად. თეორიულად ახალი სქემა იმუშავებს ბევრად უფრო სწრაფად კლასიკურზე.

იმისათვის, რომ გავიგოთ რით განსხვავდება მუშაობისას კლასიკური და ქვანტური კომპიუტერები გავიხსენოთ ის, რომ კლასიკური კომპიუტერი მეხსიერებასი ინახავს L ბიტს, რომელიც პროცესორის ყოველი ტაქტის დროს იცვლება. ქვანტურ კომპიუტერში მეხსიერებაში ინახება L ქუბიტის მნიშვნელობები, ქვანტური სისტემა კი იმყოფება მდგომარეობაში, რომელიც წარმოადგენს ყველა ბაზისური 2^L მდგომარეობების სუპერპოზიციას. შესაბამისად, ქვანტურ კომპიუტერში გამოთვლითი სიმძლავრე მიიღწევა პარალელური გამოთვლების რეალიზაციის ხარჯზე.

მოვიყვანოთ მარტივი მაგალითი. როგორც ცნობილია, კლასიკურ კომპიუტერში ინფორმაცია შედგება ბიტისგან, რომელიც ჩაწერილია 0 ან 1 სახით. მონაცემები არის ნულისა და ერთიანების გარკვეული თანმიმდევრობა, რომელსაც ეწოდება კლასიკური რეგისტრი. ქვანტურ კომპიუტერში კი ინფორმაცია ჩაიწერება ქუბიტების ან ქვანტური ბიტების საშუალებით.

კლასიკურ ბიტს შეუძლია მიიღოს ორი მდგომარეობა - 0 ან 1. მესამე არ არის მოცემული. ქუბიტი კი შეიძლება იყოს ნახევარზე 0 და ნახევარზე 1. ეს არის სუპერპოზიცია, ანუ როდესაც ქუბიტის მდგომარეობა გამოისახება ყველა შესაძლო მნიშვნელობების კომბინაციით. ანუ 8 კლასიკური ბიტი დროის კონკრეტულ მომენტში შეიძლება იმყოფებოდეს მხოლოდ ერთ მდგომარეობაში, მაგალითად, 10010110. მაგრამ 8 ბაზისური ქუბიტისთვის მდგომარეობა იქნება 256 შესაძლო ვარიაცია, 00000000-დან 11111111-მდე. და ამასთან, ერთდროულად. თუ შევადარებთ რიცხვის მარტივ მამრავლებად დაშლის სიჩქარეებს, რომელიც შედგება 155 ნიშნისგან, მაშინ ვნახავთ, რომ კლასიკურ კომპიუტერს ამის შესრულებისათვის დაჭირდება 35 წელი, ხოლო ქვანტური კომპიუტერი ამაზე დახარჯავს მხოლოდ რამოდენიმე წამს.

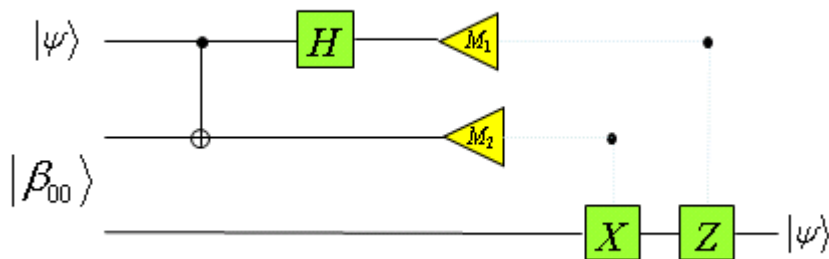
2.2 ქვანტური ინფორმაცია

კლასიკურ კომპიუტერში შენახული ინფორმაციის რაოდენობა იზრდება წრფივად, ხოლო ქვანტურში - ექსპონენციალურად. მათემატიკურად რომ გამოვსახოთ, გვექნება შემდეგი სიტუაცია. I იყოს ინფორმაციის რაოდენობა, N - ბიტების რაოდენობა, Q - ქუბიტების რაოდენობა. მაშინ კლასიკური კომპიუტერისთვის გვექნება $I = N$, ხოლო ქვანტურისათვის - $I = 2^Q$. მათემატიკური ფორმულის საშუალებით ქვანტური და კლასიკური კომპიუტერების შედარება იქნება $N = 2^Q$. აქედან გამომდინარეობს, რომ მაგალითად, თუ გვაქვს ქვანტური კომპიუტერი 512 ქუბიტით, მაშინ მისი კლასიკური ანალოგი, რომელიც უდრის შენახული ინფორმაციის რაოდენობას უნდა ჰქონდეს $2^{512} = 10^{355}$ ბიტი. მარტივი მაგალითი: კლასიკურ კომპიუტერში ორი ბიტი - ორჯერ მეტი ინფორმაცია ვიდრე ერთ ბიტში. ქვანტურ გამოთვლით მანქანაში კი 2 ქუბიტი - ოთხჯერ მეტი ინფორმაცია ვიდრე ერთში.

2.3 ქვანტური ტელეპორტაცია

ქვანტური კომპიუტერების სფეროში გვაქვს ცნება ქვანტური ტელეპორტაცია. ტელეპორტაციის ალგორითმი აკეთებს ერთი ქუბიტის მდგომარეობის მეორეზე გადატანის რეალიზაციას. მარტივ სქემაში გამოიყენება 4 ქუბიტი: წყარო, მიმღები და 2 ქვემდებარე. აღვნიშნოთ, რომ ალგორითმის მუშაობის პროცესში წყაროს საწყისი მდგომარეობა დაინგრევა. შეუძლებელია ქვანტური მდგომარეობის ზუსტი ასლის მიღება ორიგინალის დაუნგრევლად. ტელეპორტაცია გვამღებს საშუალებას გადავცეთ სისტემის ქვანტური მდგომარეობა ჩვეულებრივი კლასიკური არხების კავშირის საშუალებით. ამის შედეგად შეიძლება სისტემის დაკავშირებული მდგომარეობის მიღება, რომელიც შედგება ქვესისტემისგან, რომელიც დაშორებულია დიდ მანძილზე.

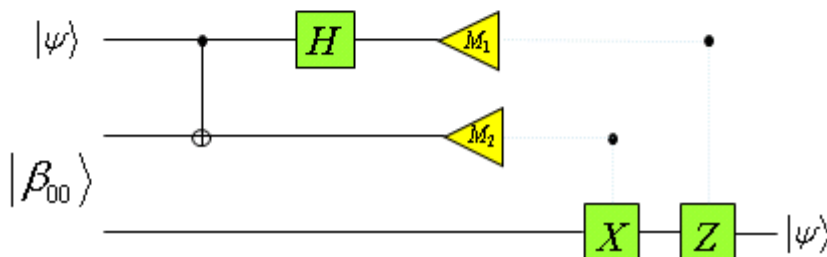
ქვანტური ტელეპორტაციის მაგალითი:



```

#include <qsim.h>
...
qubit psi(1, 2);
vector<qubit> q;
q.push_back(qubit::ZERO());
q.push_back(qubit::ZERO());
qreg reg(q);
reg.feed(qopr::H(), qopr::ID()); // Generate EPR Pair
reg.feed(qopr::CNOT()); // Generate EPR Pair
reg.push_front(psi);
reg.feed(qopr::CNOT(), qopr::ID());
reg.feed(qopr::H(), qopr::ID(), qopr::ID());
int M0 = reg.MES(0);
int M1 = reg.MES(0);
if(M1) reg.feed(qopr::X());
if(M0) reg.feed(qopr::Z());

```



თავი 3. ქვანტური კომპიუტერის კომპონენტები

3.1 ქვანტური ქუბიტი

ქვანტური კომპიუტერის მუშაობის საფუძველს წარმოადგენს ქუბიტი.



ქვანტური რეგისტრის 3 ქუბიტი ჩვეულებრივი 3 ბიტის წინააღმდეგ.

ქვანტური კომპიუტერი პრინციპიალურად განსხვავდება კლასიკური კომპიუტერისგან.

მაგალითი: გვაქვს ქუბიტი ქვანტურ მდგომარეობაში:

$$\frac{4}{5} |0\rangle - \frac{3}{5} |1\rangle$$

ამ შემთხვევაში 0-ის მიღების ალბათობაა :

$(4/5)^2 = 16/25 = 64\%$, ხოლო 1-ის მიღების ალბათობაა :

$(-3/5)^2 = 9/25 = 36\%$.

გამოთვლის შედეგად ქუბიტი გადადის ახალ ქვანტურ მდგომარეობაში $|0\rangle$, ანუ ამ ქუბიტის შემდეგი გაზომვისას მივიღებთ 0-ს 100 პროცენტით ალბათობით.

L ქუბიტების ქვანტურ სისტემას აქვს 2^L წრფივად დამოუკიდებელი მდგომარეობები, ე.ი. ქვანტური ქვანტური სუპერპოზიციის პრინციპის თანახმად ასეთი ქვანტური რეგისტრების მდგომარეობების სივრცეს წარმოადგენს 2^L გილბერტული სივრცე. ოპერაცია ქვანტურ გამოთვლებში შეესაბამება რეგისტრის მდგომარეობის შებრუნების ვექტორს ამ სივრცეში. ასე, რომ ქვანტურ გამოთვლით მოწყობილობას L ქუბიტი ზომით შეუძლია შეასრულოს პარალელურად 2^L ოპერაცია.

დავუშვათ, რომ გვაქვს ერთი ქუბიტი. ამ შემთხვევაში გამოთვლის შემდეგ, ე.წ. კლასიკურ ფორმაში, შედეგი იქნება 0 ან 1. ქუბიტი ქვანტური ობიექტია და ამიტომ განუსაზღვრელობის პრინციპის თანახმად, გამოთვლის შედეგად შეიძლება იყოს 0-იც და 1-იც განსაზღვრული ალბათობით. თუ ქუბიტი უდრის 0-ს (ან 1-ს) 100 პროცენტით ალბათობით, მაშინ მისი მდგომარეობა აღინიშნება სიმბოლოთი $|0\rangle$ (ან $|1\rangle$) დირაკის აღნიშვნებში. $|0\rangle$ და $|1\rangle$ ბაზისური მდგომარეობებია. საერთო შემთხვევაში ქუბიტის ქვანტური მდგომარეობა იმყოფება ბაზისურებს „შორის“ შემდეგი სახით:

$a|0\rangle + b|1\rangle$, სადაც $|a|^2$ და $|b|^2$ გაზომვის ალბათობებია 0 ან 1 შესაბამისად; $a, b \in \mathbb{C}$ $|a|^2 + |b|^2 = 1$. გაზომვის დამთავრებისას ქუბიტი გადადის ბაზისურ ქვანტურ მდგომარეობაში, კლასიკური შედეგის ანალოგიურად.

ახსნისათვის მოვიყვანოთ ორი მაგალითი ქვანტური მექანიკიდან:

➤ ფოტონი იმყოფება სუპერპოზიციის მდგომარეობის ორ პოლარიზაციაში;

გამოთვლები ერთხელ და სამუდამოდ აკოლაფსირებენ ფოტონის მდგომარეობას გარკვეული პოლარიზაციით.

- რადიოაქტიურ ატომს აქვს ნახევრად დაშლის გარკვეული პერიოდი;

გამოთვლებმა შეიძლება გამოარკვეოს ის, რომ იგი ჯერ არ დაშლილა, მაგრამ ეს არ ნიშნავს იმას, რომ იგი არასდროს არ დაიშლება.

გადავიდეთ ორი ქუბიტის სისტემაზე. თითოეულის გამოთვლამ შეიზლება მოგვცეს 0 ან 1. ამიტომ სისტემას აქვს 4 კლასიკური მდგომარეობა: 00, 01, 10 და 11. მათი ანალოგიური ბაზისური ქვანტური მდგომარეობებია: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.

სისტემის საერთო ქვანტურ მდგომარეობას აქვს შემდეგი სახე:

$$a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle.$$

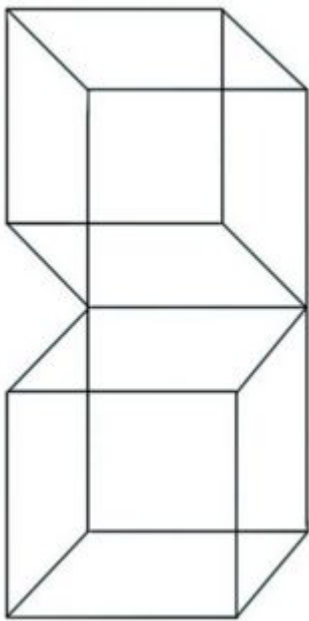
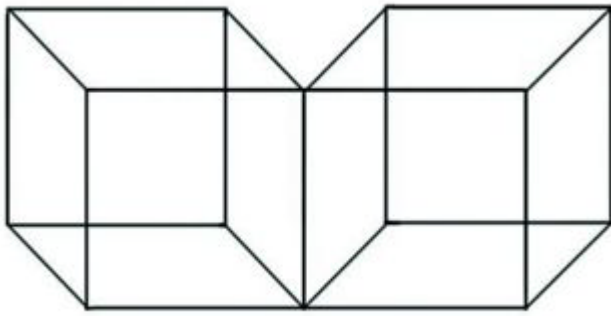
$|a|^2$ არის 00-ის გაზომვის ალბათობა და ა.შ. $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$ აღვნიშნოთ როგორც მთლიანი ალბათობა.

ასე რომ ერთი ოპერაცია ქუბიტების ჯგუფზე ეხება ყველა მნიშვნელობებს, რომლებიც შეიძლება მიიღოს, კლასიკური ბიტისგან განსხვავებით. ეს კი განაპირობებს გამოთვლების უპრეცედენტო პარალელიზმს.

აღმოჩნდა, რომ ნებისმიერი გამოთვლის აგებისათვის საკმარისია ორი ბაზისური ოპერაცია. ქვანტური სისტემა გვადლევს შედეგს მარტო რაღაც ალბათობით, რომელიც სწორია. მაგრამ ალგორითმში ოპერაციების ცოტათი გაზრდისას შეიძლება რამდენითაც გვინდა იმდენით მივაახლოვოთ სწორი შედეგის ერთიანის მიღების ალბათობა.

ბაზისური ქვანტური ოპერაციების საშუალებით შეიძლება დავასიმულიროთ ჩვეულებრივი ლოგიკური ელემენტები, რისგანაც გაკეთებულია ჩვეულებრივი კომპიუტერი. ამიტომ ნებისმიერი ამოცანა, რომელიც ამოხსნილია ამჟამად, ქვანტური კომპიუტერი ამოხსნის იგივე დროში.

შემდეგ ნახაზზე წარმოდგენილია ოპტიკური ქუბიტი:



ეს არის ე.წ. ნეკერის კუბები. ამ გამოსახულებაზე კუბები იმყოფებიან ერთდროულად ოთხ მდგომარეობაში. ყველა ოთხი მდგომარეობა არსებობს, მაგრამ როდესაც ჩვენ ვახდენთ ვიზუალურ სკანირებას, მაშინ რეალური ხდება მხოლოდ ერთი. ეს არის ქვანტური სუპერპოზიცია. ქვანტური ქუბიტები იმყოფებიან კონკრეტულ მდგომარეობაში მხოლოდ მაშინ, როდესაც ჩვენ ვაკვირდებით მათ. დანარჩენ დროს ისინი იმყოფებიან სუპერპოზიციის მდგომარეობაში, ანუ ერთდროულად იმყოფებიან რამოდენიმე მდგომარეობებში.

3.2 ქვანტური რეგისტრი

ქვანტური რეგისტრი წარმოადგენს L ქუბიტების რაღაც რიცხვის გაერთიანებას. კომპიუტერში ინფორმაციის შეტანამდე ქვანტური რეგისტრის ყველა ქუბიტი მიყვანილ უნდა იქნას ბაზისურ მდგომარეობაში $|0\rangle$. ამ ოპერაციის ეწოდება ინიციალიზაცია (მზადება). შემდეგ განსაზღვრული ქუბიტები (არა ყველა) ექვემდებარებიან სელექტიურ გარე ზემოქმედებას, რომელიც ცვლის ქუბიტების მნიშვნელობებს, ანუ მდგომარეობიდან $|0\rangle$ გადადიან მდგომარეობაში $|1\rangle$. ამასთან, მთლიანად ქვანტური რეგისტრის მდგომარეობა გადავა ბაზისური მდგომარეობების სუპერპოზიციაში $|nc$, ანუ ქვანტური რეგისტრის მდგომარეობა დროის საწყის მომენტში განსაზღვრული იქნება შემდეგი ფუნქციით:

$$|\psi(0)\rangle = \sum_{n=0}^{2^L-1} c_n |n\rangle$$

გასაგებია, რომ სუპერპოზიციის მოცემული მდგომარეობა შეგვიძლია გამოვიყენოთ n რიცხვის ბინარული (ორმაგი) წარმოდგენისათვის.

ქვანტურ პროცესორში შეყვანილი მონაცემები ექვემდებარებიან ქვანტური ლოგიკური ოპერაციების თანმიმდევრობას, რომლებიც მათემატიკური თვალსაზრისით აღიწერებიან უნიტარული გარდაქმნით $\hat{U}_{mn}$, რომელიც მოქმედებს მთლიანი რეგისტრის მდგომარეობაზე. შედეგად ქვანტური პროცესორის მუშაობის რამოდენიმე ტაქტის შემდეგ სისტემის საწყისი ქვანტური მდგომარეობა ხდება ახალი სუპერპოზიცია შემდეგი სახის:

$$|\psi(t)\rangle = \sum_{n,m=0}^{2^L-1} c_n \hat{U}_{mn} |n\rangle$$

ქვანტურ პროცესორთან დაკავშირებით გავაკეთოთ ერთი შენიშვნა. აღმოჩნდა, რომ ნებისმიერი გამოთვლის ასაგებად საკმარისია მხოლოდ ორი ბაზისური ბულის ლოგიკური ოპერაცია. ბაზისური ქვანტური ოპერაციების საშუალებით შეიძლება იმიტირება გავუკეთოთ ჩვეულებრივი ლოგიკური ელემენტების მუშაობას, რომლისგანაც გაკეთებულია ეს კომპიუტერები. რადგან ქვანტური ფიზიკის კანონები მიკროსკოპულ დონეზე არის წრფივი და შებრუნებადი, ამიტომ შესაბამისი ქვანტური ლოგიკური მოწყობილობებიც, რომლებიც ასრულებენ ოპერაციებს ცალკეული ქუბიტების ქვანტური მდგომარეობებით, აღმოჩნდებიან ლოგიკურები და თერმოდინამიურად შებრუნებადები.

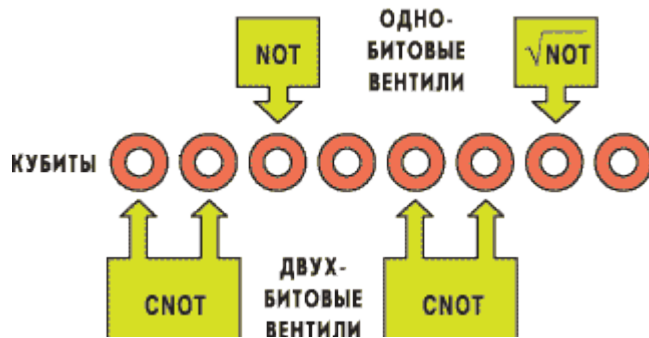
თეორიის პრინციპიალური მომენტი არის ის, რომ ეს რეგისტრი ექვემდებარება სუპერპოზიციის პრინციპს და ერთდროულად იმყოფება ყველა ბაზისურ კლასიკურ მდგომარეობებში, რომლის რიცხვი უდრის: $Q=2^N$. რეგისტრის ნებისმიერი მდგომარეობა შეიძლება ჩაიწეროს შემდეგი სახით: $|R\rangle = \sum_{i=1}^Q r_i |i\rangle$. რეგისტრის ბაზისური მდგომარეობა $|i\rangle$ უნდა გავიგოთ შემდეგნაირად: i რიცხვი ორობით ჩანაწერში გვიჩვენებს მდგომარეობებს, რომლებიც შეადგენენ ქუბიტების რეგისტრს. მაგალითად, ჩვენ ვამბობთ, რომ სამ ქუბიტის რეგისტრი იმყოფება მდგომარეობაში $|6\rangle$, ან ორობით ჩანაწერში $|6=110_2\rangle$, როდესაც შემადგენელი რეგისტრის ქუბიტებს აქვთ მდგომარეობები: $q_1=|1\rangle$, $q_2=|1\rangle$, $q_3=|0\rangle$. r_i კოეფიციენტს აქვს იგივე ალბათობითი აზრი, როგორც ქუბიტის შემთხვევაში: $|r_i|^2$ არის რეგისტრის $|i\rangle$ მდგომარეობაში აღმოჩენის ალბათობა. ასევე სრულდება ნორმირების პირობა: $\sum_{i=1}^Q |r_i|^2 = 1$.

სამ ქუბიტის ქვანტური რეგისტრის მაგალითი: $|R\rangle = \frac{1}{\sqrt{2}} |010\rangle + \frac{i}{2} |001\rangle + \frac{1}{2} |110\rangle$.

ქვანტურ რეგისტრზე გამოთვლების ჩატარების შედეგად (ფუნქციის საერთო თვისებების გამოვლენისთვის) ქვანტური გამოთვლითი მოწყობილობის გამოსასვლელზე გვაქვს ფუნქციის 2^N სუპერპოზიცია რეგისტრის ყველა კლასიკური მდგომარეობებიდან. მთავარ მომენტს წარმოადგენს ის ფაქტი, რომ რეგისტრის ნებისმიერი მდგომარეობა არ წარმოადგენს ცალკეული ქუბიტების მდგომარეობების შემდეგი ტიპის ნამრავლს:

$|R\rangle = |q_1\rangle |q_2\rangle \dots |q_N\rangle$. მაგალითად, რეგისტრის მდგომარეობაში $|R\rangle = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$ ყოველი ქუბიტისათვის შეუძლებელია მისი მდგომარეობის შემდეგი სახით მითითება: $|q\rangle = a|0\rangle + b|1\rangle$, ანუ რეგისტრის მდგომარეობა არ წარმოადგენს ქუბიტების მდგომარეობების ტენზორულ ნამრავლს. ქუბიტების ასეთ მდგომარეობებზე ამბობენ, რომ იგი „შერეულია“ სხვა ქუბიტების მდგომარეობებში. რეგისტრის შერეული მდგომარეობები არის ის მომენტი, სადაც ჩნდება ქვანტური კომპიუტერის ახალი თვისება კლასიკურთან შედარებით.

ქვანტური რეგისტრი მოწყობილია თითქმის ისე, როგორც კლასიკური. ეს არის ქვანტური ბიტების ჯაჭვი, რომლებზეც შეიძლება ერთბიტიანი და ორ-ბიტიანი ლოგიკური ოპერაციების ჩატარება.



ნახ. ქვანტური რეგისტრი - ქვანტური ბიტების ჯაჭვი. ერთი ან ორ-ქუბიტის ქვანტური ვენტილები ($\text{NOT}^{1/2}$, NOT, CNOT და სხვა) განსაზღვრავენ ლოგიკურ ოპერაციებს ქუბიტებზე ან ქუბიტების ჯგუფზე.

ქვანტური რეგისტრის ბაზისურ მდგომარეობებს, რომლებიც შექმნილია L ქუბიტებით, მიეკუთვნება L სიგრძის ნულებისა და ერთიანების ყველა შესაძლო თანმიმდევრობა, ისევე, როგორც კლასიკურში. სულ შეიძლება იყოს 2^L კომბინაცია. ეს ბაზისური მდგომარეობები არ ანადგურებენ ქვანტური რეგისტრის ყველა შესაძლო მნიშვნელობებს (კლასიკურისგან განსხვავებით), რადგან არსებობენ სუპერპოზიციის მდგომარეობებიც, რომლებიც მოცემულია კომპლექსური ამპლიტუდებით.

დავუშვათ, რომ რეგისტრზე ხორციელდება გარე ზემოქმედება, მაგალითად, სივრცის ნაწილში მიეწოდება ელექტრონული იმპულსები ან მიმართულია ლაზერული სხივები. თუ ეს არის კლასიკური რეგისტრი, მაშინ იმპულსი, რომელიც შეიძლება განვიხილოთ როგორც გამოთვლითი ოპერაცია, შეცვლის L ცვლადებს. თუკი ეს ქვანტური რეგისტრია, მაშინ იგივე იმპულსს შეუძლია ერთდროულად გარდაქმნას ცვლადებამდე. ანუ, ქვანტურ რეგისტრს პრინციპში შეუძლია დაამუშაოს ინფორმაცია ბევრად უფრო სწრაფად თავის კლასიკურ ანალოგთან შედარებით. აქედან ჩანს, რომ პატარა ქვანტური რეგისტრები ($L < 20$) შეიძლება წარმოდგენილ იქნას ცალკეული კვანძების დემონსტრირებისთვის და ქვანტური კომპიუტერის მუშაობის პრინციპისთვის.

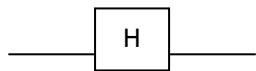
3.3 ქვანტური გეიტები

ქვანტური კომპიუტერი, კლასიკურის მსგავსად აგებულია ქვანტური სქემებით. ქვანტური სქემა ეს არის გამოთვლითი მოდელი, რომელიც წარმოადგენს ქვანტური გეიტების სიმრავლეს. ქუბიტების ტრანსფორმაცია ხორციელდება ქვანტური გეიტებით. ზოგადად n ქუბიტისანი გეიტის მდგომარეობა შეიძლება გამოვსახოთ როგორც $|\psi\rangle = \sum_{i=0}^{2^n-1} a_i |i\rangle$ ქვანტური ფიზიკის კანონებზე დაყრდნობით დადგენილია, რომ ყველა გარდაქმნა, რომელიც ხორციელდება ქვანტური პროცესებით, არის შექცევადი და უნიტარული. რაც ნიშნავს, რომ თუ გვაქვს ქვანტური სისტემა U , რომლის შესავალი მდგომარეობა არის $|\psi\rangle$, ხოლო გამოსავალზე გვაქვს განსხვავებული $|\psi'\rangle$ მდგომარეობა, მაშინ შეგვიძლია U ავღწეროთ, როგორც უნიტარული წრფივი ტრანსფორმაცია.

$U \begin{pmatrix} a & b \\ c & d \end{pmatrix} = U \begin{pmatrix} a^* & b^* \\ c^* & d^* \end{pmatrix}$ ოპერატორი, რომელიც ახორციელებს უნიტარული ვექტორის გარდაქმნას სხვა უნიტარულ ვექტორად, არის უნიტარული და აკმაყოფილებს პირობას: $U^\dagger U = 1$. ამ მხრივ მნიშვნელოვანია ჰადამარის გეიტი. ჰადამარის ოპერატორი არის

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

სქემატურად იგი გამოისახება შემდეგნაირად:



მისი მოქმედების შედეგი ასეთია:

$$H : |0\rangle \rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$H : |1\rangle \rightarrow \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

თუ გვაქვს n ქუბიტისანი რეგისტრი, მაშინ თუ გამოვიყენებთ ადამარის გარდაქმნას თითოეული ქუბიტისათვის მივიღებთ სუპერპოზიციას 2^n მდგომარეობების.

$$(H \otimes H \otimes \dots \otimes H) |00 \dots 0\rangle = \frac{1}{\sqrt{2^n}} ((|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes \dots \otimes (|0\rangle + |1\rangle)) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

ეს არის უოლშ-ჰადამარის გარდაქმნა W , რომელიც შეიძლება განისაზღვროს რეკურსიულად შემდეგნაირად:

$$W_1 = H, W_{n+1} = H \otimes W_n$$

განვიხილოთ სუპერპოზიცია ყველა შემავალი შესაძლო მნიშვნელობების, როგორც ერთი მდგომარეობა. საწყისი მდგომარეობა იყოს $|00 \dots 0\rangle$. გამოვიყენოთ უოლშ-ჰადამარის გარდაქმნა სუპერპოზიციის

$\frac{1}{\sqrt{2^n}} (|00 \dots 0\rangle + |00 \dots 1\rangle + \dots + (|11 \dots 1\rangle + |1\rangle))$ მისაღებად, რომელიც შეიძლება განვიხილოთ, როგორც სუპერპოზიცია ყველა რიცხვის $0 \leq x \leq 2^n - 1$. უწრფივი გარდაქმნა შეიძლება გამოყენებულ იქნეს ყველა ბაზისური მდგომარეობისათვის სუპერპოზიციაში დამოუკიდებლად. ამიტომ თუ მას გამოვითვლით ერთხელ, მაშინ შესაძლებელია გამოთვლილი იქნეს ყველა 2^n მნიშვნელობა $f(0), \dots, f(2^n - 1)$,

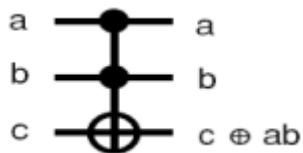
$$|\psi\rangle = U_f \left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \right) |0\rangle = \left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \right) |f(x)\rangle. \text{ ეს კი არის ქვანტური პარალელიზმის ეფექტი.}$$

ნებისმიერი ქვანტური ალგორითმი მანიპულირებს ქვანტური პარალელიზმის ეფექტით, ისე, რომ შედეგი ყოველთვის მიიღება გაზომვის მაღალი ალბათობით.

ტოფოლის გეიტი არის უნივერსალური გეიტი კლასიკური გამოთვლებისათვის, თუმცა მას საკმაოდ მნიშვნელოვანი ადგილი უჭირავს ქვანტურ გამოთვლებშიც. მისი უნივერსალურობა განპირობებულია იმით, რომ იგი k შესაძლებელია გამოყენებულ იქნეს ნებისმიერი გეიტის წარმოდგენისათვის. იგი არის სამ კუბიტიანი გეიტი. შესავალზე იღებს სამ ბიტს a, b, c ხოლო გამოსავალზე იძლევა a', b', c' . პირველი ორი a და b ბიტები არის კონტროლირებადი, რაც ნიშნავს, რომ ისინი არ იცვლებიან გამოთვლების განმავლობაში, ხოლო მესამე იცვლება იმ შემთხვევაში, თუ ორივე a, b არის 1-ის ტოლი.

შემაჯალი			გამომავალი		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	0	0	0	1	0
0	1	1	0	1	1
1	1	0	1	0	0
1	0	1	1	0	1
1	0	0	1	1	1
1	1	1	1	1	0

მისი შესაბამისი სქემა გამოისახება შემდეგნაირად:



ყველა გამოთვლა, რომელიც სრულდება კლასიკურ კომპიუტერებზე, შესაძლებელია განხორციელდეს ქვანტურ კომპიუტერზეც. უპირატესობა არის ის, რომ ქვანტური გამოთვლები, რომლებიც ხორციელდება ქვანტური ალგორითმებით არის უფრო სწრაფი. ყოველივე ეს კი განპირობებულია ქვანტური პარალელიზმით და ქვანტური აბურდვით, რომლებიც მიუღწეველია კლასიკურ კომპიუტერებში.

თავი 4. ქვანტური გამოთვლები

4.1 ქვანტური გამოთვლების გამოჩენა

ქვანტური გამოთვლების გამოყენების იდეა პირველად გამოთქვა მათემატიკოსმა იუ.ი.მანიმა 1980 წელს თავის ცნობილ მონოგრაფიაში „გამოთვლითი და არაგამოთვლითი“. ინტერსი მისი ნაშრომის მიერ წარმოიქმნა 1982 წელს ამერიკელი ფიზიკოს-თეორეტიკოსის ნობელის ლაურეატის რიჩარდ ფეინმანის მიერ იგივე თემაზე გამოქვეყნებული სტატიის შემდეგ. მან შეამჩნია, რომ გარკვეული ქვანტურ-მექანიკური ოპერაციები არ შეიძლება ზუსტად გადავიტანოთ კლასიკურ კომპიუტერზე. ამ დაკვირვებებმა მიიყვანა იმ აზრამდე, რომ მსგავსი გამოთვლები შეიძლება იყოს უფრო ეფექტური თუ მათ განვახორციელებთ ქვანტური ოპერაციების საშუალებით. მაგალითისთვის განვიხილოთ ქვანტურ-მექანიკური ამოცანა ქვანტური სისტემის მდგომარეობის ცვლილებაზე, რომელიც შედგება n სპინისგან დროის გარკვეულ მონაკვეთში. n სპინის სისტემის საერთო მდგომარეობა აღიწერება ვექტორით 2^n კომპლექსურ სივრცეში, მისი მდგომარეობის ცვლილება კი უნიტარული მატრიცით $2^n \times 2^n$ ზომის. თუ განსახილველი დროის მონაკვეთი ძალიან პატარაა, მაშინ მატრიცა აგებულია ადვილად და მისი თითოეული ელემენტი ადვილად გამოითვლება თუ ვიცით სპინებს შორის ურთიერთქმედება. თუ საჭიროა სისტემის მდგომარეობის ცვლილების გაგება დროის დიდ მონაკვეთში, მაშინ უნდა გადავამრავლოთ ისეთი მატრიცები, რომლისთვისაც დაგვჭირდება ოპერაციების ექსპონენციალურად დიდი რაოდენობა. დღესდღეობით მოცემული გამოთვლის შემცირების მეთოდი არ არსებობს და ქვანტური მექანიკის მოდელირება წარმოადგენს ექსპონენციალურად რთულ მათემატიკურ ამოცანას. მაგრამ თუ კლასიკურ კომპიუტერებს არ შეუძლიათ ქვანტური ამოცანების ამოხსნა, მაშინ შესაძლებელია თუ არა ქვანტური სისტემის გამოყენება? და თუ ეს შესაძლებელია, მაშინ შეესაბამებია თუ არა ქვანტური სისტემები სხვა ამოცანების ამოხსნას? მსგავს შეკითხვებს განიხილავდნენ ფეინმანი და მანი.

1985 წელს დევიდ დოიჩმა მოგვანახა ქვანტური მანქანის კონკრეტული მათემატიკური მოდელი. ქვანტური კომპიუტერების პრაქტიკული რეალიზაცია აღმოჩნდა ძალიან რთული. მეცნიერები პესიმიზმით ემხრობოდნენ იმას, რომ ქვანტურ ოპერაციებს შეუძლიათ გარკვეული ამოცანების ამოხსნის დაჩქარება. ასე გრძელდებოდა 1994 წლამდე, როდესაც ამერიკელმა მათემატიკოსმა პიტერ შორმა შემოგვთავაზა ქვანტური კომპიუტერისათვის n -ნიშნა რიცხვის დაყოფა მარტივ მამრავლებად პოლინომიალურად n -ზე დამოკიდებულ დროში. შორის ქვანტური ალგორითმის ფაქტორიზაცია გახდა ერთ-ერთი ძირითადი ფაქტორი, რომელსაც

მიყვარებთ ქვანტური გამოთვლების მეთოდების ინტენსიურ განვითარებასთან. ჩნდება კითხვა: რატომ მიგვიყვანა ასეთ შეცდომებთან შორის მიერ შემოთავაზებულმა ფაქტორიზაციის ქვანტურმა ალგორითმმა? საქმე იმაშია, რომ რიცხვის მარტივ მამრავლებად დაშლის ამოცანას აქვს პირდაპირი კავშირი კრიპტოგრაფიასთან, კერძოდ კი RSA შიფრაციის პოპულარულ სისტემებთან.

4.2 ქვანტური გამოთვლების იდეა

ქვანტური გამოთვლების იდეა (მაგრამ არა მისი რეალიზაცია) შედარებით მარტივი და საინტერესოა, მაგრამ მისი ზედაპირული გაგებისათვის კი საჭიროა გავეცნოთ ქვანტური ფიზიკის რამოდენიმე სპეციფიკურ ცნებებს.

განვიხილოთ პოლარიზებული ფოტონის მარტივი მაგალითი. პოლარიზებული ფოტონი არის ორდონიანი ქვანტური სისტემის მაგალითი. ფოტონის პოლარიზაციის მდგომარეობა შეგვიძლია ვექტორის მდგომარეობის მოცემით, რომელიც განსაზღვრავს პოლარიზაციის მიმართულებას. ფოტონის პოლარიზაცია შეიძლება მიმართული იყოს ზევით ან ქვევით, ამიტომ საუბრობენ ორ ძირითად ბაზისურ მდგომარეობაზე, რომლებიც აღნიშნებიან როგორც $|1\rangle$ და $|0\rangle$. მოცემული აღნიშვნები (ბრა/კეტ აღნიშვნები) შემოიღო დირაკმა და აქვთ მკაცრი მათემატიკური განსაზღვრება, რომლებიც განსაზღვრავენ მათი მუშაობის წესებს. ბაზისური მდგომარეობების აზრი მდგომარეობს იმაში, რომ ნებისმიერი პოლარიზაცია შეიძლება გამოიხატოს როგორც ბაზისური მდგომარეობების წრფივი კომბინაცია, ანუ $a|1\rangle + b|0\rangle$. რადგან გვაინტერესებს მხოლოდ პოლარიზაციის მიმართულება, ამიტომ მდგომარეობის ვექტორი შეიძლება ჩავთვალოთ ერთიანად, ანუ $|a|^2 + |b|^2 = 1$.

დავუშვათ, გვაქვს ნებისმიერი ორდონიანი ქვანტური სისტემა, რომელიც ხასიათდება ბაზისური ორთოგონალური მდგომარეობებით $|1\rangle$ და $|0\rangle$. ქვანტური მექანიკის პოსტულატების თანახმად (სუპერპოზიციის პრინციპი) ქვანტური სისტემის შესაძლო მდგომარეობებიდან იქნება ასევე სუპერპოზიციები $y = a|1\rangle + b|0\rangle$, სადაც a და b კომპლექსური რიცხვებია, რომლებსაც ამპლიტუდებს უწოდებენ. აღვნიშნოთ, რომ მდგომარეობის სუპერპოზიციის ანალოგი კლასიკურ ფიზიკაში არ არსებობს. ქვანტური მექანიკის ერთ-ერთი პოსტულატი ამტკიცებს იმას, რომ ქვანტური სისტემის მდგომარეობის გაზომვისათვის საჭიროა მისი განადგურება. ანუ ქვანტურ ფიზიკასი გაზომვის ნებისმიერი პროცესი ანადგურებს სისტემის საწყის მდგომარეობას და იგი

გადაყავს ახალ მდგომარეობაში. ამის გაგება არ არის ადვილი, ამიტომ განვიხილოთ ეს დაწვრილებით.

საერთოდ, ქვანტურ ფიზიკაში გაზომვის გაგება თამაშობს დიდ როლს და არ ღირს მისი განხილვა როგორც გაზომვა კლასიკური გაგებით. ქვანტური სისტემის გაზომვა ხდება სულ, როდესაც იგი ურთიერთქმედებაშია „კლასიკურ“ ობიექტებთან, ანუ ობიექტებთან, რომლებიც ექვემდებარებიან კლასიკური ფიზიკის კანონებს. ასეთი ურთიერთქმედების შედეგად ქვანტური სისტემის მდგომარეობა იცვლება. რომ გავზომოთ ქვანტური სისტემა, საჭიროა როგორმე ვიმოქმედოთ მასზე კლასიკური ობიექტით, რის შემდეგაც მიმი საწყისი მდგომარეობა განადგურდება. ამის გარდა, შეიძლება ვამტკიცოთ, რომ გაზომვის შედეგად ქვანტური სისტემა გადავა თავის ერთ ბაზისურ მდგომარეობაში. მაგალითისათვის ორდონიანი ქვანტური სისტემის გაზომვისათვის საჭიროა მინიმუმ ორდონიანი კლასიკური ობიექტი, ანუ კლასიკური ობიექტი, რომელსაც შეუძლია მიიღოს ორი შესაძლო მნიშვნელობა: 0 და 1. გაზომვის დროს ქვანტური სისტემის მდგომარეობა გარდაიქმნება ერთ ბაზისურ ვექტორად, ამასთან თუ გაზომვისას კლასიკური ობიექტი ღებულობს 0-ის ტოლ მნიშვნელობას, მაშინ ქვანტური ობიექტი გარდაიქმნება მდგომარეობასთან $|0\rangle$, და თუ კლასიკური ობიექტი ღებულობს 1-ის ტოლ მნიშვნელობას, მაშინ კლასიკური ობიექტი გარდაიქმნება მდგომარეობასთან $|1\rangle$. ორდონიანი ქვანტური სისტემა შეიძლება იმყოფებოდეს სუპერპოზიციის მდგომარეობის უსასრულო სიმრავლეში, მაგრამ გაზომვის შედეგად იგი ღებულობს მხოლოდ ერთს და ორ შესაძლო ბაზისურ მდგომარეობებს შორის. ამპლიტუდის მოდულის კვადრატი $|a|^2$ განსაზღვრავს სისტემის გაზომვის ალბათობას ბაზისურ მდგომარეობაში $|1\rangle$, და ამპლიტუდის მოდულის კვადრატი $|b|^2$ ბაზისურ მდგომარეობაში $|0\rangle$.

ფოტონის მდგომარეობის გასაზომად დაგვჭირდება რაღაც კლასიკური მოწყობილობა კლასიკური ბაზისით $\{1,0\}$. მაშინ ფოტონის პოლარიზაციის მდგომარეობა $a|1\rangle + b|0\rangle$ განსაზღვრული იქნება როგორც 1 (ჰორიზონტალური პოლარიზაცია) ალბათობით $|a|^2$ და 0 (ვერტიკალური პოლარიზაცია) ალბათობით $|b|^2$.

რადგან ქვანტური სისტემის გაზომვას მივყავართ მის ერთადერთ ბაზისურ მდგომარეობასთან და შესაბამისად ანადგურებს სუპერპოზიციას, ამიტომ ეს ნიშნავს, რომ გაზომვის შედეგად ქვანტური სისტემა გადადის ახალ ქვანტურ მდგომარეობაში და შემდეგი გაზომვისას მივიღებთ მნიშვნელობას $|1\rangle$ 100 პროცენტით ალბათობით.

ქვანტურ კომპიუტერზე გამოთვლის შემოკლებული სქემა შემდეგნაირია: აიღება ქუბიტების სისტემა, რომელზეც იწერება საწყისი მდგომარეობა. შემდგომ სისტემის მდგომარეობა ან მისი ქვესისტემა იცვლება უნიტარული გარდაქმნებით, რომლებიც ასრულებენ ამათუ იმ ლოგიკურ ოპერაციებს. ბოლოს იზომება მნიშვნელობა და ეს არის კომპიუტერის მუშაობის შედეგი. კლასიკური კომპიუტერის ლოგიკური ბლოკების როლს თამაშობენ უნიტარული გარდაქმნები.

გამოთვლითი პროცესი მოიცავს სამ ოპერაციას. დასაწყისში ხდება ინიციალიზაცია (საწყისი მდგომარეობის მომზადება), რომლის დროსაც ყველა ქუბიტი გადადის ძირითად ბაზისურ მდგომარეობაში - 0. შემდეგ ხდება ინფორმაციის შეტანა. ამასთან, რეგისტრი გადადის ბაზისური მდგომარეობის სუპერპოზიციაში. შემდეგი ეტაპი არის ინფორმაციის დამუშავება ქვანტური პროცესორით. ამასთან, რეგისტრზე მიმდინარეობს მთელი რიგი ლოგიკური ოპერაციებისა, რის შედეგადაც იგი იღებს ახალ ქვანტურ მდგომარეობას, რაც არის გამოთვლის შედეგი.

თავი 5. ქვანტური ალგორითმი

5.1 გროვერის ძებნის ქვანტური ალგორითმი

ისევე როგორც კლასიკური ალბათური ალგორითმები, ქვანტური ალგორითმები გამოსახავენ მდგომარეობებს სხვადასხვა ალბათური განაწილებებით. მათი საშუალებით მდგომარეობის სრულად აღწერა არ ხდება. მდგომარეობის სრულად აღწერისათვის საჭიროა მდგომარეობათა ამპლიტუდების ცოდნა, რომელიც კომპლექსური რიცხვით გამოისახება. სისტემის ევოლუცია გამოისახება მდგომარეობის ცვლილების მატრიცით. თუ ცნობილი იქნება საწყისი განაწილება და მდგომარეობის ცვლილების მატრიცა, მაშინ შესაძლებელია გამოვთვალოთ განაწილება დროის ნებისმიერ მომენტში. მდგომარეობათა ალბათობა არის კვადრატული ფესვი ამპლიტუდის აბსოლუტური მნიშვნელობიდან.

ქვანტურ გამოთვლებშიერთ-ერთი უმნიშვნელოვანესი ადგილი უჭირავს გროვერის ალგორითმს, რომლის საშუალებითაც ხდება დაულაგებელ $N=2^n$ ელემენტთან მონაცემთა ბაზაში

და რომელიც ამტკიცებს, რომ ქვანტზე ინფორმაციის თვისებებს შეუძლიათ გააუმჯობესონ გარკვეული ღირებულებების პოვნა მონაცემთა ბაზის საზღვრებში. ქვანტურ ძებნას გამოთვლით შესაბამისობაში, როგორც ამტკიცებენ, შეუძლია მიაღწიოს დაახლოებით $O(N^{1/2})$ ოპერაციას ($O(N)$ კლასიკურ ოპერაციასთან შედარებით). მაგრამ ეს გაუმჯობესება სხვა ქვანტურ ალგორითმებთან შედარებით შეიძლება ჩავთვალოთ უმნიშვნელოდ.

თითქმის ყველა ქვანტური ალგორითმი შეიძლება წარმოვადგინოთ როგორც მოდელი, სადაც შესასვლელი მოცემულია როგორც „შავი ყუთი“, რომელიც პასუხობს გარკვეული სახის შეკითხვებს. შეკითხვის მოდელში შესასვლელი $x_1, \dots, x_n$ არის შავ ყუთში და შესაძლებელია გვეპოვება წვდომა შავი ყუთის შეკითხვასთან. ყოველ შეკითხვაზე ჩვენ შავ ყუთს გადავცემთ i და შავი ყუთი გვიბრუნებს x_i -ს. მიზანი მდგომარეობს იმაში, რომ პრობლემა გადავწყვიტოთ შეკითხვების მინიმალური რაოდენობით.

ქვანტურ მოდელში შეკითხვის განსაზღვრის ორი მეთოდი გვაქვს.

პირველ შემთხვევაში გვაქვს ორი შესასვლელი i და j , სადაც i შედგება $\log_2 N$ ბიტისგან და j შედგება 1 ბიტისგან. თუ შესასვლელი ყუთთან არის ბაზისური მდგომარეობა $|i\rangle|j\rangle$, მაშინ შესასვლელი არის $|i\rangle|j\rangle \oplus x_i$, სადაც $\oplus$ არის დამატებითი მოდული 2.

თუ შესასვლელი არის სუპერპოზიცია $\sum_{i,j} a_{i,j} |i\rangle|j\rangle$, მაშინ შესასვლელი არის $\sum_{i,j} a_{i,j} |i\rangle|j\rangle \oplus x_i$.

ქვანტური მოდელის მეორე ფორმაში შავ ყუთს აქვს მხოლოდ ერთი შესასვლელი i . თუ შესასვლელი არის მდგომარეობა $\sum_i a_i |i\rangle$, მაშინ მოგვცემს $\sum_i a_i (-1)^{x_i} |i\rangle$.

პრობლემების ძირითადი ნაწილი შეიძლება წარმოდგენილი იყოს როგორც ძებნის პრობლემა შემდეგი ფორმით: ვოპოვოთ რაღაც x ისეთი, რომ $f(x)$ იყოს ჭეშმარიტი.

მონაცემთა ბაზის ასეთი პრობლემური დიაპაზონი ეძებს სორტირებით. სორტირების პრობლემა შეიძლება განვიხილოთ როგორც გადანაცვლების ძებნა, რომლისთვისაც წინადადება „ x იღებს საწყის მდგომარეობას სორტირებული მდგომარეობიდან“ არის ჭეშმარიტი.

ძებნის არასტრუქტურირებული პრობლემა არის პრობლემა, სადაც არაფერი არ არის ცნობილი ამონახსნის სტრუქტურაზე და f მდგომარეობაზე. მაგალითად, $f(x_0)$ არ გვადლევს ინფორმაციას შესაძლო $f(x_1)$ -ზე $x_0 \neq x_1$ -თვის. ძებნის სტრუქტურირებული პრობლემა არის პრობლემა, სადაც ინფორმაცია ძებნაზე და f მდგომარეობაზე შეიძლება ექსპლუტირებული იქნას. მაგალითად, ძებნა ანბანის მიხედვით დალაგებულ სიაში არის სტრუქტურირებული პრობლემა.

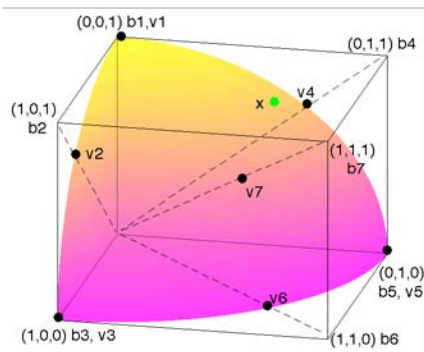
ნებისმიერმა კლასიკურმა ალგორითმმა რომ იპოვოს არასტრუქტურირებული მონაცემთა ბაზის N მოთხოვნა უნდა შეასრულოს საშუალოდ $O(N)$ ბიჯი. გროვერის არაკლასიკური კვანტური ალგორითმი ეძებს ასეთ მონაცემთა ბაზას $O(\sqrt{N})$ ბიჯის შესრულებისას $O(\sqrt{N} \lg N)$ გამოთვლითი ღირებულებით. ეს არის ექსპონენციალურად დიდი აჩქარება.

გროვერის ალგორითმი არის უფრო ადვილი განსახორციელებელი ვიდრე სხვა კვანტური ალგორითმები შემდეგი მიზეზების გამო:

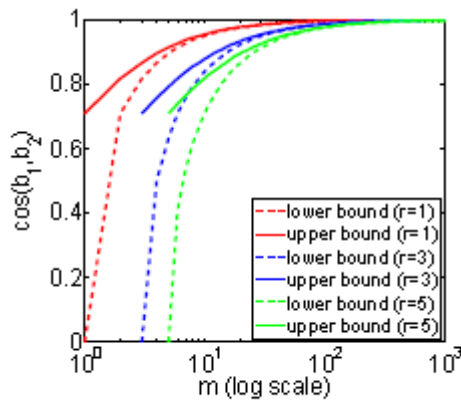
- ❖ ერთადერთი საჭირო ოპერაციები, პირველ რიგში, უოლშ-ჰადამარდის გარდაქმნები და მეორე, ფაზის ცვლილების პირობითი ოპერაცია. აქედან ორივე ადვილია იმ ოპერაციებთან შედარებით, რომლებსაც ითხოვენ სხვა კვანტური მექანიკური ალგორითმები;
- ❖ კვანტური მექანიკური ალგორითმები, რომლებიც დაფუძნებულია უოლშ-ჰადამარდის გარდაქმნებზე, უფრო ადვილად განსახორციელებადია, ვიდრე ფურიეს ფართო გარდაქმნებზე დაფუძნებულები;
- ❖ ფაზის პირობითი ცვლილება უფრო ადვილი განსახორციელებელია, თუ ალგორითმი გამოიყენებს მეთოდს, სადაც ფორმის მეხსიერება კი არ აქვს აღდგენილი, არამედ ფუნქციაა გამოთვლილი ყოველ პუნქტზე;
- ❖ იმ შემთხვევაში, თუ ელემენტები იქნა აღდგენილი, მაშინ მონაცემები შენახული უნდა იყოს კლასიკურ მეხსიერებაში;

განვიხილოთ ორობითი კოდების შესწავლის პრობლემა არაუარყოფითი მონაცემების ეფექტური ძებნისთვის. ასეთი ვექტორები ხშირად იზომება მათ შორის კუთხის კოსინუსის გამოყენებით. ჩვენ შემოვიღებთ ახალ ტექნიკას ორობითი კოდების კვანტიზაციაზე ასეთი მონაცემებისთვის და გავანალიზებთ მათ თვისებებს. ჩვენი მიზანი მდგომარეობს იმაში, რომ ვიპოვოთ კვანტიზაციის სქემა.

დავუშვათ, გვაქვს X მონაცემთა ბაზა, რომელიც შეიცავს n d -დომენსიონალ წერტილს და $X = \{x_i\}_{i=1}^n$, სადაც $x_i \in R^d$.



ქვანტიზაციის მოდელი 3D-ში.



(b) Cosine of angle between binary vertices.

მოცემული მოდელის ერთ-ერთი უმთავრესი თვისებაა ის, რომ ორიენტირის რიცხვი იზრდება ექსპონენციალურად.

შესაბამისი ალგორითმი წარმოდგენილია შემდეგი სახით:

ჰიპერსფეროზე პუნქტისთვის ყველაზე ახლო ორმაგი ორიენტირის პოვნა.

შესასვლელი: x პუნქტი ჰიპერსფეროზე.

გასასვლელი: $\hat{b}$ - ორმაგი ვექტორი, რომელსაც აქვს ყველაზე პატარა კუთხე x -თან.

1. ვასორტირებთ ჩანაწერებს კლებადობის მიხედვით $x_1, \dots, x_d$;
2. for $k=1, \dots, d$;
3. if $x_k=0$ break;
4. Form binary vector b_k whose elements are 1 for the k largest positions in x , 0 otherwise;
5. გამოვთვალოთ $\psi(x,k)=(x^T b_k)/\|b_k\|_2=(\sum_j^k x_j)/\sqrt{k}$;
6. end for;

7. return b_k , რომელსაც შეესაბამება $m = \arg \max_k \psi(x, k)$.

ალგორითმი წარმოადგენს ჩვენი ქვანტიზაციის მეთოდის ფუძეს, მაგრამ მას აქვს რამოდენიმე შეზღუდვა:

- ❖ არ შეუძლია ქვანტიზაციის შეცდომის მართვა;
- ❖ არ შეუძლია m -ის მართვა, რომელიც დაფუძნებულია ჩვენს ანალიზზე;

5.2 ძეზნის ქვანტური ალგორითმის საშუალებებით მათემატიკური პრობლემების გადაჭრა

ქვანტურმა გამოთვლებმა მიიქცია დიდი ყურადღება, როგორც აჩვენეს შორმა და გროვერმა ქვანტური ალგორითმების გამოყენების შესაძლებლობა, რომელიც ეძებს უფრო ჩქარი მეთოდებით ვიდრე ცნობილი კლასიკური ალგორითმი. შესაძლებელია გროვერის ალგორითმის გამოყენება მონაცემთა ბაზაში გარკვეული ღირებულებების მოსაძებნათ, მაგალითად, ლოგიკური ფუნქციის ნოლი: მონაცემთა ბაზაში მინიმალური ან მაქსიმალური ღირებულება. აქ ჩვენ ვაჩვენებთ ქვანტურ ალგორითმებს რომ ამოვხსნათ ეს ციტირებული მათემატიკური პრობლემები. ამოხსნა მოითხოვს ქვანტური კომპარატორის გამოყენებას. იგი ადარებს ორ ქვანტურ მდგომარეობას და აიდენტიფიცირებს, ტოლია თუ არა ისინი ან რომელია მათ შორის ყველაზე დიდი.

5.3 ლოგიკური ფუნქციის ნულის პოვნა

ერთ-ერთი გამოყენებაა ფუნქციის ნულის ძეზნის საინტერესო პრობლემა. ვივარაუდოთ, რომ U უნიტარული გარდაქმნა წარმოადგენს ფუნქციას, რომლის ნულიც უნდა ვიპოვოთ. ნახ.4-ში n ბიტის ორმაგი რიცხვია. ქვანტური კომპარატორი აქტივაციას უკეთებს $CNOT(O1=O2=0)$ -ს მხოლოდ იმ შემთხვევაში თუ $f(x)=0^n$. აქედან გამომდინარეობს, რომ ორაკული აღიქვამს მხოლოდ f ფუნქციის ნულს.

ძეზნის ქვანტური ალგორითმი დეტალებში: $(M=1, N=2^n)$

შესასვლელი:

$$x_1 = \{0,1\}, x_2 = \{0,1\}, \dots, x_N = \{0,1\}, f: \{0,1\}^N \rightarrow \{0,1\}; f(x) = 0$$

ყველა $0 \leq x \leq N$ $\omega = x_i$ $f(x_i) = 1$

➤ n ქუბიტები იმყოფებიან $|0\rangle$ მდგომარეობაში და 1 ქუბიტი კი შემდეგ მდგომარეობაში:

$$\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

1. საწყისი მდგომარეობაა

$$|0\rangle^{\otimes n} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

2. პირველი n ქუბიტებისთვის ვიყენებთ $H^{\oplus n}$ ფუნქციას →

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

3. ვიყენებთ გროვერის იტერაციას $k \approx \frac{\pi}{4} \sqrt{N}$ დროში →

$$\left[(2|\Psi\rangle\langle\Psi| - I)(I - 2|\omega\rangle\langle\omega|) \right]^k \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] \approx |\omega\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

4. პირველი n ქუბიტების გაზომვა $|\omega\rangle$

5.4 მაგალითები

თივაში ნემსის პოვნა:

მოვიყვანოთ ამოცანის მაგალითი, რომელშიც ქვანტური ალგორითმი ბვრად ჯობია კლასიკურს. ამისათვის ჩამოვაყალიბოთ ძებნის შემდეგნაირი ამოცანა.

მოცემულია: „შავი ყუთი“, რომელიც გამოთვლის ფუნქციას $f:M \rightarrow \{0,1\}$, სადაც M არის რაღაც სასრული სიმრავლე. წინასწარ ცნობილია, რომ ფუნქცია უდრის 1-ს M სიმრავლის მხოლოდ ერთ y წერტილში.

ვიპოვოთ: y წერტილი.

ჯერ დავამტკიცოთ, რომ ნებისმიერი ალბათობითი ალგორითმი, რომელიც ხსნის ამ ამოცანას ϵ შეცდომის ფიქსირებული ალბათობით, უნდა გააკეთოს წრფივი მოთხოვნების რაოდენობა M სიმრავლის ზომისგან. M სიმრავლეში ელემენტების რაოდენობა აღვნიშნოთ m -ით.

დავუშვათ, რომ ალგორითმი აკეთებს ზუსტად k მოთხოვნას და ყველა მოთხოვნის შესრულების შემდეგ უყურებს პასუხებს, ანუ ალგორითმი არის არაადაპტური. იმ მომენტამდე სანამ მოიძებნება y წერტილი ყველა პასუხი ერთნაირია და ყველა ალგორითმი იქცევა ისე როგორც რომელიმე არაადაპტური.

ჩვენ ვაფასებთ ალგორითმის მუშაობას ყველა შესაძლო შესასვლელისთვის. ამიტომ გვაინტერესებს „ცუდი შემთხვევა“. წარმოვიდგინოთ, რომ პასუხებს ამზადებს მოწინააღმდეგე, რომლის მიზანია - დაგვამალოს, რომ მივიღოთ არასწორი პასუხი. მოწინააღმდეგემ იცის ჩვენი ალგორითმი და ირჩევს ამოცანის შესასვლელს, რომელიც ეყრდნობა ამ ცოდნას და უკვე გაკეთებულ მოთხოვნებს. ის იყოს ალბათობა იმისა, რომ ალგორითმმა მოითხოვა წერტილები S , $|S|=k$.

ალგორითმის წარმატება ნიშნავს, რომ $y \in S$. წარმატების ალბათობაა:

$$p(y) = \sum_{S \ni y} p_S.$$

არსებობს ისეთი y , რომ $p(y) \leq k/m$. მართლაც რომ

$$\frac{1}{m} \sum_y p(y) = \frac{1}{m} \sum_y \sum_{S \ni y} p_S = \frac{k \sum p_S}{m} = \frac{k}{m}.$$

ცულ შემთხვევაში წარმატების ალბათობა იქნება:

$$p^* \leq \frac{k}{m}$$

$$\text{თუ } p^* > 1-\epsilon, \text{ მაშინ } 1-\epsilon < p^* \leq \frac{k}{m}$$

მაშასადამე, $k=\Omega(m)$, სადაც კონსტანტა Ω დამოკიდებულია ϵ შეცდომის ალბათობის არჩევაზე. ახლა ავაგოთ ქვანტური ალგორითმი, რომელიც ხსნის ძეზის ამოცანას მოთხოვნების შედარებით ნაკლები რაოდენობით.

$$\text{გამოვიყენოთ ფაზური მოთხოვნა: } O_y: |x\rangle \rightarrow (-1)^{\delta(y,x)} |x\rangle$$

სხვა სიტყვებით რომ ვთქვათ, „შავი ყუთი“ იძლევა პასუხს $\{y\}$ სიმრავლის ფუნქციის დახასიათების მნიშვნელობების მოთხოვნაზე. გეომეტრიული ოპერატორი O_y იძლევა გამოსახულებას $C(M)$ სივრცეში გიპერსივრცის შესაბამისად, რომელიც ორტოგონალურია $|y\rangle$ ვექტორის. დაგვჭირდება ოპერატორი:

$$R_\psi = 2|\psi\rangle\langle\psi| - I, \quad |\psi\rangle = \frac{1}{\sqrt{m}} \sum_x |x\rangle.$$

გროვერის ალგორითმი შედგება $G=R_\psi O_y$ ოპერატორის მიმდევრობით გამოყენებაში. საწყის მდგომარეობად ავირჩიოთ $|\psi\rangle$.

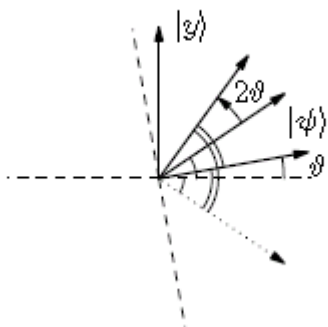
გროვერის ალგორითმი შედგება შემდეგი ბიჯებისგან:

- ❖ ვამზადებთ $|0\rangle$ მდგომარეობას;
- ❖ გარდავექმნით $|0\rangle$ მდგომარეობას $|\psi\rangle$. -ში;
- ❖ ვიყენებთ G ოპერატორს $[(\pi/4)\sqrt{m}]$ -ჯერ;
- ❖ მიღებულ მდგომარეობას ვზომავთ კლასიკურ ბაზისში;
- ❖ პასუხი: გაზომვის შედეგი;

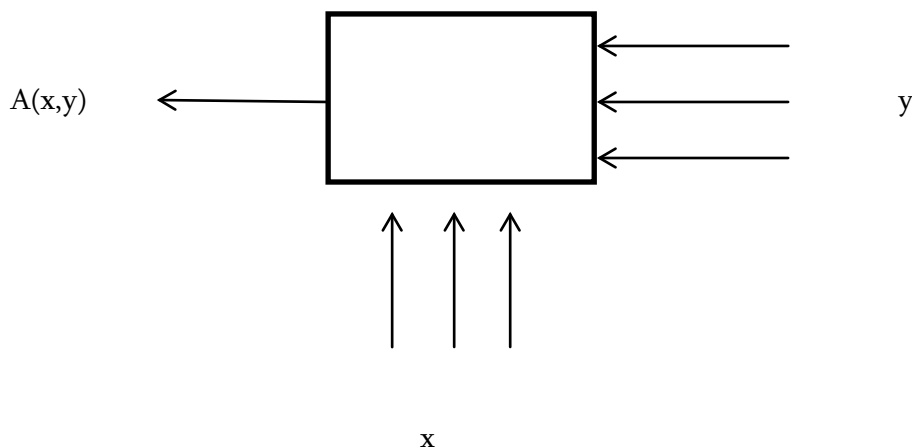
ალგორითმის აღწერიდან ჩანს, რომ იგი ასრულებს $O(\sqrt{m})$ მოთხოვნებს.

გროვერის ალგორითმი ხსნის ძებნის ამოცანას m ობიექტებს შორის $O(1/m)$ შეცდომის ალბათობით $O(\sqrt{m})$ მოთხოვნის დროს.

შემდეგ ნახაზზე მოცემულია გროვერის იტერაცია:



განვიხილოთ შემდეგი მაგალითი:



ნახაზზე მოცემულია გამოსაყენებელი ორაკულის სქემა.

ამოცანა: მოცემულია მოწყობილობა, რომელიც x, y შესასვლელებში განსაზღვრავს ბულის მნიშვნელობას $A(x, y)$. საჭიროა შემდეგი ფუნქციის გამოთვლა $F(x) = xA(x, y)$ და შემდეგის დაგვარად შესაბამისი y -ის მოძებნა.

მინიშნება: ვივარაუდოთ, რომ ყოველი x -ისთვის არსებობს ერთადერთი ისეთი y_0 , რომ $A(x, y_0) = 1$.

ალგორითმი: განვიხილოთ ოპერატორები: $U=I-2|y_0\rangle\langle y_0|$, $V=I-2|\xi\rangle\langle\xi|$, სადაც $|\xi\rangle=\frac{1}{\sqrt{N}}\sum y|y\rangle$. ოპერატორი არის ქვანტური „მონაცემთა ბაზა“. V ოპერატორი შეიძლება დავაპროექსიროთ ბაზისურთან. მაშინ $(VU)^s|\xi\rangle$, როცა $s\approx\frac{\pi}{4}\sqrt{N}$ იქნება y_0 ვექტორთან ახლოს, ანუ ე.ი. სისტემა მაღალი ალბათობით იქნება $|y_0\rangle$ მდგომარეობაში.

განმარტება: ოპერატორი VU შემოზღუდულია რაღაც ψ კუთხეზე. ამასთან $\langle\xi|y_0\rangle=\frac{1}{\sqrt{N}}\sin\frac{\psi}{2}$, ანუ ეს კუთხე პატარაა. ანუ ე.ი. დიდი N -ის დროს $\psi\approx\frac{2}{\sqrt{N}}$, ანუ $s\approx\frac{\pi}{4}\sqrt{N}$ იტერაციისას ვექტორი შემოზღუდულია დაახლოებით $\frac{\pi}{2}$ -ზე.

მაგალითი $N=4$ -თვის:

ამ შემთხვევაში ჩვენ გვსაჭიროება $n=2$ ქუბიტი და რომელიმე ერთიანი 1 ქუბიტით. გვსაჭიროება $k=\text{round}(\frac{\pi}{4}\sqrt{N})=\text{round}(\frac{\pi}{2})=1$ ორაკულის შეკითხვა, რომ გადავწყვიტოთ ძებნის პრობლემა.

საწყისი მდგომარეობა არის $|\Psi_0\rangle=|00\rangle$ და შემდეგ ვიყენებთ ჰადამარის გეითებს:

$$|\Psi\rangle = H^{\otimes 2}|00\rangle = (H|0\rangle)^{\otimes 2} = \left[\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right]^{\otimes 2} = \left[\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right]^{\otimes 2} = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

$$|\Psi\rangle = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

დავუშვათ, რომ $f(3)=1$ და $f(i)=0$ ყველა $i\neq 3$ -თვის, მაშინ გვექნება შემდეგი მატრიცა:

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

შემდეგ ბიჯზე ვიყენებთ U მატრიცის შემდეგ მდგომარეობას:

$$|\Psi\rangle = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} :$$

$$|\Psi_1\rangle = U|\Psi\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix}.$$

ვნახეთ, რომ $V = 2|\Psi\rangle\langle\Psi| - I$ ოპერატორი ექვივალენტურია ე.წ. „დიფუზიური ოპერატორის“:

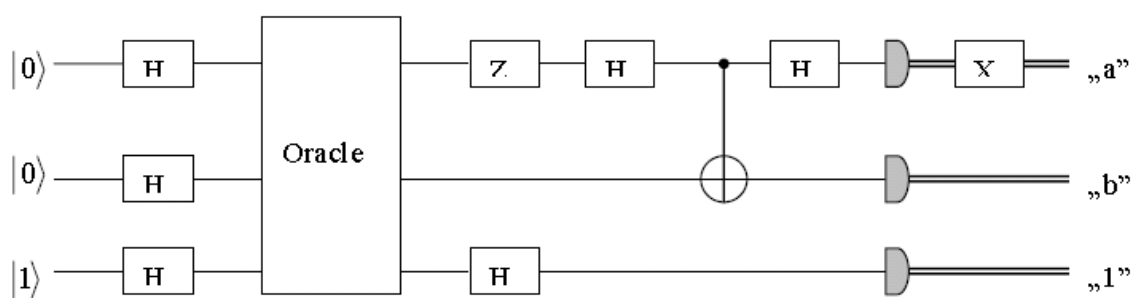
$$D = \begin{cases} \frac{2}{N} - 1 & \text{if } i = j \\ \frac{2}{N} & \text{if } i \neq j \end{cases}$$

ან შემდეგი შემთხვევის:

$$D = \begin{bmatrix} -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \end{bmatrix}$$

$$|\Psi_2\rangle = D|\Psi_1\rangle = \begin{bmatrix} -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \\ -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

ოთხ ელემენტარული გროვერის ალგორითმი გამოვსახოთ დიაგრამაზე:



თავი 6. ქვანტური კონცეპტი

6.1 ქვანტური კონცეპტის გამოკვლევა

ძეზნის სისწრაფის ასამაღლებლად და ძეზნის ეფექტურობის მისაღწევათ შემოვიტანოთ ქვანტური კონცეპტის ცნება. როდესაც ვსაუბრობთ კონცეპტზე იგულისხმება, რომ საქმე გვაქვს ცოდნის ბაზასთან. კონცეპტი არის პირობითი მენტალური სტრუქტურა. კონცეპტს აქვს შემდეგი ასეთი თვისება: რაც უფრო აბსტრაქტულია კონცეპტი, მით უფრო კონკრეტულია და პირიქით. ამ მეთოდოლოგიაზე დიდი ხანია მუშაობენ Google, Microsoft-იც და IBM-იც.

ქვანტური მექანიკის ინტერპრეტაციაში ქვანტური კონცეპტის მდგომარეობა შეიძლება აღწერილი იყოს როგორც ტალღური ფუნქცია. კონცეპტები ხშირად იცვლებიან სხვადასხვა კონტექსტში. აღვნიშნოთ, რომ ქვანტური მექანიკის ფუძემდებელი ნ.ბორი მიუთითებდა ქვანტური მექანიკის მათემატიკური ფორმალიზმის გამოყენების შესაძლებლობას ცოდნის სხვადასხვა სფეროში.

ქვანტური კოგნიტივისტიკა (*quantumcognition*) არის ახალი სფერო ქვანტური მექანიკის, ფსიქოლოგიის, ლინგვისტიკის. ამ სფეროში გამოიყენება ქვანტური თეორიის ფორმალიზმი კოგნიტიური მოვლენების მოდელირებისთვის, რომლებსაც მიეკუთვნებიან ადამიანის მეხსიერება, აზროვნება, კონცეპტები, გადაწყვეტილების მიღება.

კონცეპტების მოდელირების დროს ქვანტური კოგნიტივისტიკა ეყრდნობა რამოდენიმე პრინციპულ მოვლენას:

- ❖ მნიშვნელოვანია კონტექსტუალობის გაგება კონცეპტის ახსნისათვის;
- ❖ ქვანტური არეულობის და ინტერფერენციის გაგება კონცეპტების შესაბამისობისათვის;
- ❖ ქვანტური სუპერპოზიციის გაგება ახალი კონცეპტების აღმოჩენის ახსნისათვის;

მეცნიერების აზრით, ქვანტურ თეორიაში არსებობს ექვივალენტობა ქვანტურ და კოგნიტიურ ობიექტებს შორის. აქედან გამომდინარეობს, რომ ქვანტური მექანიკის თეორია შეიძლება გამოყენებულ იქნას როგორც კოგნიციის ანალიზისთვის, ასევე კოგნიტიური ობიექტების აღწერისთვის.

კოგნიტიური ობიექტი ხასიათდება შემდეგი თვისებებით:

- გვაქვს პოტენცილობის მდგომარეობა;

- გვაქვს აქტუალიზაციის მდგომარეობა;
- გვაქვს კონტექსტის ზემოქმედება;

მეცნიერი ვ.გეიზენბერგი წერს, რომ სიტყვა „მდგომარეობა“ ნიშნავს უფრო „შესაძლებლობას“ ვიდრე „სინამდვილეს“.

6.2 კონცეპტის ფორმირება

ინფორმაციულ ძეგნაში კლასიკურ მეთოდებთან ერთად წარმატებით იყენებენ ქვანტურ მეთოდებს. განვიხილოთ ქვანტური კონცეპტების ფორმირება.

ვთქვათ, გვაქვს $S = \{S_i\}$, $i = \overline{1, n}$ სიმრავლე, რომლის $\{S_i\}$ სიმრავლეები წარმოდგენილია $N_A = \{1, 2, \dots\}$ სახით. N_A - ნიშნების, მახასიათებელი თვისებების სიმრავლე. კონცეპტის ფორმირების პროცესში უნდა შეირჩეს ამ მახასიათებელი ნიშნების სიმრავლე, რომელიც ან შედის ამ კონცეპტში ან არ შედის და თუ a_i არის რომელიმე კონკრეტული თვისება, გვექნება a_i და $\bar{a}_i$. ე.ი. A_i ნიშანი ხასიათდება წყვილით $(a_i, \bar{a}_i)$. მაშასადამე, თითოეული ობიექტს შეიძლება ჰქონდეს m რაოდენობის ნიშანი და n მნიშვნელობათა მაქსიმალური რაოდენობა. ამგვარად გვექნება $(m \times n)$ განზომილების მატრიცა.

კონცეპტის ფორმირების პირველი ეტაპი ეს არის თითოეული ნიშნის მნიშვნელობათა ბინარიზაცია, ანუ მათი გაყოფა ორ ქვესიმრავლედ. მეორე ეტაპზე ხდება ამ ნიშნების საშუალებით იმ კონკრეტული ობიექტების აღწერა, რომელთა საშუალებითაც უნდა გამოვთვალოთ კონცეპტი. შეკრება უნდა იყოს ობიექტური, ანუ ყოველი კონკრეტული ობიექტისათვის გვექონდეს ცალსახა შეფასება. P_{ij} აღნიშნავს A_i ნიშნის a_{ij} მნიშვნელობის შეხვედრის სტატისტიკას იმ N კონკრეტულ ობიექტში, რომელთა საშუალებითაც ვითვლით კონცეპტს.

$$P_{ij} = \frac{N(a_{ij})}{N},$$

$$i = \overline{1, \dots, m};$$

$$j = \overline{1, \dots, n};$$

მაშინ A_i ნიშნისათვის გვექნება $P_i = \sum_k P_{ik}$ და $\bar{P}_i = \sum_i P_{ii}$, a_i და $\bar{a}_i$ ქვესიმრავლეების მიხედვით. იგულისხმება, რომ $P_i + \bar{P}_i = 1$, მაშინ $\varphi(p) = (\frac{p_1, p_2, \dots, p_m}{P_1, P_2, \dots, P_m})$

შემდეგი ეტაპი არის ფილტრაცია. რაც იმას ნიშნავს, რომ დავადგინოთ კონცეპტის გამოთვლის სიზუსტე, ანუ რა სიზუსტით გვჭირდება კონცეპტის აღწერა.

S კონცეპტის სიმრავლეზე შემოვიტანოთ ტრაექტორიის ცნება: $T(L)$ ტრაექტორია ეწოდება რკალურ ობიექტთა $\{S_{ij}\}$ $i=1, \dots, m$; $j=1, \dots, n$; სიმრავლეზე ისეთი L წერტილების სიმრავლეს, რომელთათვისაც A_i ნიშნების თვისებათა ერთეულობა არის რკალზე $\varphi(p)$ ფორმით $+\varepsilon$; $-\varepsilon$ სიზუსტით. $T(L_c)$ ტრაექტორია კი განისაზღვრება როგორც $T(L_c) - \varepsilon \leq T(L_c) \leq T(L_c) + \varepsilon$. (CF)-a არის კონცეპტის კანონიკური ფორმა, რომელიც განსაზღვრულია $T(L_c)$ ტრაექტორიათა სიმრავლეზე და ისინი წარმოადგენენ სიმეტრიულად მსგავს კონცეპტებს, ანუ მათემატიკურად მათი სემანტიკური მსგავსების ზომა მინიმალურია.

A და B ობიექტის სემანტიკური მსგავსების ზომა გამოითვლება შემდეგნაირად:

$\text{Sim}(C(A), C(B)) = \frac{2IC(\text{dis}(C(A), C(B)))}{IC(C(A)) + IC(C(B))}$, სადაც IC არის ინფორმაციული კონცეპტი და გამოითვლება შემდეგნაირად: $IC(C) = -\log P(C)$.

$IC(C) - C$ კონცეპტის ინფორმაციული კონცეპტი და $0 \leq IC(C) \leq 1$ მონოტონურია და ადიციური.

როგორც ზემოთ აღვნიშნეთ თუ კონცეპტს წარმოვადგენთ არა ბინარულად, არამედ ქუბიტების საშუალებით, მაშინ შესაძლებელია შევადაროთ ისინი Born-ის წესის გამოყენებით:

$$P(\Phi, \Psi) = \frac{|\langle \Phi | \Psi \rangle|^2}{\langle \Phi | \Phi \rangle \langle \Psi | \Psi \rangle}$$

$$P(\Phi, \Psi) = \frac{|\langle \Phi | \Psi \rangle|^2}{|\langle \Phi | \Phi \rangle|^2 + ||\langle \Phi \wedge \Psi \rangle||^2}$$

სადაც $\Phi \wedge \Psi$ აღნიშნავს გროსმანის გამრავლებას Φ და Ψ ვექტორებისათვის.

S სიმრავლისათვის $S = \{S_{ij}\}$ სისტემის მდგომარეობის აღსაწერად m და n ნატურალურ რიცხვებს წარმოვადგენთ ვექტორულად:

$$|n\rangle = \begin{bmatrix} n_1 \\ \vdots \\ n_N \end{bmatrix} \text{ და } |m\rangle = \begin{bmatrix} m_1 \\ \vdots \\ m_N \end{bmatrix}$$

სკალარული ნამრავლი ინვარიანტებისათვის გამოითვლება როგორც

$$P(m, n) = \frac{\sum_i m_i n_i}{\sum_i m_i^2 \sum_i n_i^2}$$

დასკვნა

საერთო ჯამში შეგვიძლია ვთქვათ, რომ თანამედროვე ფიზიკურ სამყაროში ქვანტურმა კომპიუტერმა გამოიწვია დიდი ხმაური. ეს არის მისი ძირითადი ღირებულება. დააფიქრა ყველა. ქვანტური კომპიუტერის რეალიზაციამდე ჯერ შეიძლება შორს ვართ, მაგრამ ეს უნდა მოხდეს მარტო მხოლოდ იმიტომ, რომ პრობლემა დგას ბევრი სამეცნიერო მიმართულების გადაკვეთაზე.

დღესდღეობით აქტიურად მიმდინარეობს გამოთვლების ალტერნატიული მეთოდების გამოკვლევა ქვანტური კომპიუტერების საშუალებით, რომლებიც გვამღებენ დიდ შესაძლებლობებს პარალელიზმში. ქვანტური კომპიუტერები ასრულებენ ოპერაციებს ქუბიტების განუსაზღვრელ რიცხვებზე ერთდროულად, რაც ზრდის გამოთვლების სიჩქარეს.

ვფიქრობ, რომ ნაშრომში კარგად წარმოვადგინე ის, რისი გადმოცემაც მინდოდა. ნაშრომში კარგად არის განხილული ქვანტური კომპიუტერის საკითხი და მასში ინფორმაციის დამუშავება და ძებნა. განვიხილე ორი შემდეგი მიმართულება:

1. ბაზებში ძებნა გროვერის ალგორითმის საშუალებით. და შედეგი არის პარალელიზმით გაუმჯობესება;
2. ცოდნის ბაზებში ქვანტური კონცეპტებით ძებნა;

ნაშრომში მოყვანილი მაქვს მაგალითები, რომლებიც კარგად ასახავენ ბაზებში ძებნას.

გამოყენებული ლიტერატურა:

- Shor P.W. Fault-Tolerant Quantum Computation. - LANL e-print quant-ph/9005011, <http://xxx.lanl.gov>.
- Bennett C.H., Bernstein E., Brassard G., Vazirany U. Strengths and Weaknesses of Quantum Computing. - LANL e-print quant-ph/9701001, <http://xxx.lanl.gov>, to appear in SIAM J. On Computing.
- Feynman R. Int. J. Theor. Phys. 21
- Feynman R. Quantum mechanical computers.
- Grover L. A fast quantum mechanical algorithm for database search. //Proceedings of the 28th Annual ACM Symposium on Theory of Computing
- Database Manipulation on Quantum Computers Ahmed Younes (2008)
- Elementary Quantum Gate Realizations for Multiple-Control Toffoli Gates D. Michael Miller, Robert Wille and Z. Sasanian D. Michael Miller¹, Robert Wille² and Z. Sasanian¹
- L.K.Grover, Quantum Mechanics Help in Searching for a Needle in a Haystack, Phys. Rev. Letter 79,325-328,1997.
- A fast quantum mechanical algorithm for database search Lov K. Grover
- www.ibmh.msk.su
- www.qc.ipt.ac.ru
- M.A. Nielsen and I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge (2000).
- G. Brassard, P. Høyer, and A. Tapp, Quantum Counting, quant-ph/9805082
- Grover, Lov K., A framework for fast quantum mechanical algorithms, quant-ph/9711043.
- Grover, L., Quantum mechanics helps in searching for a needle in a haystack (quant-ph/9605043)
- Jozsa, Richard, Searching in Grover's Algorithm, quant-ph/9901021
- P. G. Kwiat, J. R. Mitchell, P. D. D. Schwindt, and A. G. White, Grover's search algorithm: An optical approach, quant-ph/9905086
- Квантовые алгоритмы: возможности и ограничения. М.Вялый (Санкт-Петербург, 2011)