გ. გიორგაძე, ზ. მელიქიშვილი

კვანტური გამოთვლები

გ.გიორგაძე, ზ.მელიქიშვილი

კვანტური გამოთვლები

დანართებით

რ.ფეინმანი. კვანტურ-მექანიკური კომპიუტერი

დ.დოიჩი. კვანტური თეორია, ჩიორჩ-ტიურინგის პრინციპი და უნივერსალური კვანტური კომპიუტერი

წიგნი დაიბეჭდა კიბერნეტიკის ინსტიტუტის სამეცნიერო საბჭოს გადაწყვეტილებით და საქართველოს ეროვნული სამეცნიერო ფონდის გრანტის GNSF/ST07/3-174 ნაწილობრივი ფინანსური მხარდაჭერით.

თბილისი, 2009

UDC(უაკ)530145+519.6+004.78
გ–511

გ.გიორგაძე, ზ.მელიქიშვილი. კვანტური გამოთვლები. თბილისი, კიბერნეტიკის ინსტიტუტი, 2009. წიგნში გამოთვლების კვანტური თეორია განხილულია როგორც რთული ამოცანების ამოსახსნელი ეფექტური მოდელი. მოყვანილია გამოთვლითი პროცესის კლასიკური და კვანტური აღწერა, რისთვისაც განვითარებულია შესაბამისი მათემატიკური და ფიზიკური აპარატი. აგებულია კვანტური გამომთვლელის მოდელი და მითითებულია მის ერთ-ერთ შესაძლო ფიზიკურ რეალიზაციაზე.

კვანტური გამოთვლებით დაინტერესებული მკითხველთათვის წიგნი გამოდგება როგორც შესავალი მეცნიერების ამ ახალ დარგში.

ISBN 978-9941-0-2110-7

შინაარსი

დანართები

წინასიტყვაობა

წიგნში საუბრის თქმაა არა რეალური ტექნიკა, არამედ არაჩვეულებრივი გამოთვლითი პროცესი. საბუნებისმეტყველო მეცნიერებებში თითებზე ჩამოსათვლელია თუნდაც ერთი თქმები და ცნობა მათი აღმოჩენის შესახებ დიდხანს ტრიალებს ხოლმე მხოლოდ აკადემიურ წრეებში, ბიტერ შორის შედგი, დისკრეტული ლოგარითმის კვანტური ალგორითმის პოლითნომიალური სირთულის შესახებ, გამოქვეყნებისთანავე საყოველთაო ინტერესის საგანი გახდა, რადგან დებულებიდან გამომდინარეობს, რომ კვანტურ კომპიუტერზე რეალიზებადია ისეთი ალგორითმი, რომელიც გაშიფრავს ნებისმიერ კრიპტოსისტემას.

კვანტური გამოთვლების იდეა რიჩარდ ფეინმანისაგან მოდის. მის ნაშრომში (1982) გამოთქმული იდეების საკრძნობი გადრმავება მოხდა დეიდ დოიჩის (1985) მიერ. 1994 წელს ბიტერ შორმა გამოაქვეყნა თავისი ცნობილი ნაშრომი, რასაც ნამდვილი ბუმი მოჰყვა. კომპიუტერული მეცნიერების, მათემატიკის და კვანტური ფიზიკის მიჯნაზე დაიბადა მეცნიერების ახალი, სწრაფად განვითარებადი დარგი, რომელიც დღეს თეორიული ინფორმატიკის საფუძვლად ითვლება. მათემატიკოსთა საერთაშორისო კონგრესზე (ბერლინი, 1998) პ. შორს ნაყვანლინას პრემია მიენიჭა. ისტორიულად, ეს მეცნიერული მიმართულების პირველხარისხოვნად აღიარებას ნიშნავს. 2000 წელს კი მათემატიკოსთა ევროპულ კონგრესზე (ბარსელონა, 2000 წლის ივლისი) მუშაობდა ახალი სექცია – "კვანტური გამოთვლები".

უკანასკნელ პერიოდში კვანტურ კომპიუტერს უცხოეთში მრავალი ურნალისტური თუ პბლიცისტური სტატია მიეძღვნა. დაიწერა ბევრი საქციერო თუ პოპულარული წიგნი. კვანტური გამოთვლების საკითხებს ხშირად

განიხილავენ დასაკლეთის სამეცნიერო-პოპულარული არხები შემეცნებით პროგრამებში. იგი ისწავლება წამყვან უნივერსიტეტებში, შეიქმნა მრავალი ცენტრი და სამეცნიერო ჯგუფი, რომელთა არსებობაც კი პრესტიჟულად ითვლება უნივერსიტეტებში, აკადემიურ ინსტიტუტსა და მოწინავე ტექნოლოგიებთან დაკავშირებულ კორპორაციებში.

წიგნს საფუძვლად დაედო თბილისის სახელმწიფო უნივერსიტეტში წაკითხული ლექციათა კურსი "კვანტური გამოთვლები" (სა უნივერსიტეტო არჩევითი კურსი ბაკალავრებისათვის) და კვანტური გამოთვლების თეორიაში სამეცნიერო კვლევითი პროგრამის მასალები, რომლებიც წლების მანძილზე ი-უშაყდებოდა კიბერნეტიკის ინსტიტუტში, ხოლო მოგვიანებით კი—უბნის ბირთვული კვლევების გაერთიანებული ინსტიტუტის საინფორმაციო ტექნოლოგიების laბორატორიასთან ერთად.

რადგან ქერ კიდევ არ არსებობს კვანტური გამოთვლების საყოველთაოდ აღიარებული შეყობრი თეორია, ჩვენ მაქსიმალურად ვცდილობდით მასალა გადმოგვეცა კორექტულად და მსჯელობა ფოთლიფო ქაცრი. აბსტრაქტული მათემატიკური პრობლემები ჩვენთვის წარმოადგენენ ფასეულობათა გარანტს და მას ვიყენებდით ყველგან, სადაც ორაზროვნებას შეიძლება ჰქონოდა ადგილი. თუმცა, ჩვენ არ გამოვრიცხავთ იმის შესაძლებლობას, რომ ზოგიერთი ადგილი უფრო გაშქიერვალე გახდებოდა ან გამარტივებოდა სხვა მოსაზრებებით თუ თეორმალიზმით რომ ვყოსარგებლა. წიგნის სხვადასხვა საკითხების არაერთგვაროვნად გადმოცემა პრობლემათა სიღრმითაა გამოწვეული. გარდა ამისა, ჩვენ კვანტური გამოთვლებით დაინტერესებული ყველა ლონის მკითხველს ვთვალისწინებდით. ჩვენი გაგებით წიგნი არის მხოლოდ "საწყისი პირველი

შეხვდით" და არა მონოგრაფია, ამიტომ ციტირებებისაგან, თუ ისინი აუცილებელი არ იყო, ჩვენ თავს ვიკავებდით. ყველა საჭირო ციტირება წყაროების შესახებ მკითხველს შეუძლია ნახოს "Journal of Mathematical Sciences",vol.153,N 2,2008; Springer Verlag, N.Y.-ის საერთაშორისო კრებში, რომელიც კვანტურ გამოთვლებს ეძღვნება და რომელშიც გარკვეულწილად შეჯამებულია კვანტური გამოთვლების "მათემატიკური ნაწილი" და აგტორების მოკრძალებული წვლილი ამ თეორიაში.

წიგნის ბოლო თავებია რ.ფეინმანისა და დ.დოიჩის სტატიები, რომლებიც საძირთლიანად ითვლებიან ერთ–ერთ პიონერულ ნაშრომებად კვანტური გამოთვლების თეორიაში. პროფ. დოიჩი სიამოვნებით დათანხმა აგტორების თხოვნას მისი სტატია წიგნის დანართი ყოფილიყო, რისთვისაც მას გულწრფელ მადლობას ვუხდით.

ამ ათი წლის წინათ, როდესაც კიბერნეტიკის ინსტიტუტში დაიწყო მუშაობა ექსპერიმენტული კვანტური გამოთვლების საფუძვლების გაგების მიზნით, მაშინ მის მუშაობაში სხვადასხვა სახით მონაწილეობდნენ ქართული საერთაშორისო გადაღებისათვის საყოველთაოდ ცნობილი თეზიკოსები, პროფესორები გიგი ცინცაძე, ჯუმბერ სანიკიძე, შერმაზან ყაყიჩაშვილი; ქვეყანის ექსპერტთა დონორი, პროფესორი მიხეილ ახალაია; აკადემიკოს გურამ ხარაგიშვილისათვის ჩვენი საქმიანობა კვანტური გამოთვლების თეორიაში მუდმივ ყურადღების საგანი იყო. კვანტური გამოთვლების მათემატიკური თრთხილი და მაღალკვალიფიციური ანალიზი, ჩვენი აზრით, გაეთვალისწინეთ.

ამ წიგნით პატივი გვინდა მიეგოთ მათ ხსოვნას!

გია გიორგაძე, ზაზა მერკიშვილი
თბილისი, 2009 წელი

შესავალი

მე-19 და მე-20 საუკუნეების მიჯნაზე, 1900 წლის აგვისტოში, გერმანელმა მათემატიკოსმა დავიდ ჰილბერტმა პარიზში, მათემატიკოსთა II მსოფლიო კონგრესზე გააკეთა ისტორიული მოხსენება. კერძოდ, მან ჩამოაყალიბა 23 ამოცანა, რომელთა ამოხსნა მან ვერ შეძლო, მაგრამ მიიჩნევდა, რომ თითოეული მათგანის ამოხსნას უდიდესი მნიშვნელობა ექნებოდა არა მარტო მათემატიკის, საერთოდ საბუნებისმეტყველო მეცნიერების შემდგომი განვითარებისათვის. ამჟამად, ჰილბერტის ჩამოყალიბებული ამოცანები ცნობილია ჰილბერტის პრობლემების სახელწოდებით და ზოგიერთი მათგანი ბოლომდე დღემდე ამოხსნილი არ არის. ჰილბერტის პრობლემათაგან რიგით 23-ე ყალიბდება შემდეგნაირად: არსებობს თუ არა მექანიკური პროცედურა, რომლის შესრულებასაც ნაბიჯ-ნაბიჯ მოახერხებს ნებისმიერი ადამიანი ან მოწყობილობა, და რომელიც გიპასუხებს ნებისმიერი მათემატიკური დებულების შესახებ, მართებულია ეს ჭეშმარიტია თუ მცდარი. ჰილბერტის ეს პრობლემა მე-20 საუკუნის 30-იან წლებში ამოხსნეს ერთმანეთისაგან დამოუკიდებლად ორმა მეცნიერმა, ერთი იყო ავსტრიელი მათემატიკოსი და ლოგიკოსი კურტ გიოდელი, ხოლო მეორე კი ინგლისელი მათემატიკოსი ალან ტიურინგი. ამ უკანასკნელმა ამოცანის ამოსახსნელად ,,ააგო'' წარმოსახვითი მოწყობილობა, რომელსაც ამჟამად ტიურინგის მანქანა ეწოდება და იგი ითვლება თანამედროვე კომპიუტერის თეორიულ მოდელად. ტიურინგის მანქანა და მასზე დაფუძნებული გამოთვლების თეორია არის გამოთვლითი მათემატიკისა და ინფორმატიკის საფუძველი. ჩიორჩის თეზისი კი მდგომარეობს იმაში, რომ ნებისმიერი ალგორითმული პროცედურა შესაძლებელია განხორციელებული იქნას ტიურინგის მანქანაზე.

ციფრული ტექნოლოგიები საწყისს გასული საუკუნის 50-იანი წლებიდან იღებენ, მას შემდეგ რაც გამოგონილი იქნა ტრანზისტორი. ტრანზისტორის გამოგონებამ გზა გაუხსნა ელექტრონული მოწყობილებების მინიატურიზაციას და ასევე, საგრძნობლად შეამცირა ინფორმაციის დამმუშავებელი სისტემების შექმნაზე გაწეული ენერგეტიკული და მატერიალ-ლური ხარჯები. ამავე პერიოდში, ამერიკელმა ინჟინერმა და მათემატიკოსმა, კლოდ შენონმა გამოაქვეყნა ფუნდამენტური ნაშრომი მონაცემთა ციფრული წარმოდგენის და ციფრული გადამუშავების შესახებ. კლასიკური ინფორმაციის თეორიის ძლიერი და ასევე სუსტი მხარე გახდა მონაცემთა გადაცემის ბუნების აბსტრაგირება. ასეთ თეორიას აინტერესებს მხოლოდ ორი ასპექტი– ინფორმაციის გადაცემის რაოდენობა და გადაცემის ხარისხი. ხსენებულ მახასიათებლებს თან სდევს შემდეგი სახის უკუკავშირი: რაც უფრო ზუსტადაა საჭირო შეტყობინების გადაცემა შემაფერხებელ გარემოში, მით უფრო

შენელებული იქნება მისი გადაცემა. ინფორმაციის თეორიაში განსაკუთრებული ყურადღება ენიჭება ისეთ ოპტიმალურ მახასიათებელს, როგორიცაა არხის გამტარუნარიანობა, ანუ გადაცემის მაქსიმალური სიჩქარე კოდირების და დეკოდირების დროს, რომელიც უზრუნველყოფს ხმაურით გამოწვეულ შეცდომების გასწორებას.

დაჯდა ბოლცმანი
1862-1943

გენიალური გერმანელი მათემატიკოსი, რომელიც თანაბარი სიმრავით ფლობდა მათემატიკის ყველა დარგს. ითვლებოდა თავისი დროის ყველაზე დიდ ფიგურად მეცნიერებაში. გენიოსის უნიკალურსიტყვიერი მისი იქ მოღვაწეობის პერიოდში მსოფლიო მათემატიკურ კონტრად იქცა. არამარტო ეროვნული, არამედ ამერიკელ მეცნიერთა დიდი უმრავლესობა თავს ვალდებულად თვლიდა მოხსენებით წარმდგარიყო ბოლცმანის სემინარზე გენიოსში. გერმანიაში ხელისუფლებაში ნაცისტების მოსვლის შემდეგ (1930 წ.) ბოლცმანი აქტიური საუნივერსიტეტო ცხოვრებას ჩამოშორდა, მასთან ერთად დიდება ჩამოშორდა გენიოსის უნივერსიტეტს. ფაშისტური გერმანიის თხუთმეტწლიანმა ბოლიტიკურმა, ეკონომიკურმა და სამხედრო ძლიერებამ ვერ იხსნა გენიოსი. ატეხილობა დაარგა გერმანულმა ერამ, როცორც საქციერო ერამ. ბოლცმანის საფლავის ქვას, გენიოსში, მისივე სიტყვები აწერია: "ჩვენ უნდა ვიცოდეთ, ჩვენ გვეცოდინება"

როლფ ლანდაუერი, რომელიც დიდი ხნის მანძილზე მუშაობდა კომპანია IBM-ში და მოღვაწეობდა ინფორმაციის ფიზიკური თეორიის დარგში, ამტკიცებდა, რომ ინფორმაცია ფიზიკურია. ინფორმაციის ფუნდამენტური გადამტანია ელექტრომაგნიტური ველი, მაგალითად, ხილული სინათლე, ან რადიოტალღები. ჩვეულებრივ პირობებში, სიგნალის გადაცემის დროს შეფერხებები გამოწვეულია ველის კვანტების (ფოტონების) ქაოსური ქცევით, რომელსაც ახასიათებს სითბური ბუნება. როგორც ირკვევა, ტემპერატურის შემცირება აბსოლუტურ ნულამდე არ იძლევა ხმაურის სრულ გაქრობას. რჩება გამოსხივების კვანტური ბუნებით გამოწვეული, ე.წ. ვაკუუმური ფლუქტუაციები. მე-20 საუკუნის 50-იან წლებში მეცნიერებმა დაიწყეს ფიქრი კვანტურ-მექანიკური ფუნდამენტური სიზუსტეების ფარგლებში ინფორმაციის გადაცემის სიჩქარეზე. ინფორმაციული ტექნოლოგიების შემდგომი განვითარება, კვანტური ოპტიკის, ელექტრონიკის და მოლეკულური ქიმიის მიღწევები იმაზე

მეტყველებენ, რომ უახლოეს მომავალში ასეთი შეზღუდვები გახდება მთავარი ბარიერი არსებული ტექნოლოგიების შემდგომი განვითარების გზაზე.

ალან ტიურინგი
1912-1954

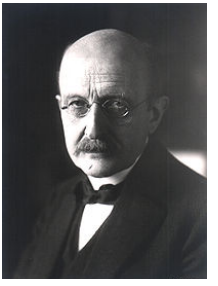
ტექნიკური ინტელექტი მატემატიკოსი და ლოგიკოსი, ინფორმატიკის ფუძემდებელი. "მე არ დავიწუებ იმის მტკიცებას, რომ იმი ტიურინგის საშუალებით მოიგეთ, მაგრამ მის გარეშე იგი შეიძლება წაგუგეო". ასე დაახასიათა ტიურინგის როლი, როგორც კრიპტოლოგისა მეორე მსოფლიო ომის დროს მისმა კოლეგამ. 42 წლის ალან ტიურინგმა ცხოვრებით გაურკვეველი ჯაშუშის ჩაკეტით მიიკლა თავი. ლეგენდაა თუ სინამდვილე ჩვენ არ ვიცით, მაგრამ კომპიუტერული კომპანია Apple-ს ლოგო, ჩაკბეჩილი ჯაშუში, სიმბოლოა ალბათ იმისა, რომ გუახსოვდეს ალან ტიურინგი, პიროველი პიროველთა შორის.

კვანტური კომპიუტერი არის ჰიპოთეტური გამომთვლელი მოწყობილობა, რომელიც გამოიყენებს სფეციფიკურ კვანტურ ეფექტებს და ბევრად მძლავრია კლასიკურ გამომთვლელ მოწყობილობასთან შედარებით. მისი მეხსიერება (კვანტური რეგისტრი) შედგება მრავალი ელემენტარული უჯრედებისაგან –ქუბიტებისგან, რომლებიც იმყოფებიან იზოლირებულ მდგომარეობაში, ხოლო ოპერაციები არიან მართვადი კვანტურ-მექანიკური ურთიერთქმედებები მათ შორის. გამოთვლების პროცესში მონაცემები წარმოადგენენ კვანტურ ინფორმაციას, რომელიც პროცესის დასრულებისას გარდაიქმნება კლასიკურად კვანტური რეგისტრის საბოლოო მდგომარეობის გაზომვით. უპირატესობა კვანტურ ალგორითმებში მიიღწევა კვანტური პარალელიზმითა და გადახლართული მდგომარეობების არსებობით.

თანამედროვე გამომთვლელი ტექნიკის ელემენტები სულ რაღაც 2-3 რიგით აღემატებიან ატომურ ზომებს. მეცნიერები თვლიან, რომ ამ სხვაობის გადალახვას დაჭირდება 10-15 წელი. კვანტური კომპიუტერის აგების ძირითადი ტექნიკური დაბრკოლებაა დეკოჰერენტიზაციის მოვლენა–კვანტური სუპერპოზიციების დაშლა, რომელიც მიკრო სისტემების მაკრო სისტემებზე გავლენის შედეგად ხდება. თუ დეკოჰერენტიზაციის სიჩქარე არ აღემატება რაღაც ზღვრულ მნიშვნელობას, მაშინ კვანტური კოდების გამოყენება შეცდომების გასწორებისათვის, თეორიულად იძლევა იმის საშუალებას, რომ კვანტური სისტემა გახდეს სტაბილური. ამასთან კვანტური რეგისტრის ზომები უნდა

გაიზარდოს რამდენიმე რიგით. ამჟამად მიმდინარეობს მეთოდების ინტენსიური ძიება ამ პრობლემების გადასაჭრელად.

ქუბიტი. კლასიკურ კომპიუტერში ბიტებზე სრულდება არითმეტიკული ოპერაციები. კვანტური კომპიუტერის ძირითადი ელემენტია კვანტური ბიტი ანუ ქუბიტი *(Quantum Bit)*. ბიტი არის კლასიკური სისტემა, რომელსაც ორი საბაზისო მდგომარეობა აქვს. შეიძლება ითქვას, რომ ბიტის მდგომარეობის სივრცე არის ორ ელემენტიანი სიმრავლე, მაგ. $\{0,1\}$. ქუბიტი კი კვანტური სისტემაა ორი საბაზისო მდგომარეობით. ამგვარი კვანტური სისტემები ბევრია. ერთ-ერთი მაგალითია ელექტრონი, რომლის სპინი ღებულობს ორ მნიშვნელობას $\frac{1}{2}$ და $-\frac{1}{2}$. რადგან სისტემა კვანტურია, ამიტომ მისი მდგომარეობის სივრცე, კლასიკურთან შედარებით, გაცილებით უფრო მდიდარია. მათემატიკურად ეს ასე შეიძლება ითქვას: ქუბიტი არის ორ განზომილებიანი კომპლექსური სივრცე. ამრიგად, 0-ისა და 1-ის მაგივრად ქუბიტი არის კომპლექსურ რიცხვთა წყვილი. კვანტური კომპიუტერი არის სისტემა, რომელშიც გამოთვლები ხორციელდება კვანტური მექანიკის კანონებით. ოპერაციები ამ სისტემებში, ისევე როგორც კვანტურ სისტემებში, ესაა სისტემის მდგომარეობათა სივრცის უნიტარული გარდაქმნები.



მაქს პლანკი
1858-1947
აკრძანგლია ფიზიკოსი,
კვანტური ფიზიკის ფუძემდებელი.
ნობელის პრემიის ლაურიატი (1918)

კვანტურ მექანიკაში სისტემის მდგომარეობის აღწერის ერთ-ერთი საშუალებაა ტალღური ფუნქცია, რომელიც უსასრულოგანზომილებიანი სივრცის ელემენტია. ფაზური სივრცე სასრულგანზომილებიანი ხდება მაშინ, როდესაც არსებითია არა თავისუფლების უწყვეტი ხარისხი, არამედ დისკრეტული, მაგალითად, სპინი. ვთქვათ, სისტემის მდგომარეობათა სივრცე 2-განზომილებიანია. ავირჩიოთ ორი საბაზისო მდგომარეობა $|1/2\rangle,|-1/2\rangle$. პირობითად შეგვიძლია ვთქვათ "სპინი მარჯვნივ" და "სპინი მარცხნივ". სუპერპოზიციის პრინციპის თანახმად არსებობს მდგომარეობა $c_1|1/2\rangle+c_2|-1/2\rangle$. ამ შემთხვევაში სისტემის მდგომარეობა განისაზღვრება კომპლექსურ რიცხვთა c_1, c_2 წყვილით. კვანტური გამოთვლების თვალსაზრისით ეს ორი საბაზისო ვექტორი– $|1/2\rangle,|-1/2\rangle$ კლასიკური გამოთვლების ნულის და ერთის ანალოგიურია.

კვანტური კომპიუტერი. კვანტური კომპიუტერი, კლასიკურის მსგავსად, *0*-ზე და *1*-ზე "მუშაობს", მაგრამ მისი ფუნქციონალური ელემენტები თვით კვანტური სისტემის ფაზურ სივრცეზე მოქმედებს ამ სივრცის უნიტარული გარდაქმნების საშუალებით.

ამრიგად, გვაქვს კომპიუტერი ნიშნავს, რომ 1) გვაქვს "კვანტური ელემენტები" – ქუბიტები. ყველა ქუბიტი "ცხოვრობს" ორგანზომილებიან კომპლექსურ სივრცეში; 2) გვაქვს რაღაც მოწყობილობა, რომელიც კვანტური სისტემის მდგომარეობების სივრცეზე (ე.ი. ორგანზომილებიანი კომპლექსური სივრცის ტენზორულ ნამრავლზე, სადაც თანამამრავლთა რაოდენობა ქუბიტების რაოდენობის ტოლია) მოქმედებს უნიტარული გარდაქმნების საშუალებით. აქვე შევნიშნოთ, რომ ეს უნიტარული გარდაქმნები უნდა წარმოქმნიდნენ გამოთვლებისათვის საჭირო ყველა უნიტარულ გარდაქმნას.

კლასიკურ კომპიუტერში ყველა საჭირო ოპერაციის შესასრულებლად ხელსაყრელია ავირჩიოთ რამდენიმე ფუნქცია (ბაზისი), რომელთა კომპოზიცია მოგვცემს ყველა სხვა ოპერაციას. ამ ხელსაყრელ ოპერაციებს აქვთ თავიანთი სახელწოდებები: კონიუნქცია, დიზიუნქცია და უარყოფა (სახელწოდებები მოდის კლასიკური ლოგიკიდან).

ანალოგიურადაა საქმე კვანტურ კომპიუტერში. არსებობს ოპერაციათა ბაზისი და მათი საშუალებით მიიღება გამოთვლებისათვის საჭირო ყველა გარდაქმნა.

ორობითი რიცხვის წარმოდგენა და ოპერაციები კვანტურ კომპიუტერში. კვანტური კომპიუტერის მდგომარეობების სივრცე ქუბიტების ტენზორული ნამრავლია. თუ ყოველ ქუბიტში ბაზისი ფიქსირებულია (იგი ორი ვექტორისაგან შედგება), მაშინ ფაზური სივრცე არის კომპლექსური წრფივი სივრცე, რომლის ბაზისი გადანომრილია 0-ებისა და 1-ებისაგან შედგენილი სიტყვებით. შესავალზე ორობითი სიტყვა განსაზღვრავს ვექტორს ბაზისიდან. მაგალითისათვის განვიხილოთ ერთი ელემენტარული ქვესისტემის–ქუბიტის ბაზისი e_0 და e_1; ავიღოთ ორი ქუბიტისაგან შემდგარი მეხსიერება–ეს არის კვანტური სისტემა, რომლის ფაზური სივრცეა

ერვინ შრედინგერი
1887-1961
ნობელის პრემიის ლაურეატი (1933)

$\mathbf{C^2 \otimes C^2}$, ხოლო ბაზისი კი არის– $e_0 \otimes e_0$, $e_0 \otimes e_1$, $e_1 \otimes e_0$ და $e_1 \otimes e_1$. სისტემის შესასვლელზე არის რიცხვი 3 (ორობით კოდში 11) ნიშნავს, რომ მოვამზადეთ ორი ნაწილაკისაგან შედგენილი სისტემა, რომლის მდგომარეობაა $e_1 \otimes e_1$ ("ორივე სპინი მარცხნივ"), რიცხვი 2 (ორობით კოდში 10) ჩაიწერება მდგომარეობით $e_1 \otimes e_0$ ("პირველი სპინი მარცხნივ, მეორე მარჯვნივ") და ა.შ.

ამრიგად, შესავალი ესაა ორობითი სიტყვების წრფივი კომბინაცია, ალგორითმი კი არის ფიქსირებული უნიტარული ოპერატორების მიმდევრობა. ვიმოქმედებთ რა ამ ოპერატორებით შესავალზე, მივიღებთ გარკვეულ ვექტორს გამოსავალზე. ამის შემდეგ ვაწარმოებთ გაზომვას. გაზომვის შედეგი საზოგადოდ არ არის ცალსახა (ეს არის ექსპერიმენტული ფაქტი და ალბათური აღწერა შედეგია არა არასრული ინფორმაციისა, არამედ ასეთია კვანტური სისტემის ბუნება). კვანტური მექანიკა იძლევა პასუხს მხოლოდ იმაზე, თუ რა ალბათობით მივიღებთ რაიმე კონკრეტულ შედეგს. ამრიგად, თუ ჩვენ საქმე გვაქვს კვანტურ სისტემასთან, რომელსაც სპინი გააჩნია და გაზომვის საშუალებით "შევხედავთ" მას, "დავინახავთ" ორი შესაძლო მდგომარეობიდან ერთ-ერთს: "სპინი ან მარცხნივაა, ან მარჯვნივ", თითოეული მდგომარეობის დამზერის ალბათობა კი–ბაზისის საშუალებით ვექტორის წარმოდგენაში შესაბამისი კოეფიციენტის მოდულის კვადრატის ტოლია. კვანტური მექანიკის პრინციპის თანახმად, გაზომვის შედეგი ალბათურია და ალბათობის გამოთვლა შესაძლებელია.

ჰოლ დირაკი
1902-1984
ინგლისელი
თეზისტი, ნობელის
პრემიის ლაურეატი
(1933)

გამოთვლების წარმოება კვანტური კომპიუტერის საშუალებით. ზოგადად გამოთვლის ამოცანა ასეთია: ვიცით x და უნდა გავიგოთ $y=f(x)$ (x და y ნატურალური რიცხვებია). ვამზადებთ $|x\rangle$ კვანტურ მდგომარებას და მასზე ვმოქმედებთ $U_1U_2...U_m$ ოპერატორით, რომელიც არის m რაოდენობის უნიტარული ოპერატორების ნამრავლი, ე.ი. კვანტურ კომპიუტერის შესავალზეა $|x\rangle$ მდგომარეობა და გამოდის $|\psi\rangle = U_1U_2...U_m|x\rangle$ მდგომარეობა. $|\psi\rangle$ წარმოვადგინოთ საბაზისო ელემენტების წრფივ კომბინაციად

$|\psi\rangle = \sum_{i=0}^{2^n-1} c_i |i\rangle = a|\, y = f(x)\rangle + \sum_{i=0, i\neq f(x)}^{2^n-1} c_i |i\rangle$. გაზომვისას $|y\rangle$ მდგომარეობას დავაფიქსირებთ $|a|^2$ ალბათობით. თუ $|a|^2 > 1-\varepsilon$, სადაც $\varepsilon > 1/2$, მაშინ ცხადია, რომ ცდის მრავალჯერ განმეორებით შეგვიძლია "ცალსახად" გამოვთვალოთ y.

არსებობს ორი არატრივიალური მაგალითი, სადაც კვანტური გამოთვლები აქამდე ცნობილ ყველა გამოთვლით მეთოდებთან შედარებით საგრძნობ უპირატესობას იძლევა.

პირველი მაგალითი: მთელი რიცხვის დაშლის ამოცანა მარტივ თანამამრავლებად.

მეორე მაგალითი: მონაცემთა ბაზაში ჩანაწერის პოვნის ამოცანა.

დისკრეტული ლოგარითმი. დავუშვათ, გვაქვს რომელიმე მარტივი რიცხვის ნაშთთა ველი. მასში არის პირველადი ფესვი - ე.ი. ისეთი ნაშთი, რომლის ხარისხებიც წარმოქმნიან მთელ ველს. თუ მოცემულია ასეთი ფესვი და მოცემულია ხარისხი, მაშინ ამ ფესვის მოცემული ხარისხის პოვნა სირთულეს არ წარმოადგენს. დისკრეტული ლოგარითმის პოვნა–შებრუნებული ამოცანაა. მოცემულია პირველადი ფესვი და ველის რომელიმე ელემენტი. საჭიროა ვიპოვოთ ისეთი ხარისხი, რომელშიც პირველადი ფესვის ახარისხება მოგვცემს ველის ელემენტს.

პიტერ შორი (დაიბ.1959 წ.) მუშაობს მასაჩუსეტსის ტექნოლოგიურ ინსტიტუტში. მიღებული აქვს როლფ ნევანლინას პრემია (1998 წ.)

ეს ამოცანა ითვლება იმდენად რთულად, რომ თანამედროვე კრიპტოგრაფიული სისტემები აგებულია იმ დაშვებით, რომ დისკრეტული ლოგარითმის რაიმე მისაღებ დროში პოვნა, როდესაც მარტივი რიცხვი (მოდული) საკმაოდ დიდია, შეუძლებელია.

შორის თეორემა. დისკრეტული ლოგარითმის გამოსათვლელად არსებობს ეფექტური კვანტური ალგორითმი.

პ.შორის ალგორითმი ემყარება იდეას, რომელიც თავისი არსით კვანტურია. იგი მდგომარეობს შემდეგში: დავუშვათ ვეძებთ რაიმე რიცხვის დისკრეტულ ლოგარითმს. დავაფიქსიროთ ბაზისი ფაზურ სივრცეში. ბაზისიდან ავიღოთ ის ვექტორი, რომლის ნომერიც მოცემული რიცხვის ტოლია.

ალგორითმის თანახმად, მის მიმართ გამოვიყენებთ ფურიეს კვანტურ გარდაქმნას, ხოლო შემდეგ კიდევ რაიმე უნიტარულ ოპერატორებს და ბოლოს მოვახდენთ დაკვირვებას ("გაზომვას"), შედეგში მივიღებთ ვექტორს, რომლის ნომერიც აღმოჩნდება საძიებელი დისკრეტული ლოგარითმი გარკვეული ალბათობით, რომელიც საკმაოდ ახლოსაა 1-თან.

სირთულე. კვანტურ კომპიუტერზე ზემოთ მოყვანილი ალგორითმი კუბური სირთულისაა, რაც უხეშად რომ ვთქვათ, იმას ნიშნავს, რომ ისეთი რიცხვის დისკრეტული ლოგარითმის გამოსათვლელად, რომელიც ბიტითაა წარმოდგენილი საჭიროა დროის გარკვეული ერთეული.

აქვე შევნიშნოთ, რომ დღემდე არაა დამტკიცებული კლასიკური კომპიუტერისთვის დისკრეტული ლოგარითმის გამოსათვლელი ამაზე სწრაფი ალგორითმის არსებობა.

კვანტური მონაცემთა ბაზა. კვანტური ალგორითმი მონაცემთა ბაზაში ჩანაწერის მოსაძებნად ეკუთვნის ლ.გროვერს.

განვიხილოთ მონაცემთა ბაზა, რომელიც 2^N ჩანაწერს შეიცავს. საჭიროა რომელიმე ჩანაწერის პოვნა. გვაქვს შემდეგი დაშვებები: 1) არსებობს გარკვეული პროცედურა, რომელიც შეამოწმებს საჭირო ობიექტი ავირჩიეთ თუ არა; 2) ჩანაწერები დალაგებულნი არ არიან. კითხვა: რა "სიჩქარით" შეგვიძლია ამოვხსნათ მოცემული ამოცანა კლასიკურ კომპიუტერზე? ყველაზე უარესია თუ მოგვიწევს ყველა 2^N ელემენტის გადასინჯვა. ალბათურ კომპიუტერზე საჭიროა 2^{N-1} ჩანაწერის ნახვა. თუ 2^{N-1}-ზე ნაკლებ ჩანაწერს გადავარჩევთ, მაშინ ალბათობა იმისა, რომ ვიპოვით საჭირო ელემენტს, მცირეა. აღმოჩნდა, რომ კვანტურ კომპიუტერზე საჭიროა $2^{N/2}$ ჩანაწერის გადარჩევა.

ამრიგად, თუ შევქმნით მონაცემთა კვანტურ ბაზას, მასში ძიების განხორციელება მარტივია. სხვანაირად, ალბათობა იმისა, რომ ძიება წარმატებით ჩაივლის, საკმაოდ დიდია.

ეს ალგორითმი ეფექტური არ არის, მაშინ როცა დისკრეტული ლოგარითმის ამოცანა ეფექტურად იხსნება. სირთულე კვლავ ექსპონენციალურია, მაგრამ მოგება კოლოსალურია. მაგალითად, თუ N=20 (ე.ი. დაახლოებით მილიონი ჩანაწერი გვაქვს) საკმარისია მონაცემთა ბაზაზე 1024 მიმართვა, მაშინ როდესაც ალბათურ კომპიუტერზე საჭიროა 512 000 მიმართვა. ხოლო თუ N=100 (თუმცა ასეთი მონაცემთა ბაზა ძნელი წარმოსადგენია), ალბათური კომპიუტერის შემთხვევაში საჭიროა 2^{49} მიმართვა, ხოლო კვანტურისათვის კი 0.5×10^{15}. მტკიცდება, რომ თუ ამოცანა დასმულია ზოგადად, ისე როგორც ზემოთ, არ არსებობს ექსპონენციალურზე უფრო ნაკლები სირთულის კლასიკური ალგორითმი.

ჯერჯერობით მხოლოდ ეს ორი ამოცანაა, რომლებისთვისაც კვანტური კომპიუტერი ეფექტურად იმუშავებდა, მაგრამ არსებობს კვანტური კომპიუტერის

გამოყენების ძალზე მნიშვნელოვანი სფერო—კვანტური პროცესის მოდელირება. კვანტური სისტემის ევოლუციური პროცესის მოდელირება კლასიკურ კომპიუტერზე ექსპონენციალური სირთულისაა, ამიტომ მნიშვნელოვანი სიძნელეები ჩნდება. კვანტურ კომპიუტერზე კი შესაძლებელია რეალური კვანტური სისტემების მოდელირება და გამორიცხული არაა, რომ კვანტური კომპიუტერების გამოყენების მნიშვნელოვანი სფერო სწორედ კვანტური სისტემების მოდელირება იქნება.

რ.ფეინმანი და კვანტური კომპიუტერი. რ.ფეინმანმა განიხილა გამოთვლების პროცედურა ფიზიკის თვალსაზრისით.

არსებობს ლოგიკური შეზღუდვები იმაზე, თუ რა შეიძლება გამოითვალოს. შესაძლებელია ისეთი ამოცანის მოფიქრება, რომლისთვისაც ალგორითმი არ არსებობს და შეიძლება ისეთი ამოცანის დასმაც, რომლისთვისაც ალგორითმი ძალიან დიდხანს იმუშავებს. არის თუ არა კომპიუტერის ფუნქციონირების ფიზიკური შეზღუდვები, რომლებიც ალგორითმების რეალიზაციას შეზღუდვებს ადებენ? ფეინმანმა აჩვენა, რომ ფიზიკური შეზღუდვები, თერმოდინამიკის მეორე კანონის ტიპისა, არ არსებობს. ამრიგად, თუ შევამცირებთ ენერგიის დანახარჯს და ხმაურს, შესაძლებელი გახდება რაგინდ გრძელი გამოთვლები ვაწარმოოთ რაგინდ მცირე დანახარჯებით. ფიზიკის ენაზე ეს იმას ნიშნავს, რომ გამოთვლა შებრუნებადი—შექცევადია.

ამრიგად, ფეინმანმა აჩვენა, რომ თუ გვაქვს კვანტური მოწყობილობა, ე.ი. ისეთი, რომელიც კვანტური მექანიკის კანონებს ემორჩილება, მაშინ აუცილებელი არაა მისი გამოთვლითი შესაძლებლობები დაემთხვეს კლასიკური მოწყობილობის გამოთვლით შესაძლებლობებს. ფეინმანმა დასვა თავისი არსით მათემატიკური ამოცანა: გამოთვლების თვალსაზრისით ასეთი მოწყობილობა მოგვცემს თუ არა რაიმე ეფექტს? ფეინმანის პუბლიკაციის შემდეგ გამოქვეყნდა დოიჩის, ბერნშტაინის და ვაზირანის, იაოს შრომები, სადაც განხილული იყო ეს ამოცანა (იხ. [6], [12]).

აქვე უნდა აღინიშნოს, რომ რუსმა მათემატიკოსმა ი. მანინმა თავის წიგნში "გამოთვლადი და არაგამოთვლადი" (მოსკოვი, 1981), აღწერა კვანტური ავტომატი და მიუთითა კლასიკურისაგან კარდინალურ განსხვავებაზე.

პ.შორმა კი პირველმა გამოიყენა კვანტური იდეოლოგია რეალური ალგორითმის ასაგებად.

> რ. ფეინმანის ინტერესი გამომთვლელი მანქანებისადმი საყოველთაოდ ცნობილია. პ.შორის ალგორითმამდე რ. ფეინმანის ნაშრომები, რომლებშიც კვანტური გამომთვლელია განხილული, ჩვენი აზრით "პოპულარული" არ იყო. ფეინმანის იდეის მათემატიკურ მოდელად შეიძლება ჩავთვალოთ ე. წ. შებრუნებადი გამოთვლები, რომელიც

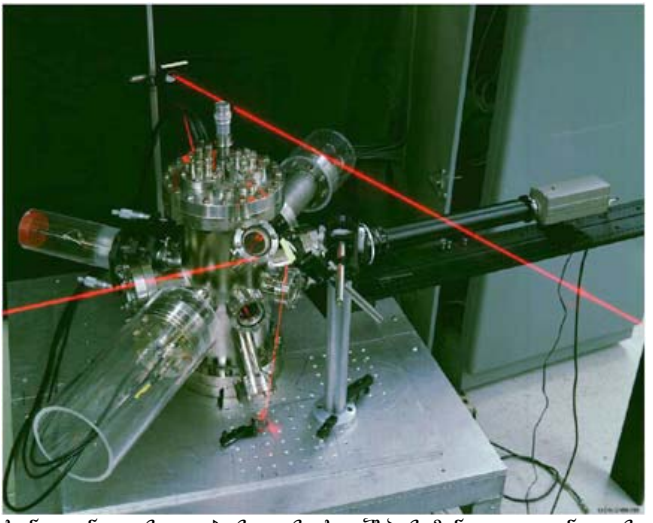
უკვე შესწავლილი იყო. ტონი ჰეი (Tony Hey) თავის სტატიაში "Richard Feynman and compution" (Contemporary Physics, 1999, vol. 40, N 4, pp. 257-265) მიუთითებს, რომ ფეინმანს საუბრები ჰქონდა "გამოთვლითი ტექნიკის ლეგენდარულ პიროვნებებთან" (Feynman . . . discussed the fundamentals of computation witch other legendary figures of the computer sciences and physics community such as Ed Fredkin, Rolf Landauer, Cavver Mead, Marvin Minsky and John Wheeler.) იგი შეხვდა აგრეთვე ჩარლ ბენეტს, შებრუნებადი გამოთვლების ერთ-ერთ ავტორს. ასე, რომ ფეინმანის ნაშრომები შემთხვევითი მოვლენა არ ყოფილა. ჟურნალ "Physics Today", February,1989 სპეციალურ გამოშვებაში, რომელიც ფეინმანს მიეძღვნა, მოთავსებულია სტატია "Richard Feynman and the Connection Machine", რომელშიც ერთი სიტყვაც არ არის ნათქვამი ფეინმანის იმ სტატიებზე, რომლებიც კვანტურ კომპიუტერს ეძღვნება.

კვანტური კომპიუტერის ფიზიკური რეალიზაცია. პ.შორის პუბლიკაციას ფიზიკოსები სკეპტიკურად შეხვდნენ. კვანტური კომპიუტერი ფიზიკურ კანონებს არ ეწინააღმდეგება, რაც თავისთავად მისი რეალიზაციის შესაძლებლობას არ ნიშნავს.

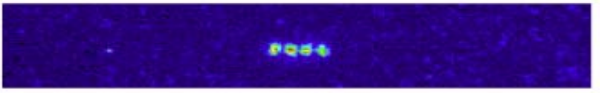
კვანტური კომპიუტერის აგების გზაზე არის სერიოზული პრობლემები. საქმე იმაშია, რომ ნებისმიერი ფიზიკური რეალიზაცია მიახლოებითი იქნება. პირველი: შეუძლებელია ისეთი მოწყობილობის შექმნა, რომელიც ფაზური სივრცის ნებისმიერ ვექტორს მოგვცემს. მეორე სირთულე დაკავშირებულია შემთხვევით შეცდომებთან. კვანტურ სისტემაში საკმარისია ერთი ნაწილაკის შემთხვევითი შერხევა, რომ ყველაფერი შეიცვლება. ამიტომ თავიდანვე დაისვა კითხვა: შესაძლებელია კი კვანტური გამოთვლების ორგანიზება ისეთ საიმედო კვანტურ ელემენტებზე, რომ გამოთვლის შედეგები საიმედო იყოს? კლასიკურ კომპიუტერზე ეს ამოცანა მარტივად იხსნება, მაგალითად დამატებითი ბიტით. არსებობს აგრეთვე სპეციალური მაკორექტირებელი კოდები. ყველაფერი დიდი ხნის წინ იქნა დამუშავებული და საკმაოდ ეფექტურად მუშაობს. ცნობილია, რომ ჯერ კიდევ IBM/360-ში ბაიტი შედგებოდა 9 ბიტისაგან, რომელთაგან მე-9 განკუთვნილი იყო შეცდომების კონტროლისათვის.

კვანტური კომპიუტერის შემთხვევაში ეს პრობლემა გაცილებით ღრმაა. ის ადგილი, სადაც კვანტური გამოთვლების თვისობრივად ახალი შესაძლებლობა ჩნდება, ესაა გადახლართული მდგომარეობა (entangled states). თუ ბიტები არსებობენ თავისთავად რაიმე მდგომარეობაში, მაშინ ეს ალბათური კომპიუტერია. კვანტურ კომპიუტერში გვაქვს შერეული მდგომარეობები "შებმულები" გარკვეული კანონზომიერებით. ამის გამო კვანტურ კომპიუტერში შეუძლებელია უცნობი რომელიმე ბიტის კოპირება. საიმედობის პრობლემა კვანტურ კომპიუტერში ტექნიკურად ძნელად გადასაწყვეტია, თუმცა თეორი-

ულად ნაჩვენებია, რომ გამოთვლები შესაძლებელია ვაწარმოოთ მოცემული სიზუსტით. ეს გაკეთებულია შეცდომების გამასწორებელი კლასიკური კოდების ანალოგიურად.



ლოს ალამოსის ნაციონალური ლაბორატორიის ექსპერიმენტული დანადგარი გაციებული ჩაჭერილი იონების კვანტური სისტემა.



ოთხი კალციუმის იონის მძივი. მძივის სიგრძე 80 μm (მიკრომეტრი)

რაც შეეხება ტექნოლოგიურ მხარეს, არსებობს პუბლიკაციები ქუბიტების შექმნის შესახებ. ქუბიტების რეალიზაციის რამდენიმე ვარიანტია უკვე შემოთავაზებული. მათ შორის ყველაზე უფრო იმედის მომცემია ე.წ. გაციებული ჩაჭერილ იონების (cold ion traps) ბაზაზე აგებული ექსპერიმენტული კომპიუტერი. ეს ტექნოლოგია და მისთვის საჭირო თეორიის საფუძვლები გადმოცემულია მეორე თავში. გარდა ამისა ნაჩვენებია, რომ კვანტური სისტემა–გაციებულ ჩაჭერილ იონებზე მოქმედი ლაზერული გამოსხივება, აკმაყოფილებს ყველა იმ მოთხოვნას (მონაცემები აღებულია დ. დივინჩეცოს პუბლიკაციიდან *Topics in quantum computers*, IBM Research Division. იხ. აგრეთვე [13]), რომელმაც კვანტური კომპიუტერის რეალიზაცია უნდა მოახდინოს. კერძოდ,

1.სისტემა უნდა შედგებოდეს ფიქსირებული რაოდენობის ნაწილაკებისაგან.

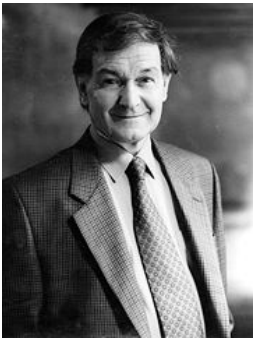
2.შესაძლებელი უნდა იყოს სისტემის მიყვანა ცნობილ (განსაზღვრულ) მდგომარეობამდე.

3.გარე სამყაროსაგან იზოლაციის ხარისხი ძლიერ მაღალი უნდა იყოს.

4.უნდა არსებობდეს სისტემის მდგომარეობის ცვლის ისეთი მექანიზმი ფაზური სივრცის უნიტარული გარდაქმნების მიმდევრობის საშუალებით, რომ სისტემა დარჩეს კოჰერენტულ მდგომარეობაში.

5.უნდა არსებობდეს სისტემის მდგომარეობის გაზომვის საშუალება.

აქვე გავაკეთოთ შენიშვნა, რომელიც ეხება ნეიროქსელებსა და ნეიროკომპიუტერებს: გამოთვლების თვალსაზრისით, ნეიროქსელების ის მოდელები, რომლებიც დღემდე არსებობენ, კლასიკური კომპიუტერისაგან არ განსხვავდებიან. ნეიროკომპიუტერის იმიტირება შესაძლებელია კლასიკურ კომპიუტერზე. უფრო მეტიც, ის ნეიროჩიპები, რომლებიც დღეს იყიდება, ზუსტად ამას აკეთებენ.



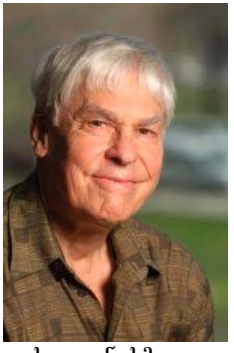
სერ როჯერ პენროუზი
დაიბ.1931 წ.

თანამედროვეობის უდიდესი ინგლისელი მეცნიერი. მატემატიკის კათედრის ხელმძღვანელი ოქსფორდის უნივერსიტეტში. სამეცნიერო გზადაგზა აღსანიშნავია ჯოლფის პრემია (სტიუენ ჰოუკინგთან ერთად), დირაკის მედალი, ალბერტ აინშტაინის პრემია და საქეთო საზოგადოების მედალი. 1994 წელს მეცნიერებაში უდიდესი დამსახურებისათვის ინგლისის დედოფალმა მას სერის ტიტული მიანიჭა.

ამრიგად, გამოთვლების თვალსაზრისით, ნეიროკომპიუტერსა და კვანტურ კომპიუტერს საერთო არაფერი აქვთ. რაც შეეხება მეორე მნიშვნელოვან კითხვას, რომელიც ამ კონტექსტში ჩნდება, ასეთია: "ადამიანის ტვინი ხომ არ არის კვანტური კომპიუტერი?" ხომ შეიძლება, რომ აზროვნება დაკავშირებული იყოს კვანტურ პრობლემებთან? ფიზიკოსთა უმრავლესობას ეს აბსურდად

მიაჩნია. არგუმენტი დაახლოებით ასეთია: ის ეფექტები, რომლებზედაც კვანტური კომპიუტერი უნდა დაფუძნდეს, სპონტანურად ქრება გარე სამყაროსთან ურთიერთშეხების დროს. მათ ჩაკეტილი სისტემა ჭირდებათ. სისტემის ჩაკეტილობა კი მაღალ ტემპერატურაზე წარმოუდგენელია. გაუგებარია, ტვინში ეს სად შეიძლება ხდებოდეს. 60-იან წლებში იყო ჰიპოტეზა იმის შესახებ, რომ ტვინში ადგილი აქვს ზეგამტარებლობას, თუმცა ექსპერიმენტებით ეს ჰიპოთეზა დღემდე არ დამტკიცებულა. აზროვნების ფენომენის აქ მოყვანა რაიმე შორეული ანალოგია კი არ არის, არამედ ჩვენ მხედველობაში გვაქვს როჯერ პენროუზის წიგნი "Shadows of the Mind" (*Oxford University Press, 1994*).

როგორი არასრული და ზერელე ანალიზიც არ უნდა გავაკეთოთ ინფორმატიკის, კომპიუტერული მეცნიერების, კიბერნეტიკის თუ ინფორმაციის თეორიის, ვერაფრით გვერდს ვერ ავუვლით ჰილბერტის პრობლემებს, კერძოდ, მე-10-სა და 23-ეს, რომელთა ამოხსნის მცდელობებმაც კი დასახებული დარგების (და არამარტო მათი) არნახული პროგრესი გამოიწვია. ერთი საუკუნის შემდეგ ს.სმეილს კვლავ მოუწევს ჰილბერტის რამდენიმე პრობლემის ახლა უკვე თვით სმეილის პრობლემების ნუსხაში შეტანა. ვენდოთ სმეილის ალღოს და ინტუიციას მეცნიერებაში (ამის საფუძველს სმეილი ნამდვილად იძლევა), და ჩამოვაყალიბოთ მე-18 პრობლემა ამ სიიდან:



სტივენ სმეილი
დაიბ. 1930 წ.

ამერიკელი მათემატიკოსი. ფილდსის პრემიის ლაურიატი (1966). დაჯილდოებულია აკრეთვე ჯოლფის პრიზით 2007 წელს. კალიფორნიის უნივერსიტეტის (ბერკლი) პროფესორი 1960-1961 და 1964-1995 წლებში. 1995 წლიდან ექერიტუს პროფესორი ბერკლში და ჰონ კონგის უნივერსიტეტის პროფესორი. 1998 წელს ჩამოაყალიბა 21-ე საუკუნის პრობლემები მათემატიკაში, რომელიც სმეილის პრობლემების სახელწოდებითაა ცნობილი.

"როგორია ინტელექტის, როგორც ხელოვნურის, ისე ადამიანურის, საზღვრები?"

უკანასკნელი ოცი წლის მანძილზე საქმის ყველაზე დიდი ცოდნით და ფართო მეცნიერული ხედვით (რაც გვერწმუნეთ არც თუ ისე უმნიშვნელოა!) ეს ამოცანა რ.პენროუზმა განიხილა. სმეილის აზრით, პენროუზის მტკიცებებს მის

მიერ გამოყენებული კვლევის აპარატის შეზღუდულობა აზარალებს და მიღებული დასკვნები ფარდობითია, ანუ სამართლიანია მხოლოდ ცოდნის გარკვეულ (აქსიომათა) საზღვრებში. მისი აზრით, მათემატიკური მოდელირების საყოველთაოდ მიღებულ აპარატს–ნამდვილ რიცხვებს, აპროქსიმაციაციას, ალბათობის თეორიას, თუ გეომეტრიას უნდა დაემატოს ამოცანათა ამოხსნის, თამაშის და სწავლების თეორიები. მოგვიანებით სმეილმა თანაავტორებთან ერთად გამოაქვეყნა სწავლების მათემატიკური თეორია. კვანტური გამოთვლების იდეოლოგიის საზღვრებში გავაგრძელებთ მსჯელობას გამოთვლადისა და გამოუთვლელის შესახებ და მოვიყვანთ ერთ უახლეს შედეგს, რომლის თანახმად ადიაბატური პროცესი არაალგორითმულ ამოცანას ალგორითმიზებულს ხდის (ჰილბერტის მე-10 პრობლემა). ამ დებულებას ჰყავს ოპონენტებიც. ჩვენი აზრით, დებულების მტკიცება კვანტური გამოთვლების თეორიის ფარგლებში წინააღმდეგობას არ შეიცავს და ვფიქრობთ, რომ იგი ღირსია შემდგომი ანალიზის საგანი გახდეს. მაგრამ, ‘‘შემდგომი ანალიზის საგანი’’ არაერთი დებულებაა კვანტურ გამოთვლებში. რეალურად შესაძლებელია თუ არა იმის გაკეთება რაც ბუნების კანონებს არ ეწინააღმდეგება, ცოდნის ამ ეტაპზე ფაქტი არ არის.

თავი I

კვანტური ალგორითმები

1. კლასიკური გამოთვლები და სირთულე

ალგორითმი არის ცალსახად განსაზღვრულ ისეთ ინსტრუქციათა ერთობლიობა, რომლებიც შესავალ მონაცემებზე მოქმედებენ და გვაძლევენ შედეგს, ამასთან ყველა ინსტრუქცია ელემენტარულია, ე.ი. მათი შესრულება ხდება მექანიკურად. ალგორითმის ცნების ფორმალიზება მრავალი გზითაა შესაძლებელი. ერთ-ერთი მათგანი ემყარება ტიურინგის მანქანის ცნებას.

განმარტება. ტიურინგის მანქანა არის ექვსეული $(S,\#,A,Q,q_0,\delta)$, სადაც S,A,Q სასრული სიმრავლეებია, ამასთან $A \subset S$, S-ს ეწოდება *ალფავიტი*, A-ს *გარე ალფავიტი*, ხოლო Q კი არის მმართველი მოწყობილობის მდგომარეობათა სიმრავლე, $\#$ რაიმე გამოყოფილი ელემენტია $S \setminus A$ სიმრავლიდან, რომელსაც ცარიელი სიმბოლო ეწოდება, q_0 მდგომარეობათა Q სიმრავლის ელემენტია და ეწოდება საწყისი მდგომარეობა, ხოლო δ-ს კი *გადასვლის* ფუნქცია:

$$\delta : Q \times S \to Q \times S \times \{-1,0,1\}.$$

ტიურინგის მანქანის მდგომარეობა ცალსახად მოიცემა (σ,p,q) სამეულით, სადაც σ არის S ალფავიტისაგან შედგენილი უსასრულო სიტყვა. σ სიტყვის სიმბოლოები ჩაწერილია ლენტაზე, შესაბამის უჯრაში, რომლის ნომერსაც მიუთითებს s_j სიმბოლოს j-ური ინდექსი. ლენტას აქვს თაურა, რომელიც კითხულობს სიმბოლოს p უჯრიდან. გარდა ამისა, ტიურინგის მანქანას აქვს მმართველი მოწყობილობა, რომლის მდგომარეობა q არის Q სიმრავლის ელემენტი.

ტიურინგის მანქანის მდგომარეობა იცვლება დისკრეტულად. დავუშვათ ტიურინგის მანქანა იმყოფება (σ,p,q) მდგომარეობაში. მუშაობის ერთი ტაქტის დროს მმართველი მოწყობილობა ასრულებს შემდეგ მოქმედებებს.

ა) კითხულობს იმ სიმბოლოს, რომელიც თაურას ქვეშაა. ე.ი. გამოიცნობს s_p სიმბოლოს.

ბ) გამოითვლის გადასვლის ფუნქციას: $\delta(q,s_p)=(q',s,\Delta_p)$ თუ (q,s_p)

წყვილზე გადაცემის ფუნქცია განსაზღვრული არ არის, მაშინ ტიურინგის მანქანა ჩერდება.

გ) p -უჯრაში ჩაწერს s სიმბოლოს, მოხდება თაურას ძვრა Δp -თი და სისტემა (ტიურინგის მანქანა) გადავა სხვა q' მდგომარეობაში. ეს სხვა მდგომარეობა იქნება:

$$\left((s_0,\ldots,s_{p-1},\ldots),p+\Delta_p,q'\right)$$

დ) თუ $p+\Delta_p<0$ მანქანა მუშაობას წყვეტს.

ტიურინგის მანქანა მუშაობას იწყებს $(\alpha\#,\ldots,0,q_0)$ მდგომარეობიდან, სადაც α სასრულ სიტყვას, რომელიც გარე ალფავიტის სიმბოლოებისაგან შედგება, მოსდევს ცარიელი სიმბოლოებისაგან შედგენილი უსასრულო ჯაჭვი.

გარე ალფავიტისაგან შედგენილი სიტყვების სიმრავლე აღინიშნება A^*-ით. $\alpha\in A^*$ სიტყვას აქვს სახე: $\sigma\#,\ldots,$ სადაც σ სიტყვის ბოლო სიმბოლო არ არის ცარიელი, მას, როგორც აღვნიშნეთ, მოსდევს ცარიელი სიმბოლო. σ სიტყვას ეწოდება ლენტის გამოყენებული ნაწილი.

ასრულებს რა თანმიმდევრობით ტიურინგის მანქანა ტაქტებს, ვიღებთ მდგომარეობათა მიმდევრობას:

$$(\sigma_0,0,q_0),(\sigma_1,p_1,q_1),(\sigma_2,p_2,q_2)\ldots,$$

როდესაც ტიურინგის მანქანა გაჩერებულია, ლენტის გამოყენებული ნაწილის ბოლოს წინა ტაქტის რეზულტატი არის შედეგი.

დავაფიქსიროთ რაიმე M ტიურინგის მანქანა და განვიხილოთ φ_M ფუნქცია, რომელიც განსაზღვრულია A^*-ზე ან მის ქვესიმრავლეზე და მნიშვნელობებს ღებულობს A^*-ში. თუ არსებობს ისეთი შესავალი, რომლის დროსაც ტიურინგის მანქანა არ ჩერდება ან შედეგი შეიცავს სიმბოლოს $S\backslash A$-დან, მაშინ φ_M განსაზღვრული არ არის. ყველა სხვა შემთხვევაში ამბობენ, რომ M ტიურინგის მანქანა ახდენს φ_M ფუნქციის გამოთვლას, ან სხვა სიტყვებით, φ_M *გამოთვლადია* M ტიურინგის მანქანაზე.

განმარტება. ნებისმიერ $f:A^*\to A^*$ ფუნქციას ეწოდება *გამოთვლადი*, თუ არსებობს ისეთი M ტიურინგის მანქანა, რომ $\varphi_M=f$.

პრედიკატი ეწოდება ნებისმიერ $\tau:A^*\to\{0,1\}$ ფუნქციას. იმის შესაბამისად, τ ღებულობს 1-ის თუ 0-ის ტოლ მნიშვნელობას, პრედიკატს შესაბამისად ეწოდება ჭეშმარიტი ან მცდარი. სხვა სიტყვებით რომ ვთქვათ, პრედიკატი არის პირობა, რომელსაც უნდა აკმაყოფილებდეს სიტყვა. ამრიგად,

ყველა პრედიკატს შეესაბამება A^*-ს ისეთი ქვესიმრავლეები, რომლის ყოველ ელემენტზე იგი ჭეშმარიტია. ამ ქვესიმრავლეებს ეწოდებათ *ენები*. ყოველ პრედიკატს შეესაბამება *მახასიათებელი ფუნქცია*, რომელიც ერთის ტოლია მხოლოდ იმ სიტყვებზე, რომელთათვისაც პრედიკატი ჭეშმარიტია. τ პრედიკატის მახასიათებელი ფუნქციის აღსანიშნავად ვიხმართ კვლავ τ სიმბოლოს. პრედიკატს ეწოდება *ამოხსნადი*, თუ მისი შესაბამისი მახასიათებელი ფუნქცია გამოთვლადია. ტიურინგის იმ მანქანაზე, რომელიც გამოითვლის პრედიკატის მახასიათებელ ფუნქციას ვიტყვით, რომ ის იძლევა პასუხს კითხვაზე "ჭეშმარიტია თუ არა პრედიკატი α შესავალი სიტყვისათვის".

გამოთვლადი ფუნქციისა და ამოხსნადი პრედიკატის ცნებები შემოვიტანოთ მრავალი ცვლადის შემთხვევაში.

ვთქვათ n ნატურალური რიცხვია, A ალფავიტია, ხოლო M კი ტიურინგის მანქანაა $A \cup \{*\}$ გარე ალფავიტით. განვმარტოთ მრავალი ცვლადის ფუნქცია $\left(A^*\right)^n$-ზე შემდეგნაირად:

$$\varphi_{M,n}(\alpha_1,...,\alpha_n) = y,$$

ტოლობა სრულდება მაშინ, როდესაც M მანქანის მუშაობის შემდეგ შედეგი $\alpha_1 * \alpha_2 * ... * \alpha_n *$ შესავალზე ემთხვევა y-ს. იმ შემთხვევაში, როდესაც მანქანა არ ჩერდება, ან ლენტაზე ჩაიწერება სიმბოლო, რომელიც არ ეკუთვნის A^*-ს, მაშინ ტიურინგის მანქანა ჩერდება.

განმარტება. $f = \left(A^*\right)^n \to A^*$ ფუნქციას ვუწოდოთ *გამოთვლადი*, თუ არსებობს ისეთი M ტიურინგის მანქანა, რომ $\varphi_{M,n} = f$.

მრავალი ცვლადის პრედიკატს ეწოდება *ამოხსნადი*, თუ მისი მახასიათებელი ფუნქცია გამოთვლადია.

გამოთვლების მახასიათებელია ის რესურსები, რომლებსაც გამოთვლა მოწყობილობისაგან მოითხოვს. მნიშვნელოვან რესურსებს ეკუთვნის *დრო* და *მეხსიერება*. ვიტყვით, რომ M მანქანა n სიგრძის შესავალ მონაცემებზე მუშაობს $T_M(n)$ დრო, თუ M-ის გაჩერებამდე შესრულებული ტაქტების მაქსიმალური რაოდენობაა $T_M(n)$. ანალოგიურად, M საჭიროებს $S_M(n)$ მეხსიერებას, თუ n სიგრძის შესავალ მონაცემებთან მუშაობის დამთავრების შემდეგ თაურას მდებარეობის დაშორება ლენტის საწყისი მდებარეობიდან არ აღემატება $S_M(n)$-ს.

ნათელია, რომ $T_M(n) \subset S_M(n)$, რადგან ერთ ტაქტში ტიურინგის მანქანა მიაღწევს მხოლოდ სასრული რაოდენობის ახალ უჯრამდე.

სივრცულ-დროითი დუალიზმი, რომელიც საბუნებისმეტყველო მეცნიერებათა გარკვეული მახასიათებელია, არსებობს აგრეთვე იდეალიზებულ კომპიუტერთა დისკრეტულ სამყაროშიც. კითხვა, რომელიც $T_M(n)$-სა და $S_M(n)$ -ის ერთმანეთთან მიმართებაში ჩნდება ასეთია: არის თუ არა $T_M(n) \subset S_M(n)$ ჩართვა მკაცრი? გამოთვლების პრაქტიკა ამბობს, რომ ეს მართლაც ასეა. სამეცნიერო სენსაცია იყო კირკხოფის, პოლისა და ვალიანტის თეორემა, რომლის თანახმადაც ადგილი აქვს ჩართვას: $T_M(n) \subset S_M(n/\log n)$, საიდანაც გამოდის პასუხი ზემოთ დასმულ კითხვაზე- $T_M(n) \subset S_M(n)$ ჩართვა მკაცრია. გ. ვეილის კლასიკური გამონათქვამის პერიფრაზის შესაბამისად ეს შედეგი ასე ყალიბდება: "სივრცე და დრო სხვადასხვა რამეებია!"

ცხადია, რომ ალგორითმის ზემოთ მოყვანილ არაფორმალურ განმარტებას აკმაყოფილებს ტიურინგის მანქანის მუშაობის პრინციპი. შებრუნებული დებულება ჩიორჩის თეზისის სახელწოდებითაა ცნობილი.

ჩიორჩის თეზისი. *ნებისმიერი ალგორითმის რეალიზება შესაძლებელია ტიურინგის მანქანაზე.*

ეს დებულება მოიხსენება თეზისის (სამეცნიერო ლიტერატურაში მას ზოგჯერ ჩიორჩ-ტიურინგის პრინციპსაც უწოდებენ) სახით იმის გამო, რომ იგი ემპირიული ფაქტია, რომლის თეორემად "ქცევა" შეუძლებელია, რადგან არ არსებობს ალგორითმის მათემატიკურად უნიფიცირებული, მკაცრი განმარტება.

გამოთვლების ქვეშ გაიგება შემდეგი: გამოსახულება შესაძლებელია ჩაიწეროს ბულის გამოსახულებების საშუალებით, ხოლო ბულის გამოსახულება კი შესაძლებელია ჩაწერილი იქნას ფიქსირებული ლოგიკური ოპერაციების NOT, OR, AND-ს საშუალებით, რომლებსაც ლოგიკურ *გეიტებს* უწოდებენ, ნებისმიერი მოწყობილობა რომელიც შესაძლებელია აიგოს ლოგიკური გეიტების *უნივერსალური* ერთობლიობიდან, განმარტებით არის უნივერსალური გამომთვლელი მანქანა. გეიტების უნივერსალური სისტემა, რომელიც ჩვენ ვახსენეთ ცნობილია აგრეთვე *შაჰისის* სახელწოდებით. გეიტების უნივერსალურ სისტემაში შემავალი გეიტებისაგან არც მინიმალურობა მოითხოვება და არც დამოუკიდებლობა. ე.ი. იმის მოთხოვნა, რომ რომელიმე მათგანი არ გამოისახება დანარჩენების საშუალებით "ტექნიკური მოსაზრებების" გამო, აუცილებელი არ არის. მაგალითად, გეიტების უნივერსალური სისტემებია

$$\{NOT, AND\}, \{NOT, OR\}, \{XOR, AND\}.$$

გამოთვლით ტექნიკაში გამოიყენება $\{NOT, OR, AND\}$ გეიტების უნივერსალური სისტემა. გეიტები შეგვიძლია განვიხილოთ როგორც $\boldsymbol{B} = \{0,1\}$ სიმრავლეზე განსაზღვრული ოპერაციები, კერძოდ:

$$AND: \boldsymbol{B} \times \boldsymbol{B} \to \boldsymbol{B},$$
$$OR: \boldsymbol{B} \times \boldsymbol{B} \to \boldsymbol{B},$$
$$XOR: \boldsymbol{B} \times \boldsymbol{B} \to \boldsymbol{B},$$
$$NOT: \boldsymbol{B} \to \boldsymbol{B},$$

აქედან, AND, OR და XOR ("გამორიცხული არა"), ე.წ. ბინარული (ორ ადგილიანი) ოპერაციებია, ხოლო NOT კი უნარული (ერთ ადგილიანი) ოპერაციაა. ამ ფუნქციების მნიშვნელობები ყოველი $(x, y) \in \boldsymbol{B} \times \boldsymbol{B}$ წყვილისათვის მოცემულია ცხრილში:

x	y	AND	OR	XOR	NOT x
0	0	0	0	0	1
0	1	0	1	1	1
1	0	0	1	1	0
1	1	1	1	0	0

ბულის სქემა განმარტებით არის ნებისმიერი $f : \boldsymbol{B}^n \to \boldsymbol{B}^m$ ფუნქციის გამოთვლის საშუალება. მოვიყვანოთ მისი განმარტება.

განმარტება. ვთქვათ F არის ბაზისი ბულის ფუნქციების სიმრავლისათვის. $x_1, x_2, ..., x_n \in \boldsymbol{B}^n$ ცვლადების გარდა შემოვიტანოთ $y_1, ..., y_s$ დამხმარე ცვლადები.

სქემა არის მინიჭების $Y_1, ..., Y_s$ ოპერატორთა მიმდევრობა. ყოველ Y_i აქვს სახე:

$y_i = f_j(u_{k_1}, ..., u_{k_r})$, სადაც $f_j \in F$ ხოლო u_{k_p} ცვლადები არიან

ან ა) x_t ცვლადები, $1 \le t \le n$;

ან ბ) დამხმარე y_l ცვლადები, თუ სრულდება პირობა $1 \le l \le i$.

ამრიგად, საწყისი ცვლადების ნებისმიერი $x_1, ..., x_n$ მნიშვნელობისათვის გამოთვლის შედეგი არის $f(x_1, ..., x_n)$.

ბაზისს ეწოდება *სრული*, თუ ბულის ნებისმიერი f ფუნქციისათვის არსებობს სქემა ამ ბაზისში, რომელიც გამოითვლის f ფუნქციას.

სრულ ბაზისში შესაძლებელია ნებისმიერი $f : \boldsymbol{B}^n \to \boldsymbol{B}^m$ ფუნქციის გამოთვლა. ჩვენს უახლეს მიზანს წარმოადგენს ამ დებულების დამტკიცება.

კონიუნქცია და დიზიუნქცია განსაზღვრულნი არიან ცვლადების ნებისმიერი რაოდენობისათვის. კერძოდ, $\wedge(x_1,\ldots,x_n)=1$ მხოლოდ მაშინ, როდესაც $x_1=\ldots=x_n=1$, $\vee(x_1,\ldots,x_n)=0$ მხოლოდ მაშინ, როდესაც $x_1=\ldots=x_n=0$. $\{OR,\wedge,\vee\}$ არის სრული ბაზისი ბულის ფუნქციათა სიმრავლისათვის. ამ ბაზისს ჩვენ ვუწოდებთ *სტანდარტულს*. მრავალი ცვლადის კონიუნქცია და დიზიუნქცია ბუნებრივია სტანდარტულ ბაზისში გამოითვლებიან $n-1$ ზომის სქემების საშუალებით.

ნებისმიერ x ცვლადს ან მის $\neg x$ უარყოფას ვუწოდოთ *ლიტერალი*. ნებისმიერი მახასიათებელი $\chi_u(x)$ ფუნქცია, რომელიც ერთის ტოლ მნიშვნელობას ღებულობს x ცვლადის მხოლოდ იმ მნიშვნელობისათვის, როდესაც $u=x$, შესაძლებელია წარმოდგენილი იქნას ლიტერალების კონიუნქციის სახით. მართლაც, თუ $u_i=1$, მაშინ ლიტერალების კონიუნქციაში შევიტანოთ x_i ცვლადი, ხოლო თუ $u_i=0$, მაშინ კი კონიუნქციაში $\neg x_i$ ჩავრთოთ. რადგან ნებისმიერი $f:\boldsymbol{B}^n\to\boldsymbol{B}^m$ ფუნქცია შესაძლებელია წარმოვადგინოთ როგორც ბულის ფუნქციათა დალაგებული m-ეული, ამიტომ f შეიძლება ჩაიწეროს შემდეგნაირად:

$$f(x)=\bigvee_{u:f(u)=1}\chi_m(x).$$

ამ შემთხვევაში ამბობენ, რომ f ფუნქცია წარმოდგენილია *დიზიუნქციური ნორმალური ფორმით*, ე.ი. ლიტერების კონიუნქციის დიზიუნქცია. მაგრამ როგორც აღვნიშნეთ, რამდენიმე ცვლადის დიზიუნქცია გამოითვლება სტანდარტული ბაზისის საშუალებით. ეს კი ნიშნავს, რომ ნებისმიერი $f:\boldsymbol{B}^n\to\boldsymbol{B}^m$ ფუნქციისათვის არსებობს სქემა სტანდარტული ბაზისით, რომლის საშუალებითაც გამოითვლება f. ამრიგად, ჩვენ დავამტკიცეთ კლასიკური გამოთვლების ცენტრალური თეორემა.

თეორემა. *$\{NOT,OR,AND\}$ ბაზისი არის სრული.*

სქემის ზომა ეწოდება სქემაში მინიჭების ოპერაციების რაოდენობას. F ბაზისში სქემის მინიმალურ ზომას, რომელიც f-ს გამოითვლის, ეწოდება F ბაზისში f ფუნქციის *სქემური სირთულე*. მტკიცება, რომ ერთი ბაზისიდან მეორეზე გადასვლა არ ცვლის სქემურ სირთულეს. ეს ინვარიანტი აღვნიშნოთ $c(f)$-ით.

გამოთვლის სირთულე. დისკრეტულ და კომბინატორულ ამოცანათა უმრავლესობა იხსნება სრული გადარჩევის გზით. ასეთია მაგალითად ე.წ. ზურგჩანთის ამოცანაც (რაც შეიძლება მეტი საჭირო ნივთი ჩავტიოთ

ზურგჩანთაში იმ პირობებში, როდესაც მათი საერთო წონა (ან მოცულობა შეზრუდულია). მოვიყვანოთ მისი ფორმულირება:

ვიპოვოთ ისეთი მთელი a_j რიცხვები, რომელთათვისაც სრულდება ტოლობა:

$$\sum_{j=1}^{n} a_j x_j = b, \quad x_i = 0,1,$$

b მოცემული მთელი რიცხვია.

ეს ამოცანა ამოიხსნება $X = (x_1,\ldots,x_n) \in \mathbf{Z_2^n}$ ვექტორების გადარჩევის გზით, მაგრამ ნაბიჯების რაოდენობა იზრდება ექსპონენციალურად n-ის მიმართ (ე.წ. ამოცანის ზომის მიმართ.) ასეთი ტიპის ამოცანებს ეწოდებათ *გადარჩევითი.*

ზოგიერთი გადარჩევითი ამოცანებისათვის არსებობს ეფექტური, (ნაკლებად შრომატევადი, ვიდრე სრული გადარჩევაა) ამოხსნის მეთოდები, მაგრამ ასეთ ამოცანათა რიცხვი ცოტაა.

ეფექტური ალგორითმების ძიებამ და ამოცანის სირთულეთა ანალიზმა მკვლევარები მიიყვანა დისკრეტული მათემატიკის ცენტრალურ პრობლემამდე: შესაძლებელია თუ არა გვერდი ავუაროთ სრული გადარჩევის პროცედურას? არსებობენ ე.წ. ირიბი დებულებები, რომლებიც მიგვანიშნებენ, რომ ასეთი რამ თითქოს არ უნდა იყოს შესაძლებელი.

ძნელად ამოსახსნელ ამოცანათა ფენომენი ახალი არ არის მათემატიკისათვის. ალგორითმის ცნების დაზუსტების შემდეგ აღმოჩნდა, რომ არსებობენ ამოცანათა კლასები, რომელთათვისაც ალგორითმი საერთოდ არ არსებობს. ყველაზე ცნობილი მაგალითია ჰილბერტის მეათე პრობლემა: "არსებობს თუ არა ალგორითმი, რომელიც მოცემული მთელკოეფიციენტებიანი $P(X) = \sum_{|\alpha| \le p} n_\alpha X^\alpha$ მრავალწევრისათვის გაარკვევს, აქვს თუ არა $P(X) = 0$ განტოლებას ამონახსნი მთელ რიცხვებში". აქ α მულტიინდექსია, რომლის ზომა დამოკიდებულია X მთელკოორდინატებიანი ვექტორის განზომილებაზე. 1970 წელს ი.მ. მატიასევიჩმა აჩვენა, რომ ეს ამოცანა არაალგორითმიზებადია (იხ.[4]).

გადარჩევით ამოცანებში არსებობს ვარიანტთა სასრული სიმრავლე, რომელშიც ამოცანის ამონახსნია მოთავსებული. ასეთია მაგალითად ზემოთ მოყვანილი ამოცანა ზურგჩანთის შესახებ. ამონახსნი უნდა ვეძებოთ $X \in \mathbf{Z_2^n}$ ბულის ვექტორთა შორის, რომელთა რაოდენობა (განსხვავებულების) იქნება 2^n. თუ ყველა 2^n რაოდენობის n სიგრძის ვექტორისათვის შევამოწმებთ პირობას,

მივიღებთ პასუხს, მაგრამ n-ის ზრდასთან ერთად შესამოწმებელ ვექტორთა რიცხვი ექსპონენციალურად იზრდება (2^n ექსპონენციალური ფუნქციაა) და ამოცანა ხდება "ძნელად ამოსახსნელი", ანუ პრაქტიკულად ამოუხსნელი. ამიტომ გადარჩევით ამოცანებში გამოიყო კლასი, რომელსაც ეწოდება *ეფექტური.* მასში ის ამოცანები შევიდა, რომელთა ალგორითმის მუშაობის დრო ამოცანის ზომის მიმართ ფიქსირებული ხარისხის პოლინომით არის შემოსაზღვრული.

შემოვიტანოთ შემდეგი განმარტება:

განმარტება. ამბობენ, რომ გადარჩევითი Π_2 ამოცანა *რედუცირდება* გადარჩევით Π_1 ამოცანაზე, თუ Π_2 ამოცანის ამოხსნის მეთოდი შესაძლებელია გარდავქმნათ Π_1 ამოცანის ამოსახსნელ მეთოდად. რედუცირებას ეწოდება *პოლინომიალური*, თუ ასეთი გარდაქმნის განხორციელება შესაძლებელია პოლინომიალურ დროში.

გადარჩევითი ამოცანების რედუცირების ეფექტური (პოლინომიალური) კონცეფცია ჩამოაყალიბეს ს.კუკმა (1970), პ.კარპმა (1972) და ლ.ლევინმა (1973) (იხ.[1]). თეორია შეისწავლის იმ გადარჩევით ამოცანათა *P* კლასს, რომლებიც პოლინომიალურ დროში იხსნება.

NP (Nondeterministically Polynomial) - კლასში გამოვლენილია ისეთი უნივერსალური ანუ *NP* სრული ამოცანები, რომლებზედაც ეფექტურად რედუცირდება ნებისმიერი სხვა ამოცანა *NP*-დან. ამ აზრით უნივერსალური ამოცანები არიან სირთულის ეტალონები. დღეს ცნობილია მრავალი *NP* ამოცანა, რომლებიც ეფექტურად რედუცირების თვალსაზრისით ექვივალენტურნი არიან. თუ დამტკიცდება, რომ ერთი მაინც *NP* სრული ამოცანა ეკუთვნის *P*-ს, მაშინ დამტკიცდება, რომ *NP= P;* დღეს ეს პრობლემა ღიაა. შესაძლებელია აღმოჩნდეს, რომ *NP≠ P* ჰიპოთეზას ვერც ვუარყოფთ და ვერც ვამტკიცებთ (კონტუნუუმ ჰიპოთეზის მსგავსად).

არსებობს ინდივიდუალური ამოცანები, რომლებისთვისაც კარგად მუშაობს ისეთი გამოთვლითი მეთოდები, რომლებიც ექსპონენციალური სირთულის არიან. მაგალითად, წრფივი პროგრამირების ამოცანების ამოსახსნელად შემუშავებული სიმპლექს-მეთოდი (C. S Klee, G.Y.Minty (1972), N.Zadeh (1973)).

ალგორითმი *ექსპონენციალურია* თუ შესავალზე მოდებულია *N*-ოროობითი თანრიგი, ხოლო ალგორითმის მუშაობის დროა 2^N, ანალოგიურად ალგორითმს ეწოდება *პოლინომიალური*, თუ *N*-თანრიგის დასამუშავებელი დროა N^k, სადაც *k* რაიმე ფიქსირებული ნატურალური რიცხვია. ამრიგად, თუ ალგორითმი ექსპონენციალურია და შესავალზე მილიონი ოროობითი კოდი გვაქვს, გამომთვლელი

მოწყობილობის სისწრაფის გაზრდა და საკმაოდ დიდი პარალელიზმიც კი, გამოთვლის თვალსაზრისით, ეფექტს ვერ მოგვცემს.

დავუშვათ *N* თანამედროვე მანქანაზე *1* საათში ამოხსნილი ამოცანის პირობითი მაქსიმალური ზომაა. მაშინ ალგორითმების სირთულის შესაბამისად *N*-ის ზრდის დინამიკა მანქანის სიჩქარესთან ერთად მოცემულია ქვემოთ: (მონაცემები აღებულია (იხ.[1]-დან)

ალგორითმის სირთულე	თანამედროვე ეგმ-ზე	ეგმ-ზე რომელიც 100-ჯერ სწრაფია	ეგმ-ზე რომელიც 1000-ჯერ სწრაფია
წრფივი=u	*N*	*100 N*	*1000 N*
კვადრატული= u^2	*N*	*10 N*	*31.6N*
კუბური= u^3	*N*	*4.64N*	*10N*
მე-5 ხარისხის = n^5	*N*	*2.5N*	*3.98N*
ექსპონენციალური= 2^n	*N*	*N+6.64*	*N+9.97*
ექსპონენციალური= 3^n	*N*	*N+4.19*	*N+6.29*

უხეშად რომ ვთქვათ, თუ თანამედროვე ეგმ-ზე ჩვენ შეგვიძლია დავამუშაოთ 100-თანრიგიანი სიტყვა ექსპონენციალური ალგორითმით, მაშინ 110 თანრიგიანი სიტყვის დამუშავებისათვის საჭიროა სისწრაფის გაზრდა 1000-ჯერ.

ეფექტურად ითვლება ალგორითმი, თუ მისი მუშაობის დრო შემოსაზღვრულია შესავალი სიტყვის სიგრძის ***(N)*** რაიმე ხარისხით (N^k). პოლინომიალური ალგორითმები რეალიზებადად შეიძლება ჩაითვალოს, ხოლო უფრო რთული ალგორითმი რეალიზებადად არ ითვლება. რეალურად საქმე უფრო რთულადაა. კვადრატული ალგორითმიც (ყოველი ბიტის დასამუშავებლად იხარჯება N^2 დროის ერთეული) კი სასურველი არ არის. ამ მიმართულებით ემპირიული ფაქტი ასეთია: ამოცანათა უმრავლესობისათვის თუ "გაჩნდა" პოლინომიალური ალგორითმი, მალევე ჩნდება უფრო ეფექტური ვერსიები.

ამრიგად, გვაქვს გარკვეული დუალობა: ალგორითმების და სირთულის თეორიები. ალგორითმების თეორია ამუშავებს ეფექტურ ალგორითმებს, ხოლო სირთულის თეორია კი ამტკიცებს, რომ ზოგიერთი ამოცანისათვის ეფექტური ალგორითმი არ არსებობს.

საზოგადოდ, ამოცანა შეიცავს რამდენიმე პარამეტრს ანუ თავისუფალ ცვლადს, რომელთა მნიშვნელობა განსაზღვრული არ არის. ***A*** ამოცანა

განისაზღვრება შემდეგი ინფორმაციით: 1) პარამეტრთა სიით; 2) იმ თვისებების ფორმულირებით, რომელსაც პასუხი უნდა აკმაყოფილებდეს.

ინდივიდუალური I ამოცანა მიიღება ***A*** -ამოცანიდან, თუ ***A*** -ს ყველა პარამეტრს გარკვეული მნიშვნელობა მიენიჭება.

როგორც უკვე აღვნიშნეთ, ალგორითმი ამოცანის ამოხსნის პროცედურას ნაბიჯ-ნაბიჯ ასრულებს. დაკონკრეტების მიზნით ალგორითმის ქვეშ ვიგულისხმებთ პროგრამას ეგმ-თვის. ვიტყვით, რომ ალგორითმი ხსნის ***A*** ამოცანას, თუ იგი ხსნის ნებისმიერ I ინდივიდუალურ ამოცანას. (აქ ხაზი გავუსვათ იმას, თუ იხსნება რომელიმე I ინდივიდუალური ამოცანა, არ ჩავთვალოთ, რომ იხსნება ***A*** ამოცანა).

ინდივიდუალური ამოცანისათვის თავიდანვე შეირჩევა გარკვეული წესი და ყოველი ***A*** ამოცანისათვის არსებობს გარკვეული ფიქსირებული კოდირების სქემა, რომელიც ინდივიდუალურ ამოცანას სიმბოლოების ჯაჭვად წარმოადგენს. ***A*** ამოცანის I ინდივიდუალური ამოცანის შესავალი სიგრძე არის ***A*** ამოცანის კოდირების სქემის შესაბამისი სიმბოლოების რაოდენობა I ინდივიდუალური ამოცანისათვის. ამოცანის შესავალი სიგრძე არის ინდივიდუალური ამოცანის ზომის ფორმალური მახასიათებელი. ალგორითმის დროითი სირთულე ასახავს მის შესასრულებლად საჭირო დროს ("დროის დანახარჯს"). ალგორითმის *დროითი სირთულე* არის ფუნქცია, რომელიც ყოველ n შესავალ სიგრძეს უთანადებს იმ მაქსიმალურ დროს, რომელსაც საჭიროებს ალგორითმი მოცემული n სიგრძის ინდივიდუალური ამოცანის ამოსახსნელად.

ბუნებრივია, რომ ალგორითმის დროითი სირთულე სრულად განსაზღვრული არ იქნება, თუ დაფიქსირებული არ არის ინდივიდუალური ამოცანის შესავალი სიგრძე და არჩეული არ იქნება მოწყობილობა (ან მისი თეორიული მოდელი). მიუხედავად ამისა, ამოცანათა კლასიფიკაცია მაინც მოხერხდა. ამიტომ, შესაძლებელია აზროვრივად დავაფიქსიროთ კონკრეტული ამოცანისათვის კოდირების სქემა, კონკრეტული გამომთვლელი მოწყობილობა (ან მოდელი) და ამის შემდეგ განვიხილოთ ალგორითმის დროითი სირთულე.

ვიტყვით, რომ $f(n)$ ფუნქცია არის $O(g(n))$–ი, თუ არსებობს ისეთი c მუდმივი, რომ $|f(n)| \le c|g(n)|$ უტოლობა სრულდება ნებისმიერი $n \ge 0$ -თვის.

პოლინომიალური ალგორითმი. (ან ალგორითმი პოლინომიალური დროითი სირთულით) ეწოდება ისეთ ალგორითმს, რომლის დროითი სირთულე $O(p(n))$-ის ტოლია, სადაც $p(n)$ რაიმე პოლინომიალური ფუნქციაა, ხოლო n კი ალგორითმის შესავალი სიგრძეა. იმ ალგორითმებს, რომელთათვისაც არ არსებობს ანალოგიური შეფასება, ეწოდებათ ექსპონენციალური. აქვე შევნიშნოთ, რომ მიუხედავად იმისა, რომ $\log n$ სახის ფუნქცია არ არის პოლინომიალური, იგი ექსპონენციალურად არ ითვლება სირთულის თვალსაზრისით.

ამოცანათა სირთულის ამგვარი დახასიათება ეკუთვნის ა.კობჰემსა და ჯ.ედმონდს (იხ. [1]). ედმონსმა პოლინომიალური ალგორითმები გააიგივა "კარგ" ალგორითმებთან და გამოთქვა მოსაზრება, რომ მთელრიცხოვანი პროგრამირების ზოგიერთი ამოცანისთვის არსებობს "კარგი" ალგორითმები. ამ თვალსაზრისით ექსპონენციალური ალგორითმები "კარგ" ალგორითმებად არ ითვლებიან. ხშირ შემთხვევაში ეს მართლაც ასეა. ექსპონენციალურ ალგორითმთა უმრავლესობა სრული გადარჩევაა. არსებობს შეთანხმება, რომლის თანახმადაც ამოცანა არ ითვლება "კარგად ამოხსნისათვის" მანამ, სანამ მისთვის არ მოინახება პოლინომიალური ალგორითმი. ამოცანას ვუწოდებთ რთულს, თუ მისთვის პოლინომიალური ალგორითმი არ არსებობს. ჩვენ მოვიყვანეთ "რთულ ამოცანათა" ერთ-ერთი შესაძლო განმარტება. "ეფექტურ" (პოლინომიალურ) და "არაეფექტურ" (ექსპონენციალურ) ალგორითმებს შორის განსხვავებამ შეიძლება საპირისპირო ხასიათი მიიღოს, როდესაც ამოსახსნელი ამოცანის ზომა დიდი არ არის. მაგ. $f(n)=2^n$ ექსპონენციალური ფუნქციის "ყოფაქცევა" უკეთესია $g(n)=n^5$ ფუნქციაზე, როდესაც $n \le 20.$

ამოცანის დროითი სირთულე, დამოკიდებული არ არის კოდირების სქემასა და ეგმ-ის მოდელზე. *კოდირების სქემები*, რომლებიც დღეს პრაქტიკაში გამოიყენება, ერთმანეთისაგან განსხვავდებიან არაუმეტეს პოლინომიალური რიგით, თუმცა, თეორიულად, არაპოლინომიალური რიგით განსხვავებული კოდების მოგონებაც შეიძლება.

ყველა დღემდე არსებული *ეგმ-ის მოდელი* (ტიურინგის მანქანა, მანქანა ხელმისაწვდომი მეხსიერებით) დროითი სირთულის თვალსაზრისით ექვივალენტურია. აქვე შევნიშნოთ, რომ ჩვენ ვგულისხმობთ აგრეთვე იმ თეორიულ თუ რეალურ ეგმ-ს, რომლებიც სასრული რაოდენობის პარალელიზმის თვისების მატარებლები არიან.

ბევრი პრაქტიკული ამოცანა გარკვეული სახეცვლილების შემდეგ ხვდება NP კლასში. NP კლასს ეკუთვნის ე.წ. SAT(*Satisfiability*)-ამოცანა (SAT-ამოცანა არის ბულის ფორმულა, რომელიც შედგება ცვლადების სახელებისაგან, ფრჩხილებისა და AND, OR, NOT ლოგიკური ოპერაციებისაგან. ამოცანა მდგომარეობს იმის გარკვევაში, შესაძლებელია თუ არა ფორმულაში შემავალ ყველა ცვლადებს ისე მივანიჭოთ მნიშვნელობები (ჭეშმარტი ან მცდარი), რომ ფორმულა გახდეს ჭეშმარიტი). თუ ეს ამოცანა სრულდება პოლინომიალურ დროში, მაშინ NP-ს ნებისმიერი ამოცანა პოლინომიალურ დროში იხსნება. აქედან, თუ *შესრულების* ამოცანა პოლინომიალურ დროში იხსნება, მაშინ ნებისმიერი ამოცანა NP კლასიდან იხსნება პოლინომიალურ დროში. ეს კი ნიშნავს, რომ შესრულების ამოცანა "ყველაზე ძნელი" ამოცანაა NP

კლასიდან. "ყველაზე ძნელი" ამოცანების ქვეკლასმა NP-დან მიიღო სახელწოდება NP სრული ამოცანები (ან უნივერსალურ ამოცანათა კლასი).

როგორც აღვნიშნეთ, ყველაზე ხელსაყრელი საშუალება იმის შესაფასებლად, თუ როგორი სისწრაფით ამოხსნის კონკრეტული ალგორითმი მოცემულ ამოცანას, არის ის, რომ გავარკვიოთ, ალგორითმის შესასრულებლად საჭირო ბიჯების რაოდენობა როგორ იზრდება შესავალი მონაცემების ზრდასთან ერთად. მაგალითისათვის განვიხილოთ ფაქტორიზაციის ამოცანა, რომელიც ეკუთვნის NP კლასს. N ნატურალური რიცხვის ფაქტორიზაცია ნიშნავს N-ის დაშლას მარტივ მამრავლებად. ამ ამოცანისათვის შესავალი მონაცემები არის თვით ნატურალური N რიცხვი, რომლის სიგრძეა $\log N$. ლოგარითმული ფუნქციის ფუძე განისაზღვრება თვლის სისტემით. რადგან თანამედროვე ეგმ-ებში თვლის სისტემა ორობითია, ამიტომ შესავალი რიცხვის ზომას ჩავთვლით $\log_2 N$-ის ტოლად.

თანამედროვე ეგმ-ებში ფაქტორიზაციის ამოცანის აქამდე ცნობილი საუკეთესო ალგორითმი სრულდება $e^{\sqrt[3]{\frac{64}{9}}(\ln N)^{\frac{1}{3}}(\ln\ln N)^{2/3}}$ ნაბიჯში (იხ. [1]). ამრიგად, ეს ალგორითმი იზრდება ექსპონენციალურად შესავალი მონაცემების ზრდასთან ერთად, უფრო დაწვრილებით ამ ამოცანას ჩვენ ქვემოთ განვიხილავთ.

ს.ბრაუნშტეინს [16] თავის სტატიაში მოყვანილი აქვს ასეთი ფაქტი: "1994 წელს 129-ნიშნიანი რიცხვი (რომელიც *RSA129*-ის სახელწოდებითაა ცნობილი) დაშლილი იქნა მარტივ მამრავლებად ამ ალგორითმის საშუალებით ქსელში გაერთიანებული 1600 ეგმ-ის საშუალებით 8 თვის განმავლობაში". აქედან გამოდის, რომ იგივე რესურსები 250-ნიშნიანი რიცხვის დაშლას დაჭირდება $\approx 8.10^5$ წელი, ხოლო 1000-ნიშნიანი რიცხვის ფაქტორიზაციას კი $\approx 10^{25}$ წელი, რაც გაცილებით აჭარბებს სამყაროს წლოვანებას.

საზოგადოდ, მისაღებ ალგორითმად ითვლება ისეთი ალგორითმი, რომელშიც ნაბიჯების რაოდენობა იზრდება როგორც შესავალი მონაცემების მიმართ მრავალწევრი არაუმეტეს მეორე ან მესამე ხარისხისა.

2. კვანტური ფიზიკის მათემატიკური საფუძვლები

ცნებები და დებულებები. ამ პარაგრაფში ჩვენ განვავითარებთ კვანტური მექანიკის მათემატიკურ ფორმალიზმს მხოლოდ ელემენტარულ დონეზე. აქ მოყვანილი ცნებების და დებულებების უმრავლესობას გამოვიყენებთ მომდევნო პარაგრაფებში. დებულებები ძირითადად დამტკიცებების

გარეშეა მოყვანილი, მათი ნახვა შესაძლებელია მრავალ სახელმძღვანელოში. მასალის გადმოცემისას ჩვენ ვსარგებლობდით [3]-ით.

განმარტება. L კომპლექსურ წრფივ სივრცეს დადებითად განსაზღვრული ერმიტული სკალარული ნამრავლით ეწოდება *უნიტარული სივრცე.*

თუ $a,b \in L$, მაშინ მათი სკალარული ნამრავლი განისაზღვრება ფორმულით:

$$(a,b) = \sum_i a_i \overline{b_i}$$

სადაც $a = (a_1, a_2, ...), \quad b = (b_1, b_2, ...), \quad \overline{b_i}$ აღნიშნავს b_i-ს კომპლექსურად შეუღლებულს,

$$|a| = \sqrt{(a,a)} = \left(\sum_{i=1}^{n} |x_i|^2 \right)^{\frac{1}{2}}$$

ნამდვილ რიცხვს ეწოდება a ვექტორის ნორმა.

უნიტარულ სივრცეს, რომელიც სრულია ამ ნორმის მიმართ, ეწოდება *ჰილბერტის* სივრცე. აქედან, სასრულგანზომილებიანი უნიტარული სივრცეები ჰილბერტის სივრცეებია.

მოვიყვანთ ორ დებულებას წრფივი ალგებრიდან:

1.ყოველ სასრულგანზომილებიან უნიტარულ სივრცეს აქვს ორთონორმირებული ბაზისი (ყველა ვექტორის სიგრძე ამ ბაზისიდან 1-ის ტოლია).

2.სასრულგანზომილებიანი უნიტარული L სივრცე იზომორფულია $\mathbf{C^n}$-ის, სადაც $n = dim L$.

კვანტური სისტემის მდგომარეობის სივრცე. კვანტური მექანიკის პოსტულატის თანახმად, ისეთ ფიზიკურ სისტემებს, როგორებიცაა ელექტრონი, წყალბადის ატომი და ა.შ. შესაძლებელია დავუკავშიროთ მათემატიკური მოდელი, რომელიც შედგება შემდეგისაგან:

1. $\mathbf{H}$ *უნიტარული სივრცისაგან,* რომელსაც სისტემის მდგომარეობის სივრცე ეწოდება. ჩვეულებრივ $\mathbf{H}$ არის სივრცე-დროზე განსაზღვრული ფუნქციების სიმრავლე, რომელიც უსასრულო განზომილებიანია. სასრულ-განზომილებიანი $\mathbf{H}$ წარმოიშობა, როგორც *სისტემის შიგა თავისუფლების ხარისხის სივრცე.* ასეთია მაგალითად ელექტრონის "სპინური მდგომარეობის" სივრცე, რომელიც ორგანზომილებიანია და ამრიგად $\mathbf{C^2}$-ის იზომორფულია.

2. *სისტემის მდგომარეობისაგან,* რომელიც $\mathbf{H}$-ის ერთგანზომილებიანი ქვესივრცის ელემენტი. გეომეტრიულად სისტემის მდგომარეობა არის *სხივი.* მას *სუფთა მდგომარეობას* უწოდებენ.

მთელი ინფორმაცია სისტემის მდგომარეობის შესახებ დროის ფიქსირებულ მომენტში განისაზღვრება $l \subset \mathbf{H}$ სხივის, ან არანულოვანი $\psi \in \mathbf{H}$ ვექტორის მოცემით. ψ უწოდებენ მდგომარეობის შესაბამის ψ-ფუნქციას, ან მდგომარეობის ვექტორს.

კვანტური მექანიკის ერთ-ერთი პოსტულატია ე.წ. *სუპერპოზიციის პრინციპი: ψ ფუნქციები წარმოქმნიან კომპლექსურ წრფივ სივრცეს.* $\sum_{j=1}^{n} a_j \psi_j$, $a_j \in \mathbf{C}$ წრფივ კომბინაციას ეწოდება $\psi_1,\ldots,\psi_n$ მდგომარეობების სუპერპოზიცია. შევნიშნოთ, რომ რადგან ფიზიკური აზრი აქვს მხოლოდ სხივებს (აღვნიშნოთ ისინი $\mathbf{C}\psi_j$, და არა თვით ψ_j ვექტორებს) ამიტომ a_j კოეფიციენტებისათვის ცალსახად მნიშვნელობების მიწერა შეუძლებელია, მაგრამ თუ ავირჩევთ ψ_j ვექტორებს ისე, რომ ისინი იყვნენ ა) ნორმირებულები, ე.ი. $|\psi_j|^2 = 1$, ბ) წრფივად დამოუკიდებლები, გ) წრფივი კომბინაცია $\sum_{j=1}^{n} a_j \psi_j$ იყოს ნორმირებული, ე.ი. $\left|\sum_{j=1}^{n} a_j \psi_j\right| = 1$ მაშინ $\mathbf{C}\psi_j$ სხივზე ψ_j ვექტორის არჩევის არაცალსახობა დაიყვანება $e^{i\varphi_j}$ მამრავლის სიზუსტემდე. ამ უკანასკნელს ეწოდება *ფაზური მამრავლი.* ანალოგიურ არაცალსახობას ექნება ადგილი a_j კოეფიციენტების არჩევის დროს, მაშინაც როდესაც a_j რიცხვებს ჩავთვლით ნამდვილ, არაუარყოფით რიცხვებად, ხოლო თუ დამატებით მოვითხოვთ $\left|\sum_{j=1}^{n} a_j \psi_j\right| = 1$ ნორმირების პირობის შესრულებას, მაშინ a_j-ები განისაზღვრებიან ცალსახად.

კვანტური მექანიკის მეორე პოსტულატია შემდეგი: სისტემა, რომელიც მომზადდება $\psi \in \mathbf{H}$ მდგომარეობაში, შესაძლებელია მაშინვე გადავიდეს $\chi \in \mathbf{H}$ მდგომარეობაში $\dfrac{|(\psi,\chi)|^2}{|\psi|^2|\chi|^2} = \cos^2\theta$-ს ტოლი ალბათობით, სადაც θ არის კუთხე ψ და χ ვექტორებს შორის.

თუ ψ და χ მდგომარეობები ნორმირებულია, მაშინ ψ-დან χ მდგომარეობაში გადასვლის ალბათობა ტოლია $|(\psi,\chi)|^2$ – ის, ხოლო თვით სკალარული

ნამრავლი (ψ, χ) არის კომპლექსური რიცხვი და ეწოდება ψ-დან χ-ში გადასვლის *ალბათობის ამპლიტუდა*. კვანტურ მექანიკაში განიხილება ისეთი სკალარული ნამრავლი, რომელიც ანტისიმეტრიულია პირველი არგუმენტის მიმართ და (ψ, χ) ჩანაწერის მაგივრად იხმარება აღნიშვნა: $\langle\chi|\psi\rangle$. $|\psi\rangle$ ეწოდება კეტ-ვექტორი, ხოლო $\langle\chi|$-ს კი ბრა-ვექტორი. $|\psi\rangle$ არის $\mathbf{H}$-ის ელემენტი, ხოლო $\langle\chi|$ კი $\mathbf{H}^*$-ის ელემენტი, სადაც $\mathbf{H}^*$ არის $\mathbf{H}$-ზე წრფივი ფუნქციონალების სივრცე, ამრიგად, $\langle\chi|\psi\rangle$ არის χ ფუნქციონალის მნიშვნელობა ψ-ზე (სახელწოდება ბრა და კეტ ვექტორები და შესაბამისი აღნიშვნები მოდის დირაკიდან, რომელმაც ასეთი დასახელება აიღო **< >** ბრჩხილის ინგლისური შესატყვისის *bracket*-ის გაყოფით: *bra* და *cket*.)

თუ ψ და χ მდგომარეობები ორთოგონალურია, ე.ი. თუ $(\psi, \chi) = 0$, მაშინ ψ მდგომარეობის "აღმოჩენა" χ მდგომარეობაში (ψ-ს მდგომარეობის მომზადებისთანავე), შეუძლებელია, ანუ სისტემის ψ მდგომარეობა B_χ მოწყობილობას ვერ გაივლის ყველა სხვა შემთხვევაში ψ აღმოჩენა χ მდგომარეობაში შესაძლებელია სხვადასხვა ალბათობით.

მდგომარეობათა ნებისმიერი ორთონორმირებული $\{\psi_1, ..., \psi_n\}$ ბაზისები ადგენენ სისტემის *ბაზისურ მდგომარეობათა* ერთობლიობას. დავუშვათ გვაქვს B ტიპის $B_{\psi_1}, ..., B_{\psi_n}$ მოწყობილობები. თუ მასში მრავალჯერ გავატარებთ სისტემას, რომელიც იმყოფება $\psi = \sum_{i=1}^{n} a_i \psi_i, 0 \le a_i \le 1$ მდგომარეობაში, გამოსავალზე აღმოვაჩენთ ψ_i მდგომარეობას a_i^2-ის ტოლი ალბათობით. ამრიგად, ამ წრფივ კომბინაციაში a_i კოეფიციენტები შესაძლებელია "გავზომოთ" სტატისტიკური მეთოდებით. ეს არის ერთ-ერთი მიზეზი იმისა, რომ კვანტური-მექანიკური გაზომვები საჭიროებენ დიდი რაოდენობის სტატისტიკური მონაცემების დამუშავებას და ამრიგად, მრავალჯერ დაკვირვებას. ექსპერიმენტები ისეთია, რომ ψ მდგომარეობაში მყოფი სისტემები "გადიან" B ტიპის მოწყობილობაში "ნაკადის" სახით და გამოსავალზე a_i^2-ის ტოლი ალბათობით მიიღებიან მდგომარეობები ინტენსივობების, გარკვეული სახის სპექტრალური წირების სახით. ეს ინტენსივობები უკვე არიან სტატისტიკური გაშუალედების შედეგები.

ფეინმანის წესი. ვთქვათ H -ში ამორჩეულია $\{\psi_1,\ldots,\psi_n\}$ ორთონორმირებული ბაზისი. ნებისმიერი $\psi \in H$ მდგომარეობის ვექტორისათვის გვაქვს წარმოდგენა: $\psi = \sum_{i=1}^{n}(\psi,\psi_i)\psi_i$, საიდანაც

$$(\psi,\chi) = \sum_{i=1}^{n}(\psi,\psi_i)(\psi_i,\chi). \tag{1.2-1}$$

ანალოგიურად,

$$(\psi,\psi_i) = \sum_{j=1}^{n}(\psi,\psi_j)(\psi_j,\psi_i), \tag{1.2-2}$$

თუ (1.2-2)-ს ჩავსვამთ (1.2-1)-ში მივიღებთ:

$$(\psi,\chi) = \sum_{i_1,i_2=1}^{n}(\psi,\psi_{i_1})(\psi_{i_1},\psi_{i_2})(\psi_{i_2},\chi). \tag{1.2-3}$$

უფრო ზოგად შემთხვევაში, ნებისმიერი m -თვის (1.2-3)-ის ანალოგიურად გვექნება:

$$(\psi,\chi) = \sum_{i_1,\ldots i_m=1}^{n}(\psi,\psi_{i_1})(\psi_{i_1},\psi_{i_2})\ldots(\psi_{i_m},\chi). \tag{1.2-4}$$

წრფივი ალგებრის ზემოთ მოყვანილი ფორმულების ინტერპრეტაცია მოახდინა ფეინმანმა და ჩამოაყალიბა როგორც "კომპლექსური ალბათობის თეორიის" კანონი. ეს კანონი ქვემოთაა აღწერილი.

იდეალიზებული სისტემა აღიწერება შემდეგნაირად: გვაქვს ფიზიკური A ტიპის A_ψ მოწყობილობები, რომელსაც შეუძლია წარმოქმნას ჩვენი სისტემის ψ მდგომარეობების (უფრო ზუსტად $\mathbf{C}\psi$ -ის) მრავალი ეგზემპლარი სხვადასხვა ψ -ებისათვის $\mathbf{H}$ -დან. გარდა ამისა, ვთქვათ გვაქვს ფიზიკურ მოწყობილობათა მეორე B ტიპი, მაგალითად, χ მდგომარეობისათვის - B_χ, რომელთა შესავალზე "მოდებულია" სისტემები ψ მდგომარეობაში, ხოლო გამოსავალზე კი გვაქვს χ მდგომარეობები, ან არაფერი (ე.ი. ψ სისტემა ვერ გადის B_χ "ფილტრში")

მდგომარეობათა $(\psi,\psi_{i_1},\psi_{i\,2},\ldots,\psi_{i_m},\chi)$ მიმდევრობას შევხედოთ როგორც სისტემის "კლასიკურ სტრუქტურას", რომელსაც გაირბენს სისტემა ფრჩხილებში მოთავსებული მდგომარეობის თანმიმდევრული გავლით, ხოლო $(\psi,\psi_{i_1})(\psi_{i_1},\psi_{i_2})\ldots(\psi_{i_m},\chi)$ რიცხვს შევხედოთ როგორც ψ მდგომარეობიდან χ მდგომარეობაში გადასვლის ამპლიტუდას შესაბამისი კლასიკური ტრაექტორიის გავლით, ეს ამპლიტუდა ტოლია ψ -დან ψ_{i_1}-ში, ψ_{i_1}-დან ψ_{i_2}-ში, ..., ψ_{i_m}-დან χ -

ში გადასვლის ამპლიტუდების ნამრავლის. ამრიგად, (1.2-4) ფორმულა ნიშნავს: ψ -მდგომარეობიდან χ -მდგომარეობაში გადასვლის ამპლიტუდა ტოლია ψ -დან χ -ში ყველა შესაძლო კლასიკურ ტრაექტორიაზე გადასვლის ამპლიტუდების ჯამის.

ფეინმანის ზემოთ მოყვანილი წესის თანახმად გადასვლების ამპლიტუდა შესაძლებელია გამოისახოს კლასიკური ტრაექტორიების უსასრულო განზომილების ფუნქციონალურ სივრცეზე აღებული კონტინუალური ინტეგრალის საშუალებით. გადასვლის ამპლიტუდის გამოთვლის რ.ფეინმანის ამ ნახევრად ევრისტიკული მეთოდის დასაფუძნებელი მათემატიკური თეორია დღემდე არ არის შექმნილი, თუ კი ასეთი თეორია იარსებებს, მაშინ ფიზიკოსთა ბევრი გამონათქვამი იქნება კორექტული მათემატიკის თვალსაზრისით. მიუხედავად ამისა, ფეინმანის ამ წესის გამოყენებით მიღებული თეორიული დასკვნების მართებულობა ხშირ შემთხვევაში ექსპერიმენტითაა დადასტურებული.

გაზომვის პროცედურა კვანტურ მექანიკაში. კვანტური მექანიკის რიგით მესამე პოსტულატი შემდეგნაირად ყალიბდება: დავუშვათ H რაიმე კვანტური სისტემის მდგომარეობათა სივრცეა. ყოველ ფიზიკურ სიდიდეს (კოორდინატი, ენერგია, სპინი, იმპულსი, და ა.შ.) რომლის მნიშვნელობის გაზომვაც შესაძლებელია, შეესაბამება $A:\mathbf{H}\to\mathbf{H}$ თვითშეუღლებული ოპერატორი, რომელიც აკმაყოფილებს შემდეგ პირობებს:

1) A ოპერატორის სპექტრი არის გასაზომი სიდიდის მნიშვნელობათა ის სრული სიმრავლე, რომელიც მიიღება ამ სიდიდის გაზომვით სისტემის სხვადასხვა მდგომარეობაში ყოფნის დროს.
2) თუ $\psi\in\mathbf{H}$ არის A ოპერატორის საკუთრივი ვექტორი λ საკუთრივი მნიშვნელობით, მაშინ ψ მდგომარეობაში A-ს გაზომვით საკმაოდ დიდი ალბათობით მივიღებთ λ-ს.
3) უფრო ზოგადი დებულება. A სიდიდის გაზომვა ψ მდგომარეობაში $\left(|\psi|=1\right)$, მოგვცემს A ოპერატორის სპექტრიდან რომელიმე λ საკუთრივ მნიშვნელობას ალბათობით, რომელიც λ-ს შესაბამისი $\mathbf{H}(\lambda)$ სრულ საკუთრივ ქვესივრცეზე ψ -ს ორთოგონალური პროექციის ნორმის კვადრატის ტოლია.

წრფივი ალგებრის კურსში მტკიცდება, რომ $\mathbf{H}$ იშლება ორთოგონალურ სივრცეთა $\oplus_{i=1}^{m}\mathbf{H}(\lambda_i)$, $\lambda_i\neq\lambda_j, i\neq j$, პირდაპირ ჯამად, ამიტომ ψ შესაძლებელია დაიშალოს $\psi_i\in H(\lambda_i)$, $i=1,\ldots,m$ შესაბამისი პროექციების ჯამად და სამართლიანია პითაგორას თეორემა $|\psi|^2=\sum_{i=1}^{m}|\psi_i|^2=1$;

ამ დებულების ინტერპრეტაცია ასეთია: A დაკვირვებადი სიდიდის გაზომვა ნებისმიერ ψ მდგომარეობაში 1-ის ტოლი ალბათობით მოგვცემს A-ს რომელიმე მნიშვნელობას ყველა შესაძლო მნიშვნელობათა სიმრავლიდან.

ფიზიკურ სიდიდეებს, რომელთა გაზომვაც შესაძლებელია და აგრეთვე, მათ შესაბამის ოპერატორებს ეწოდებათ *დაკვირვებადი.* პოსტულატი დაკვირვებადი სიდიდეების შესახებ ზოგჯერ უფრო ზოგადად ყალიბდება და ითვლება, რომ ყოველ თვითშეუღლებულ ოპერატორს შეესაბამება რაიმე დაკვირვებადი სიდიდე.

ზემოთ მოყვანილი B ტიპის B_χ მოწყობილობა, რომელიც დაკვირვებად სიდიდეს ზომავს, წარმოქმნილ ქვესივრცეზე ორთოგონალური პროექციაა. მას მიეწერება 1-ის ტოლი მნიშვნელობა თუ სისტემამ "გაიარა" B მოწყობილობა, წინააღმდეგ შემთხვევაში მიეწერება 0. A ტიპის A_ψ მოწყობილობა კი წარმოქმნის სისტემას სხვადასხვა მდგომარეობებში და B_χ მოწყობილობა ატარებს სისტემას მხოლოდ მაშინ, როდესაც იგი იმყოფება ψ მდგომარეობაში. ამ მაგალითიდან ჩანს, რომ B_χ მოწყობილობა, რომელიც ზომავს დაკვირვებად სიდიდეს ψ მდგომარეობაში, საზოგადოდ ცვლის ამ მდგომარეობას: $|(\psi,\chi)|^2$ ალბათობით ψ გადაყავს χ-ში, ხოლო $1-|(\psi,\chi)|^2$ ალბათობით "ანადგურებს" სისტემას. ამიტომ ტერმინ "გაზომვას", რომლის ქვეშაც გაიგება ფიზიკური სისტემისა და მოწყობილობის ურთიერთქმედების აქტი, საერთო არაფერი აქვს "გაზომვასთან" კლასიკური ფიზიკის თვალსაზრისით.

საშუალო მნიშვნელობა და განუზღვრელობის პრინციპი. დავუშვათ A რაიმე დაკვირვებადი სიდიდეა, $\{\lambda_i\}$-მისი სპექტრია, $\mathbf{H}=\bigoplus_i \mathbf{H}_i$-ორთო-გონალური დაშლაა. უკვე აღვნიშნეთ, რომ A მოქმედებს $|\psi\rangle$ მდგომარეობაზე $(|\psi|=1)$ და ღებულობს λ_i მნიშვნელობას $(\psi, p_i\psi)$-ს ტოლი ალბათობით, სადაც $p_i:\mathbf{H}\to\mathbf{H}(\lambda_i)$ ორთოგონალური პროექტორია. A-ს $\hat{A}_\psi$ საშუალო მნიშვნელობა (რომელიც მიიღება მრავალჯერადი გაზომვით) გამოითვლება შემდეგნაირად:

$$\hat{A}_\psi=\sum_i \lambda_i(\psi,p_i\psi)=\sum_i(\psi,\lambda_i p_i\psi)=(\psi,A\psi).$$

თუ A და B ოპერატორები თვითშეუღლებულებია, და ისინი არ კომუტირებენ, მაშინ AB თვითშეუღლებული ოპერატორი არ არის. მართლაც,

$$(AB)^*=B^*A^*=BA\neq AB,$$

მაგრამ A^2, $A-1.\lambda$, $\lambda \in \mathbf{R}$ ოპერატორები და კომუტატორი

$$\frac{1}{i}[A,B]=\frac{1}{i}(AB-BA)$$

თვითშეუღლებული ოპერატორია.

$\left(A-\hat{A}_\psi\right)^2$ დაკვირვებადი სიდიდის $\left[\left(A-\hat{A}_\psi\right)^2\right]^{\wedge}_{\hat{\psi}}$ საშუალო მნიშვნელობა $|\psi\rangle$ მდგომარეობაში არის $\hat{A}$-ს მნიშვნელობის საშუალო სტანდარტული გადახრა საშუალო მნიშვნელობიდან.

შემოვიტანოთ აღნიშვნა: $\widehat{\Delta A_\psi}=\sqrt{\left[\left(A-\widehat{A_\psi}\right)^2\right]_{\hat{\psi}}}$.

დებულება (ჰაიზენბერგის განუზღვრელობის პრინციპი) [3]. **H** უნიტარულ სივრცეში A და B თვითშეუღლებული ოპერატორებისათვის ადგილი აქვს უტოლობას:

$$\widehat{\Delta A_\psi}\widehat{\Delta B_\psi}\geq\frac{1}{2}|([A,B]\psi,\psi)|.$$

ზემოთ მოყვანილი დებულება გვიჩვენებს, რომ არაკომუტირებადი დაკვირვებადი A და B სიდიდეების ერთდროულად გაზომვა შეუძლებელია.

ჰაიზენბერგის უტოლობის გამოყენება განსაკუთრებით მნიშვნელოვანია იმ შემთხვევაში, როდესაც საქმე გვაქვს *კანონიკურად შეუღლებულ* დაკვირვებად სიდიდეთა წყვილთან. ასეთი წყვილი განმარტებით არიან ისეთი A და B ოპერატორები, რომლებიც აკმაყოფილებენ პირობას: $\frac{1}{i}[A,B]=id$, მაშინ ჰაიზენბერგის უტოლობას ნებისმიერი ψ-თვის აქვს სახე:

$$\widehat{\Delta A_\psi}\widehat{\Delta B_\psi}\geq\frac{1}{2}.$$

შევნიშნოთ, რომ სასრულგანზომილებიან სივრცეში ასეთი ოპერატორები (კანონიკურად შეუღლებული) არ არსებობენ. უსასრულოგანზომილებიან სივრცეში კი კანონიკურად შეუღლებული წყვილი არსებობს. მაგალითად, x და $\frac{d}{dx}$ ოპერატორები ასეთ წყვილს ქმნიან:

$$\frac{1}{i}\left[x,\frac{1}{i}\frac{d}{dx}\right]=id$$

და გამოიყენებიან კლასიკური სისტემების ისეთ კვანტურ მოდელებში, რომლებიც კლასიკური ფიზიკის ენაზე ყალიბდებიან შემდეგნაირად: "ნაწილაკი მოძრაობს ერთგანზომილებიან პოტენციალურ ველში".

აღვწეროთ რამდენიმე დაკვირვებადი სიდიდე.

1. დაკვირვებადი კოორდინატი. *დაკვირვებადი კოორდინატი* არის $\{f:\mathbf{R}\to\mathbf{C}\}$ ნამდვილ კომპლექსურმნიშვნელობიან ფუნქციათა სივრცეზე განსაზღვრული x -ზე გამრავლების ოპერატორი, რომელშიც სკალარული ნამრავლი განმარტებულია ფორმულით:

$$(f,g)=\int_{\mathbf{R}}\mathbf{f}(x)\overline{g}(x)dx,\ f,g\in L.$$

იგი შეესაბამება **R** "გარე ველში წრფეზე მოძრავი ნაწილაკის" კვანტურ მოდელს.

2. *დაკვირვებადი იმპულსი* არის იმავე L სივრცეზე განსაზღვრული $\frac{1}{i}\frac{d}{dx}$ დიფერენციალური ოპერატორი.
3. *კვანტური ოსცილატორის დაკვირვებადი ენერგია* არის L -ზე განსაზღვრული $\frac{1}{2}\left(-\frac{d^2}{dx^2}+x^2\right)$ ოპერატორი.
4. *სპინის დაკვირვებადი პროექცია კვანტური სისტემისათვის* "ნაწილაკი $\frac{1}{2}$-ის ტოლი სპინით" არის ნებისმიერი თვითშეუღლებადი ოპერატორი ორგანზომილებიან უნიტარულ სივრცეში ± 1 საკუთარი მნიშვნელობებით.

დაკვირვებადი ენერგია და სისტემის ევოლუცია დროში. კვანტური სისტემის აღწერაში დაკვირვებადობის **H** სივრცესთან ერთად საჭიროა $H:\mathbf{H}\to\mathbf{H}$ ფუნდამენტური დაკვირვებადი სიდიდის - ენერგიის, *ჰამილტონის ოპერატორის* ანუ *ჰამილტონიანის* მოცემა. მის ტერმინებში კვანტური მექანიკის ბოლო, ჩვენთან კიდევ ერთი მეოთხე პოსტულატი ყალიბდება შემდეგნაირად:

თუ დროის ნულოვანი მომენტისათვის სისტემა იმყოფებოდა $|\psi\rangle$ მდგომარეობაში და დროის შუალედში განვითარდა როგორც იზოლირებული სისტემა (კერძოდ არ შესრულდა გაზომვა), მაშინ დროის t მომენტისათვის სისტემა იქნება $e^{-iHt}=\sum_{n=0}^{\infty}\frac{(-iHt)^n}{n!}:\mathbf{H}\to\mathbf{H}.$

$U(t)=e^{-itH}$ ოპერატორი უნიტარულია და ზოგჯერ ქმედების ფუნქციონალს ან ევოლუციის ოპერატორსაც უწოდებენ. $\{U(t):t\in\mathbf{R}\}$ უნიტარულ ოპერატორთა ერთპარამეტრიანი ჯგუფი სრულად განსაზღვრავს იზოლირებული სისტემის ევოლუციას.

ფიზიკური განზომილებას (ენერგია)×(დრო) ეწოდება *ქმედება.* ექსპერიმენტები საშუალებას იძლევა განისაზღვროს ქმედების უნივერსალური ერთეული - პლანკის მუდმივა $\hbar = 1 \cdot 055 \cdot 10^{-34}$ ჯ.წმ. ჩვენ ზემოთ ვიგულისხმებთ, რომ Ht იზომება $\hbar$ ერთეულებში. ამის ხაზგასასმელად ხშირად ქმედების ფუნქციონალს წერენ $e^{\frac{Ht}{i\hbar}}$ სახით.

კვანტური სისტემის ევოლუციის კანონი აღიწერება შემდეგი დიფერენციალური განტოლებით:

$$\frac{d}{dt}\left(e^{-iHt}\psi\right) = -iH\left(e^{-iHt}\psi\right) \qquad (1.2\text{-}5)$$

თუ $\psi(t)$-თი აღვნიშნავთ $e^{-iHt}\psi$-ს, მაშინ (1) ჩაიწერება შემდეგნაირად:

$$\frac{d\psi}{dt} = iH\psi \qquad (1.2\text{-}6)$$

(1.2-6) განტოლებას ეწოდება *შრედინგერის* განტოლება.

აქვე გავაკეთოთ მნიშვნელოვანი შენიშვნა. არსებობს კვანტური პროცესის ორი კლასი: *ევოლუცია*, შრედინგერის განტოლების თანახმად და *გაზომვა*, რომელიც მიიღება პროექტირების ოპერატორის საშუალებით. მხოლოდ რა ფიზიკური პროცესია ეს უკანასკნელი ცხადი არ არის. რადგან გაზომვის შედეგი ალბათური ხასიათისაა, ამიტომ გაზომვები შემთხვევითი პროცესების თვისებების მატარებელია.

ენერგეტიკული სპექტრი და სისტემის სტაციონალური მდგომა-რეობა. კვანტური სისტემის ენერგეტიკული სპექტრი ეწოდება H ჰამილ-ტონიანის სპექტრს. სტაციონალური მდგომარეობა კი ისეთ მდგომარეობას, რომელიც დროში არ იცვლება. ასეთი მდგომარეობები (სხვები) ინვარიანტულები არიან e^{iHt} ოპერატორის მოქმედების მიმართ, ე.ი. ისინი ამ ოპერატორის ერთგანზომილებიანი საკუთრივი ქვესივრცეებია, რომლებიც იმავდროულად არიან H ოპერატორის საკუთრივი ქვესივრცეები. ჰამილტონიანის E_j საკუთრივ მნიშვნელობებს ეწოდებათ სისტემის *ენერგეტიკული დონეები.* ენერგეტიკულ დონეებს შეესაბამებათ ევოლუციის ოპერატორის $e^{itE_j} = \cos tE_j + i\sin tE_j$ საკუთრივი მნიშვნელობები, რომლებიც დროში იცვლებიან.

თუ H ოპერატორს მარტივი სპექტრი აქვს, მაშინ H მდგომარეობების სივრცეს აქვს ორთონორმირებული ბაზისი, რომელიც სტაციონალური მდგომა-რეობებისაგან შედგება და განისაზღვრებიან $e^{i\psi}$ მამრავლის სიზუსტით. თუ E ენერგეტიკული დონის ჯერადობა 1-ზე მეტია, მაშინ ასეთ დონეს და შესაბამის

მდგომარეობას ეწოდება გადაგვარებული, ხოლო E-ს ჯერადობას - *გადაგვარების ხარისხი.*

ყველა მდგომარეობას, რომელიც შეესაბამება ქვედა დონეს, ე.ი. H-ის უმცირეს საკუთრივ მნიშვნელობას, ეწოდება სისტემის ძირითადი მდგომარეობა. ძირითადი მდგომარეობა ერთადერთია, თუ ქვედა დონე გადაუგვარებელია. ტერმინი ძირითადი მდგომარეობა დაკავშირებულია იმ წარმოდგენასთან, რომლის თანახმადაც კვანტური სისტემის განხილვა როგორც გარე სამყაროსგან იზოლირებული სისტემისა შეუძლებელია: გარკვეული ალბათობით სისტემა გასცემს ან შთანთქავს ენერგიის გარკვეულ პორციას. გარკვეულ პირობებში უფრო ალბათურია, რომ ენერგია დაიკარგება, ვიდრე შეიძინება და ამრიგად, სისტემა მიისწრაფის თავის ქვედა მდგომარეობისაკენ, რომლის მიღწევის შემდეგაც იგი ამ მდგომარეობაში რჩება. ამის გამო არაძირითად მდგომარეობებს ეწოდებათ *აღგზნებული.*

როგორც ზემოთ აღვნიშნეთ კვანტური ოსცილატორის ჰამილტონიანს აქვს სახე: $\frac{1}{2}\left(-\frac{d^2}{dx^2}+x^2\right)$. ხოლო $e^{-\frac{x^2}{2}}\mathrm{H}_n(x)=(-1)^n e^{\frac{x^2}{2}}\frac{d^n}{dx^n}\left(e^{-x^3}\right)$ ფუნქცია არის $-\frac{d^2}{dx^2}+x^2$ ოპერატორის საკუთრივი ვექტორი $-(2n+1)$ საკუთრივი მნიშვნელობით ყოველი $n\geq 0$-თვის, სადაც

$$H_n(x)=(-1)^n e^{x^2}\frac{d^n}{dx^n}\left(e^{-x^2}\right)$$

ერმიტის მრავალწევრია. ჩვენი შემოტანილი ტერმინოლოგიით თუ ვისარგებლებთ, შეგვიძლია ვთქვათ, რომ $e^{-\frac{x^2}{2}}\mathrm{H}_n(x)$ ფუნქციები ქმნიან სტაციონალურ მდგომარეობათა სიმრავლეს $E_n=n+\frac{1}{2}$, $n=1,2,...$ ენერგეტიკული დონეებით. ცოტა უფრო ღრმა ანალიზი გვიჩვენებს, რომ ამ შემთხვევაში ენერგია იზომება $\hbar\omega$ ერთეულებში, სადაც ω არის შესაბამისი კლასიკური ოსცილატორის რხევის სიხშირე. სისტემის მდგომარეობათა აღსაწერად შესაძლებელია არჩეულ იქნეს ისეთი უნიტარული სივრცე, რომლისთვისაც $e^{-\frac{x^2}{2}}\mathrm{H}_n(x)$ ფუნქცია იქნება სტაციონალურ მდგომარეობათა სრული სიმრავლე. როდესაც $u>0$ ოსცილატორი გასცემს $E_n-E_m=\hbar\omega(n-m)$ ენერგიის პორციას და ψ_n მდგომარეობიდან გადავა ψ_m მდგომარეობაში. ელექტრომაგნიტური ველის კვანტური თეორიის თანახმად ეს ნიშნავს $m-n$ ფოტონის გამოსხივებას ω სიხშირით. შებრუნებული პროცესი

ცხადია იქნება $m-n$ ფოტონის შთანთქმა, რომლის დროსაც ოსცილატორი გადავა აგზნებულ ზედა მდგომარეობაში. მნიშვნელოვანია ის ფაქტი, რომ სისტემის მიერ მიღებული ან გაცემული ენერგია $\hbar\omega$-ის მთელი ჯერადი იქნება. ძირითად მდგომარეობაში ოსცილატორს აქვს $\frac{1}{2}\hbar\omega$-ს ტოლი (ცხადია არანულოვანი!) ენერგია, რომლის გადაცემა უკვე აღარ შეიძლება, რადგან უფრო დაბალი დონე ოსცილატორს არ აქვს. კვანტური მოდელებში ელექტრომაგნიტური ველი განიხილება როგორც უსასრულო რაოდენობის ოსცილატორების სუპერპოზიცია, რომლებსაც თავიანთი ω აქვთ. ამიტომ, ძირითად, ვაკუუმის მდგომარეობაში, ველს ექნება უსასრულო ენერგია, მაშინ როდესაც კლასიკური ფიზიკის აზრით მისი ენერგია 0 უნდა იყოს (რადგან მისთვის ენერგიის წართმევა არ შეიძლება, სისტემამ არ შეიძლება რაიმეზე იმოქმედოს).

კვანტური სისტემის მდგომარეობათა ტენზორული ნამრავლი. დავუშვათ $L_1,...,L_p$ სასრულგანზომილებიანი წრფივი სივრცეებია ($\mathbf{R}$-ის ან $\mathbf{C}$-ს მიმართ) და $dim\, L_j = n_j, j = 1,...p.$ $f : L_1 \times ... \times L_p \to L$ ასახვას ეწოდება მრავალწრფივი, თუ f წრფივია ნებისმიერი $a_j \in L_j$ არგუმენტის მიმართ, როდესაც ყველა დანარჩენი ფიქსირებულია.

რომელიმე ფიქსირებული j-თვის აღვნიშნოთ $\{a_{j_k}^{(k)}\}$-თი L_j, $j_k = 1,...,n_j$ სივრცის ბაზისი. განვიხილოთ $a_{j_1}^{(1)} \otimes a_{j_2}^{(2)} \otimes ... \otimes a_{j_p}^{(p)}$ სახის ფორმალური გამოსახულება და მოვჭიმოთ მასზე ვექტორული სივრცე და აღვნიშნოთ $L_1 \otimes ... \otimes L_p$-ით. ამ სივრცის ნებისმიერ ელემენტს აქვს სახე:

$$\sum_{j_1,...,j_p} \alpha_{\alpha_1...\alpha_p} a_{j_1}^{(1)} \otimes a_{j_2}^{1} \otimes ... \otimes a_{j_p}^{(1)}.$$

მტკიცდება, რომ $L_1 \otimes ... \otimes L_p$ არის $n_1 \times n_2 \times ... \times n_p$ განზომილებიანი ვექტორული სივრცე. მას ეწოდება $L_1 \otimes ... \otimes L_p$ ვექტორული სივრცეების ტენზორული ნამრავლი. თუ $L_1 = L_2 ... = L_p$, მაშინ L სივრცის ტენზორული ნამრავლის აღსანიშნავად იხმარება ჩანაწერები $T^p(L)$ და $L^{\otimes p}$.

მაგალითი. დავუშვათ $L = \mathbf{C^2} \otimes \mathbf{C^2}$, $\mathbf{C^2}$-ის თითოეული ეგზემპლარის საბაზისო ელემენტებისათვის შემოვიტანოთ აღნიშვნა: $\{e_1^{(1)}, e_2^{(1)}\}$ და $\{e_1^{(2)}, e_2^{(2)}\}$. მაშინ $\mathbf{C^2} \otimes \mathbf{C^2}$-ის ბაზისი იქნება $e_1^{(1)} \otimes e_1^{(2)}$, $e_1^{(1)} \otimes e_2^{(2)}, e_2^{(1)} \otimes e_1^{(2)}, e_2^{(1)} \otimes e_2^{(2)}$.

თუ $\mathbf{C}^2$-ში ავირჩევთ სტანდარტულ ბაზისს $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, მაშინ $\mathbf{C}^2 \otimes \mathbf{C}^2$ ტენზორული ნამრავლი კანონიკურად იზომორფული იქნება $\mathbf{C}^4$-ის შემდეგი სტანდარტული ბაზისით:

$$|0\rangle \otimes |0\rangle = |0\rangle|0\rangle = |00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |0\rangle \otimes |1\rangle = |0\rangle|1\rangle = |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},$$

$$|1\rangle \otimes |0\rangle = |1\rangle|0\rangle = |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |1\rangle \otimes |1\rangle = |1\rangle|1\rangle = |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

ვთქვათ S_p ჩასმათა ჯგუფია. ყოველ $\sigma \in S_p$ შეესაბამება

$$f_\sigma : \mathrm{T}^p(L) \to \mathrm{T}^p(L)$$

წრფივი ასახვა,რომელიც $a_1 \otimes \ldots \otimes a_p \in \mathrm{T}^p(L)$ ტენზორზე მოქმედებს შემდეგი წესით:

$$f_\sigma(a_1 \otimes \ldots \otimes a_p) = a_{\sigma(1)} \otimes \ldots \otimes a_{\sigma(p)}.$$

$\mathrm{T} \in \mathrm{T}^p(L)$ ტენზორს ეწოდება *სიმეტრიული*, თუ ყოველი $\sigma \in S_p$-სათვის სრულდება ტოლობა: $f_\sigma(\mathrm{T}) = f(\mathrm{T})$. სკალარები (იმ ველის ელემენტები, რომლის მიმართაც L არის ვექტორული სივრცე) ითვლებიან სიმეტრიულ ტენზორებად. აღვნიშნოთ $S^p(L)$-ით $\mathrm{T}^p(L)$-ის ქვესივრცე, რომელიც სიმეტრიული ტენზორებისაგან შედგება.

განვიხილოთ

$$S = \frac{1}{p!} \sum_{\sigma \in S_p} f_\sigma : \mathrm{T}^p(L) \to \mathrm{T}^p(L)$$

სიმეტრიზაციის ოპერატორი. თუ $\{e_{j_1} \otimes \ldots \otimes e_{j_p}\}$ ტენზორები $\mathrm{T}^p(L)$-ის ბაზისია, მაშინ მათი სიმეტრიზაცია $S(e_{j_1} \otimes \ldots \otimes e_{j_p}) \equiv e_{L_1} \ldots e_{i_p}$ წარმოქმნის $S^p(L)$ სიმეტრიულ ტენზორთა სივრცეს.

დებულება 1. 1) $e_{i_1}....e_{i_p}$ ფორმალური ნამრავლი არ იცვლება ინდექსების გადანაცვლებით.

2) $\{e_{i_1}...e_{i_p}\}$ არის $S^p(L)$-ის ბაზისი.

3) $dim\, S^p(L) = \begin{pmatrix} n+p-1 \\ p \end{pmatrix}$;

$\mathrm{T} \in \mathrm{T}^p(L)$ ტენზორს ეწოდება ანტისიმეტრიული, თუ ნებისმიერი $\sigma \in S_p$-სათვის ადგილი აქვს ტოლობას: $f_\sigma(\mathrm{T}) = \varepsilon(\sigma)\mathrm{T}$. აქ $\varepsilon(\sigma)$ არის σ გადასმის ნიშანი. ანტისიმეტრიული ტენზორები ქმნიან $\mathrm{T}^p(L)$-ის ქვესივრცეს.

შემოვიტანოთ კიდევ ერთი ოპერატორი:

$$A = \frac{1}{p!}\sum_{\sigma \in S_p} \varepsilon(\sigma) : \mathrm{T}^p(L) \to \mathrm{T}^p(L).$$

დებულება 2. $A^2 = A$ და $Im\, A = \wedge^p(L)$.

A-ს ეწოდება ანტისიმეტრიზაციის ოპერატორი. შემოვიტანოთ აღნიშვნა:

$$A(e_{i_1} \otimes ... \otimes e_{i_p}) = e_i, \wedge ... \wedge e_{ip} \qquad (1.2\text{-}7)$$

ნიშანი "$\wedge$" აღნიშნავს გარე ნამრავლს. სიმეტრიული ტენზორებისაგან განსხვავებით ანტისიმეტრიული ტენზორი იცვლის ნიშანს (1.2-7)-ის მარჯვენა მხარის ნებისმიერი ვექტორის გადასმის დროს. ამიტომ $e_{i_1} \wedge ... \wedge e_{i_p} = 0,$ თუ $i_k = i_l$ რომელიმე k და l ინდექსებისათვის.

$\wedge^p(L)$ ვექტორული სივრცე წარმოქმნილია $e_{i_1} \wedge ... \wedge e_{i_p}$ სახის ანტისიმეტრიული ტენზორებით, სადაც $1 \le i_1 < i_2 ... < i_p \le n$. აქედან გამოდის, რომ $\wedge^m(L) = 0,$ თუ $m > n = dim\, L.$

დებულება 3. 1) $\{e_{i_1} \wedge ... \wedge e_{i_p}\}$, $1 \le i_1 < i_2 < ... < i_p \le n$ არის $\wedge^p(L)$-ის ბაზისი.

2) $dim \wedge^p(L) = \begin{pmatrix} n \\ p \end{pmatrix}$,

3) $dim \oplus \wedge^p \left(L\right)_{p=0}^{n} = 2^n.$

დავუშვათ $\mathbf{H}_1, ..., \mathbf{H}_n$ კვანტური სისტემების მდგომარეობის სივრცეებია. მაშინ იმ სისტემის მდგომარეობის სივრცე, რომელიც ამ სისტემის გაერთიანებით

მიიღება არის $\mathbf{H}_1 \otimes .... \otimes \mathbf{H}_n$ ტენზორული ნამრავლის რაიმე ქვესივრცე. ეს დებულება არის კვანტური მექანიკის რიგით *მეხუთე* პოსტულატი. ჩვენ განვიხილავთ ისეთ სისტემებს, რომლისთვისაც $\mathbf{H}_i$ სასრულგანზომილებიანია და

$$\mathbf{H} = \mathbf{H}_1 = ... = \mathbf{H}_n .$$

ვთქვათ $\psi_i \in \mathbf{H}_i$ ქვესისტემის რაიმე მდგომარეობაა, მაშინ $\psi_1 \otimes ... \otimes \psi_n$ მდგომარეობა არის გაერთიანებული კვანტური სისტემის ერთ-ერთი შესაძლო მდგომარეობა. იგი შეესაბამება იმ შემთხვევას, როდესაც ყოველი ქვესივრცე იმყოფება თავის ψ_i მდგომარეობაში, მაგრამ $\psi_1 \otimes ... \otimes \psi_n$ სახის ვექტორები არ ამოწურავენ მთელ $\mathbf{H}_1 \otimes .... \otimes \mathbf{H}_n$-ს რადგან ეს სივრცე შეიცავს კიდევ მათ წრფივ კომბინაციებს (მდგომარეობათა სუპერპოზიციას). როდესაც გაერთიანებული სისტემა იმყოფება ერთ-ერთ ასეთ "დაუშლად" მდგომარეობაში, მათი ქვესისტემების ცნება აზრს კარგავს, რადგან ისინი (ქვესივრცეები) და მათი მდგომარეობები ცალსახად ვერ გამოიყოფიან. სხვა სიტყვებით, ქვესისტემების მდგომარეობათა უმრავლესობა გაერთიანებულ სისტემაში იმყოფება ვირტუალურ მდგომარეობაში. ასეთ მდგომარეობებს *გადაბლართული* მდგომარეობები (Entangled states) ეწოდებათ.

აინშტაინს, როზენსა და პოდოლსკის ეკუთვნის შემდეგი წარმოსახვითი ექსპერიმენტი: ვთქვათ გაერთიანებული სისტემის ორად გაყოფის შემდეგ ეს ქვესისტემები საკმაო მანძილით დავაშორეთ ერთმანეთს. ერთ-ერთ სისტემაზე გაზომვის ჩატარება მეორე სისტემას "ელვისებურად" გადაიყვანს რაიმე განსაზღვრულ მდგომარეობაში, მაშინ როდესაც კლასიკური მექანიკის თვალსაზრისით ამ პროცესს გარკვეული არანულოვანი დროის ინტერვალი ჭირდება. კვანტური სისტემის ეს თვისება უდევს საფუძვლად კვანტურ ტელეპორტაციას, რომელიც მოცემულ მომენტში განიხილება როგორც ინფორმაციის კვანტური თეორიის ნაწილი და კომუნიკაციის თვისობრივად ახალ შესაძლებლობებს იძლევა.

თუ გაერთიანებულ სისტემაში ქვესისტემები ერთმანეთთან არ ურთიერთქმედებენ და თითოეული ქვესისტემის ჰამილტონიანს აღვნიშნავთ $H_i : \mathbf{H}_1 \to \mathbf{H}_i$-ით, მაშინ გაერთიანებული სისტემის ჰამილტონიანი იქნება:

$$H_1 \otimes id \otimes ... \otimes id + id \otimes H_2 \otimes ... \otimes id + ... + id \otimes id \otimes ... \otimes H_n ,$$

სადაც $id : \mathbf{H}_i \to \mathbf{H}_i$ იგივური ოპერატორია. თუ გაერთიანებულ კვანტურ სისტემას ასეთი ჰამილტონიანი აქვს და დროის საწყის მომენტში იმყოფებოდა $\psi_1 \otimes ... \otimes \psi_n$ მდგომარეობაში, მაშინ დროის t მომენტისათვის იგი აღმოჩნდება $e^{-i\mathrm{H}_1 t}(\psi_1) \otimes ... \otimes e^{i\mathrm{H}_n t}(\psi_n)$ მდგომარეობაში, რაც იმას ნიშნავს, რომ ქვესისტემები

განვითარდნენ ერთმანეთისაგან დამოუკიდებლად. ზოგად შემთხვევაში გაერთიანებული სისტემის ჰამილტონიანი არის თავისუფალი ნაწილისა (რომელიც უკვე აღვწერეთ, ე.ი. ჰამილტონიანი სისტემისა ურთიერთქმედების გარეშე) და ისეთი ოპერატორის ჯამი, რომელიც ურთიერთქმედებას შეესაბამება.

თუ n ეგზემპლარი სისტემის გაერთიანებული სივრცე არის $S^n(\mathbf{H})$ სიმეტრიულ ტენზორთა სივრცე, მაშინ $\mathbf{H}$-ს ეწოდება *ბოზონი*. ბოზონები არიან ფოტონები და ალფა ნაწილაკები.

კვანტურ სისტემას, რომლის მდგომარეობათა სივრცეა $\mathbf{H}$ ეწოდება *ფერმიონები*, თუ n ეგზემპლარი გაერთიანებული სისტემის მდგომარეობათა სივრცე არის $\wedge^n(\mathbf{H})$-ი. ფერმონებია ელექტრონები, პროტონები, ნეიტრონები.

დავუშვათ $\{\psi_1,...,\psi_m\}$ ბოზონური ან ფერმიონული სისტემის მდგომარეობათა სივრცის ბაზისია, მაშინ $S^n(\mathbf{H})$-ისა და $\wedge^p(\mathbf{H})$-ის ბაზისები შესაბამისად იქნება:

$$\left|a_1,...,a_m\right\rangle = \begin{cases} S\left(\underbrace{\psi_1 \otimes ...\psi_1}_{k_1} \otimes ..... \otimes \psi_m \otimes .... \otimes \underbrace{\psi_m}_{k_m}\right), & S^n(\mathbf{H}) - \text{ში.} \\ A\left(\underbrace{\psi_1 \otimes .... \otimes \psi_1}_{k_1} \otimes ... \otimes \psi_m \otimes ... \otimes \underbrace{\psi_m}_{k_m}\right), & \wedge^n(\mathbf{H}) - \text{ში.} \end{cases}$$

სადაც $k_1 + ... + k_m = n$. ბოზონებისათვის k_j რიცხვები ღებულობენ ნებისმიერ არაუარყოფით მნიშვნელობას, ხოლო ფერმიონებისათვის მხოლოდ 0-სა და 1-ს, $\wedge^p(\mathbf{H})$-ს ელემენტების ანტისიმეტრიულობის გამო. ამ უკანასკნელის კვანტურ-მექანიკური ინტერპრეტაცია ასეთია: *ორი ქვესისტემა არ შეიძლება იმყოფებოდეს ერთსა და იმავე მდგომარეობაში.* ეს დებულება ცნობილია პაულის *"აკრძალვის პრინციპის "* სახელწოდებით.

გადახლართული მდგომარეობა. როგორც ზემოთ აღვნიშნეთ, $\mathbf{H}_1 \otimes ... \otimes \mathbf{H}_n$ მდგომარეობათა სივრცის ტენზორულ ნამრავლში არსებობენ ისეთი მდგომარეობები, რომლებიც არ წარმოიდგინებიან თითოეული სისტემის მდგომარეობების ტენზორული ნამრავლის სახით, ე.ი. არსებობს ისეთი $|\psi> \epsilon \mathbf{H}_1 \otimes ... \otimes \mathbf{H}_n$, რომ $|\psi> = |\psi_1> \otimes |\psi_2> \otimes ... \otimes |\psi_n>$ ტოლობა არ სრულდება არც ერთი $|\psi_i> \epsilon \mathbf{H}_i$ მდგომარეობისათვის. ასეთ მდგომარეობას ეწოდება *გადახლართული* მდგომარეობა. ვთქვათ, $R: \mathbf{H}_1 \otimes ... \otimes \mathbf{H}_n \to \mathbf{H}_1 \otimes ... \otimes \mathbf{H}_n$ ისეთი უნიტარული ოპერატორია, რომ $R|\psi>$ გადახლართული მდგომარეობაა რომელიმე $|\psi>$-სათვის, ასეთ შემთხვე-

ვაში R-ს ეწოდება *გადახლართვის ოპერატორი.* დავუშვათ $\mathbf{H}_1 = \ldots = \mathbf{H}_n = \mathbf{C^2}$ და დავახასიათოთ $\mathbf{C^2} \otimes \mathbf{C^2} \to \mathbf{C^2} \otimes \mathbf{C^2}$ გადახლართვის ოპერატორები.

განმარტება. $(R\otimes I)(I\otimes R)(R\otimes I) = (I\otimes R)(R\otimes I)(I\otimes R)$ სახის განტოლებას, სადაც უცნობია $R\colon \mathbf{C^2} \otimes \mathbf{C^2} \to \mathbf{C^2} \otimes \mathbf{C^2}$ ოპერატორი, ხოლო $I\colon \mathbf{C^2} \to \mathbf{C^2}$ იგივური ოპერატორია, ეწოდება *იანგ-ბაქსტერის* განტოლება.

აღმოჩნდა, რომ იანგ-ბაქსტერის განტოლების ის ამონახსნები, რომლებიც უნიტარული ოპერატორებია, მხოლოდ სამი სახისაა და ყველა დანარჩები მისი მსგავსია. ეს ამონახსნებია:

$$R_1 = \begin{pmatrix} 1/\sqrt{2} & 0 & 0 & 1/\sqrt{2} \\ 0 & 1/\sqrt{2} & -1/\sqrt{2} & 0 \\ 0 & 1/\sqrt{2} & 1/\sqrt{2} & 0 \\ -1/\sqrt{2} & 0 & 0 & 1/\sqrt{2} \end{pmatrix},\ R_2 = \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & 0 & b & 0 \\ 0 & c & 0 & 0 \\ 0 & 0 & 0 & d \end{pmatrix},$$

$$R_3 = \begin{pmatrix} 0 & 0 & 0 & a \\ 0 & b & 0 & 0 \\ 0 & 0 & c & 0 \\ d & 0 & 0 & 0 \end{pmatrix}.$$

სადაც a, b, c, d კომპლექსური რიცხვებია მოდულით ერთი.

კრიტერიუმი. $|\psi> \in \mathbf{C^2} \otimes \mathbf{C^2}$ მდგომარეობა გადახლართულია მაშინ და მხოლოდ მაშინ, როდესაც $\mathbf{C^2} \otimes \mathbf{C^2}$-ის $|00>, |01>, |10>, |11>$ სტანდარტულ ბაზისში მისი $|\psi> = a|00> + b|01> + c|10> + d|11>$ სახით წარმოდგენის დროს $ad - bc \neq 0$.

იანგ-ბაქსტერის განტოლების ზემოთ მოყვანილი ამონახსნები და ეს კრიტერიუმი საშუალებას იძლევა "აღმოვაჩინოთ" გადახლართული მდგომარეობები და ავაგოთ გადახლართვის ოპერატორები. მაგალითად, იანგ-ბაქსტერის განტოლების R_1 ამონახსნი არის გადახლართვის ოპერატორი. მისი მოქმედება $\mathbf{C^2} \otimes \mathbf{C^2}$-ის სტანდარტულ ბაზისზე იძლევა გადახლართულ მდგომარეობებს, რომლებსაც *ბელის ბაზისი* ეწოდება. რაც შეეხება R_2 და R_3 ამონახსნებს, ისინი გადახლართვის ოპერატორები არიან მაშინ და მხოლოდ მაშინ, როდესაც $ad - bc \neq 0$. არ ჩავღრმავდებით დეტალებში, მხოლოდ აღვნიშნავთ, რომ იანგ-ბაქსტერის განტოლების ამონახსნი, ე.წ. R-მატრიცი, ერთ-ერთი ცენტრალური ობიექტია ტოპოლოგიური კვანძების თეორიაში. ჩვენს კონტექსტში

მხოლოდ ასეთი შედარებით შემოვიფარგლებით: *კვანტური გადაჯაჭვა უფრო ძლიერია, ვიდრე ტოპოლოგიური.*

3. შებრუნებადი (შექცევადი) გამოთვლები და კვანტური სქემები.

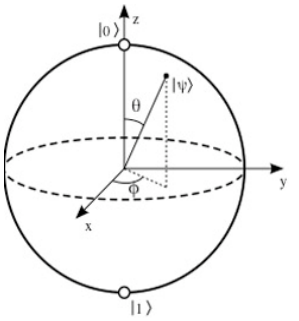
დეტერმინირებული გამოთვლითი მოწყობილობის შებრუნებადობა (შექცევადობა) შესავალი და გამოსავალი მონაცემების ცალსახად აღდგენის თვისებაა. მოწყობილობის ასეთ თვისებას ეწოდება ლოგიკური შებრუნებადობა. თუ დამატებით შესაძლებელია ლოგიკურად შებრუნებადმა მოწყობილობამ იმუშაოს შებრუნებულად დროში (უკუ მიმართულებით), მაშინ მას ეწოდება ფიზიკურად შებრუნებადი. ამ დროს თერმოდინამიკის მეორე კანონის თანახმად არ გასცემს ტემპერატურას.

შებრუნებადი გამოთვლებით დაინტერესდნენ მას შემდეგ, რაც დაისვა კითხვა: *რა რაოდენობის ენერგიაა საჭირო გამოთვლებისათვის?* ანალიზმა აჩვენა, რომ ენერგიის დანაკარგი თითქმის ნულია გამოთვლებისათვის საჭირო იმ ოპერაციებისათვის, რომლებიც შებრუნებადნი არიან. როდესაც სრულდება შეუბრუნებადი ოპერაცია, მაგალითად ბიტის წაშლა, ბიტის ორი განსხვავებული მდგომარეობა 0 და 1, ხდება 0-ის ტოლი. მიკროსამყაროს ფიზიკური კანონები შებრუნებადნი არიან, ამიტომ ძველ მდგომარეობას (0 და 1) შორის განსხვავება შენახული უნდა იქნას არაკონტროლირებად ფიზიკურ თავისუფლების ხარისხში. ეს ნიშნავს, რომ ენტროპია გაიზარდა, რაც ბუნებაში სითბოს გამოყოფის სახით შეიმჩნევა. ენერგია, რომელიც ერთი ბიტი ინფორმაციის წაშლას ჭირდება, ძალიან მცირე სიდიდეა, დაახლოებით *kT*, მაგრამ მაინც სასრული და ნულისაგან განსხვავებული რიცხვია. წაშლის ოპერაციის შეუბრუნებადობის გამო, ერთ გიგაბაიტიანი მყარი დისკის დაფორმატებას 3×10^{-11} ჯოული ენერგია ჭირდება, ეს კი შეესაბამება იმ ენერგიის დანახარჯს, რაც ესაჭიროება დისკის თავურის გადაადგილებას წყალბადის ატომის დიამეტრის ნახევარზე. რაც, რა თქმა უნდა რამდენიმე რიგით მცირეა, ვიდრე ფორმატირების დროს თავურის რეალური გადაადგილება. მეორეს მხრივ, თუ მყარი დისკის მოცულობის ზრდის დღევანდელი ტემპი იქნა შენარჩუნებული კიდევ სამი საუკუნე, მაშინ ასეთი დისკის დაფორმატებას ოცდამესამე საუკუნის ბოლოს დაჭირდება მზის წლიური ენერგიის ტოლი ენერგია. ეს იმას ნიშნავს, რომ ოპერაციის ლოგიკური შეუბრუნებადობა ფიზიკური პროცესია და დაკავშირებულია ენერგიის დისიპაციასთან.

კლასიკური გამოთვლებისათვის საჭირო ელემენტარული გეიტებიდან შებრუნებადი ოპერაციაა მხოლოდ *NOT*. ქვემოთ ჩვენ ავაგებთ შებრუნებადი გეიტების უნივერსალურ სისტემას და ვაჩვენებთ, რომ სტანდარტულ ბაზისში

გამოთვლადი ნებისმიერი ფუნქცია გამოთვლადია ახალ, შებრუნებადი ოპერაციებისაგან შედგენილ ბაზისშიც.

როგორც აღნიშნეთ, კლასიკურ კომპიუტერში მეხსიერების ელემენტი იმყოფება ორი შესაძლო მდგომარეობიდან ერთ-ერთში, ანუ სხვანაირად რომ ვთქვათ, სისტემის მდგომარეობა აღიწერება ორ ელემენტიანი $\{0,1\}$ სიმრავლით. ორმდგომარეობიანი კვანტული სისტემის მდგომარეობათა სივრცე კი აღიწერება 2-განზომილებიანი კომპლექსური სივრცით.



ქუბიტი

განვიხილოთ $\boldsymbol{C}^2$ ორგანზომილებიანი სივრცე კანონიკური $\{|0\rangle,|1\rangle\}$ ბაზისით და ვუწოდოთ მას ქუბიტების (კვანტური ბიტების) სივრცე (ჩვენი აზრით, ტერმინი ქუბიტი პირველად იხმარა ბ.შუმახერმა თავის ნაშრომში "Quantum Coding". *Phys.Rev. 1995, vol. A51, N 4, pp.2738-1747*). მოსახერხებელია აღვნიშნოთ იგი $\mathbf{P}$-თი. კვანტურ სისტემას, რომელიც n რაოდენობის ქუბიტებისაგან შედგება, ე.ი. $\mathbf{P}\otimes\ldots\otimes\mathbf{P}=\mathbf{P}^{\otimes n}$ ვუწოდოთ n სიგრძის ან *n-რეგისტრი*. მაგალითად, ელექტრონი მუდმივ ელექტრომაგნიტურ ველში არის ქუბიტის მაგალითი. მართლაც, ელექტრონის სპინი ორი $|0>,|1>$ შესაძლო მდგომარეობიდან ერთ-ერთში დაიმზირება გაზომვის შემდეგ. მეორეს მხრივ, იგი არის კვანტური დინამიური სისტემა, რომლის ევოლუციაც დროში $U:\mathbf{C}^2\to\mathbf{C}^2$ უნიტარული ოპერატორით აღიწერება. ხოლო n ქუბიტის დინამიკა კი $(C^2)^{\otimes n}\to(C^2)^{\otimes n}$ სივრცეზე მოქმედი ოპერატორით.

დავუშვათ n-სიგრძის რეგისტრში A ქუბიტების რაიმე სიმრავლეა. განვიხილოთ ოპერატორი რომელიც ამ რეგისტრის A ქვესიმრავლეზე მოქმედებს როგორც U უნიტარული ოპერატორი, ხოლო დანარჩენებზე კი როგორც იგივური. აღვნიშნოთ ეს ოპერატორი $U(A)$-თი. მაგალითად,

$U[1,...,r]=U\otimes I$, სადაც U მოქმედებს პირველ r ქუბიტზე, ხოლო დანარჩენებზე მოქმედებს იგივური ოპერატორი. განვიხილოთ კიდევ ერთი მაგალითი: $H[2]:\mathbf{P}^{\otimes 3}\to\mathbf{P}^{\otimes 3}$, სადაც $H=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$. $H[2]$ სამი ქუბიტიდან მხოლოდ მეორეზე მოქმედებს როგორც H ოპერატორი, ხოლო დანარჩენებზე კი როგორც იგივური. ამრიგად,

$$H[2]=I\otimes H\otimes I=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\otimes\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\otimes\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}=$$

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

განმარტება. *(კვანტური სქემა)* დავუშვათ $\mathfrak{I}$ უნიტარულ ოპერატორთა რაიმე სიმრავლეა. ვუწოდოთ მას ბაზისი. $\mathfrak{I}$ ბაზისში კვანტური სქემა არის $U_l[A_l],...,U_l[A_l]$ უნიტარული ოპერატორების მიმდევრობა, სადაც A_j ბაიტების რაიმე სიმრავლეა, ხოლო $U_j\in\mathfrak{I}$.

$U:\mathbf{P}^{\otimes n}\to\mathbf{P}^{\otimes n}$ ოპერატორს ეწოდება რეალიზებადი კვანტურ სქემაში, თუ $U=U_l[A_l]..U_l[A_l]$.

ზემოთ მოყვანილი განმარტება არ შეიცავს გამოთვლების დროს დამატებითი მეხსიერების გამოყენებას, ამიტომ საჭიროა გავაფართოოთ ოპერატორების რეალიზების ცნება. U ოპერატორს ეწოდება *ზოგადი კვანტური სქემით რეალიზებადი*, თუ $W=U_l[A_l]..U_l[A_l]$ ოპერატორი მოქმედებს N ქუბიტზე $N\geq n$, ისე, რომ ნებისმიერი $|\xi\rangle\in\mathbf{P}^{\otimes n}$-თვის ადგილი აქვს ტოლობას:

$$W\left(|\xi\rangle\otimes\left|0^{N-n}\right\rangle\right)=\left(U|\xi\rangle\right)\otimes\left|0^{N-n}\right\rangle.$$

კლასიკური ობიექტი, რომელიც შეესაბამება უნიტარულ ოპერატორს არის გადასმა. პირიქით, ნებისმიერ $G : \boldsymbol{B}^{k} \to \boldsymbol{B}^{k}$ გადასმას ბუნებრივად ეთანადება $\hat{G}$ უნიტარული ოპერატორი განმარტებული ტოლობით: $\hat{G}|x\rangle = |Gx\rangle$.

კვანტური სქემის ანალოგიურად, შესაძლებელია განვმარტოთ შებრუნებადი კლასიკური სქემები, რომლებიც ახდენენ გადასმების რეალიზაციას.

შებრუნებადი კლასიკური სქემა. დავუშვათ $\mathfrak{I}$ გადასმების $G : \boldsymbol{B}^{k} \to \boldsymbol{B}^{k}$ სიმრავლის რაიმე ქვესიმრავლეა, ვუწოდოთ მას ბაზისი. შებრუნებადი კლასიკური სქემა $\mathfrak{I}$ ბაზისში არის $U_l[A_l],...,U_l[A_l]$ გადასმების მიმდევრობა, სადაც A_j ბიტების სიმრავლეა, ხოლო $U_j \in \mathfrak{I}$.

გადასმა, რომელიც რეალიზებადია შებრუნებადი სქემით არის $U_l[A_l]..U_l[A_l]$ გადასმების ნამრავლი.

U გადასმა, რომელიც რეალიზებადია ზოგადი შებრუნებული სქემით ისეთი გადასმაა, რომ გადასმების ნამრავლი $W = U_l[A_l]..U_l[A_l]$ მოქმედებს N ბიტზე ($N \geq n$) და ნებისმიერი x-თვის $\boldsymbol{B}^{n}$-დან აკმაყოფილებს პირობას:

$$W(x,0^{N-n}) = (Ux,0^{N-n}).$$

ჩვენი მიზანია გავარკვიოთ, თუ რა შემთხვევაშია შესაძლებელი ბულის სქემით რეალიზებული ფუნქციის რეალიზაცია შებრუნებადი სქემით.

როგორც აღვნიშნეთ, შებრუნებული სქემების საშუალებით შესაძლებელია მხოლოდ გადასმების მიღება. ნებისმიერი $f : \boldsymbol{B}^{n} \to \boldsymbol{B}^{m}$ ფუნქციის გამოსათვლელად საჭიროა გამოვთვალოთ $F : \boldsymbol{B}^{n+m} \to \boldsymbol{B}^{n+m}$ ფუნქცია, რომელიც მოცემულია შემდეგი სახით:

$$F(x,y) = (x, y \oplus f(x)),$$

სადაც $\oplus$ არის $mod\,2$-ით შეკრება. მაშინ f-ის მნიშვნელობა მოიცემა შემდეგნაირად $F(x,0) = (x, f(x))$. F-ის მაგივრად შემდეგში ჩვენ ვიხმართ აღნიშვნას $f_{\oplus}$.

სტანდარტულ ბაზისში ბულის სქემით მოცემული ფუნქციის გამოსათვლელად საკმარისი არ არის ავიღოთ შებრუნებადი სქემა ისეთი ბაზისით, რომელიც ორი ბიტის გადასმაა, რადგან ორი ბიტის ნებისმიერი გადასმა $g : \boldsymbol{B}^{2} \to \boldsymbol{B}^{2}$ არის წრფივი ფუნქცია: $g(x,y) = (ax \oplus by \oplus c, dx \oplus ey \oplus f)$, სადაც $a,b,d,e,f \in \mathbf{Z}_2$, აქედან ყველა ფუნქცია რომელიც გამოითვლება შებრუნებადი სქემით ორი ბიტის გადასმით მიღებულ ბაზისში, არის წრფივი, ხოლო

თუ ავიღებთ შებრუნებად სქემას ბაზისით, რომელიც შედგება სამი ბიტის გადასმისაგან, ეს საკმარისი აღმოჩნდება ნებისმიერი ფუნქციის გამოსათვლელად. კერძოდ, საკმარისია შებრუნებადი სქემის ბაზისად ავიღოთ ორი ფუნქცია: უარყოფა და *ტოფოლის* $\mathrm{T} : \boldsymbol{B}^3 \to \boldsymbol{B}^3$ ელემენტი, განმარტებული შემდეგნაირად:

$$\mathrm{T} : (x, y, z) \mapsto (x, y, z \oplus xy),$$

რომ ადგილი ჰქონდეს ნებისმიერი ოპერატორის ზოგადი სქემით რეალიზაციას.

ჩამოვაყალიბოთ ზემოთ მოყვანილი დებულება ზუსტად და მოვიყვანოთ მისი დამტკიცება.

თეორემა. ნებისმიერი $F : \boldsymbol{B}^n \to \boldsymbol{B}^m$ ფუნქცია რეალიზებადია შებრუნებადი სქემით $\{NOT, \mathrm{T}\}$ გადასმების ბაზისში. ანუ სხვა სიტყვებით გეიტების $\{NOT, \mathrm{T}\}$ სიმრავლე შებრუნებადი გამოთვლებისათვის სრული ბაზისია.

თეორემის დასამტკიცებლად გამოვიყენებთ შემდეგ ლემებს:

ლემა 1. დავუშვათ $F : \boldsymbol{B}^n \to \boldsymbol{B}^m$ ფუნქცია რეალიზებადია L ზომის ბულის სქემის საშუალებით $\mathfrak{I}$ ბაზისში, მაშინ შესაძლებელია $(x,0) \to (F(x, G(x)))$ ფუნქციის რეალიზება შებრუნებადი სქემის საშუალებით ისეთ $\mathfrak{I}_\oplus$ ბაზისში, რომელიც შედგება ისეთი $f_\oplus$, $f \in \mathfrak{I}$ და $\hat{\oplus} : (x, y) \mapsto (x, x \oplus y)$ ფუნქციებისაგან.

შენიშვნა. თეორემაში მითითებული $G(x)$ ფუნქცია ჩვენ არ გვჭირდება, იგი "უსარგებლო ინფორმაციაა".

ლემის დამტკიცება. განვიხილოთ F-ის გამოსათვლელი ბულის სქემა. დავუშვათ $x_1, \ldots, x_n$ შესავალი ცვლადებია. დავუშვათ სქემის დამხმარე ცვლადები და შედეგის ბიტებია $x, x_{n+1}, \ldots, x_{n+L}$. შებრუნებად სქემაში მათ შევუსაბამოთ დამატებითი ბიტები, რომლებიც იმყოფებიან ნულოვან საწყის მდგომარეობაში. დავუშვათ სქემაში ყოველ მინიჭებას აქვს სახე: $x_{n+k} = f_k(x_{j_k}, \ldots x_{l_k})$, სადაც $f_k \in \mathfrak{I},\ j_k, \ldots, l_k < n + k$.

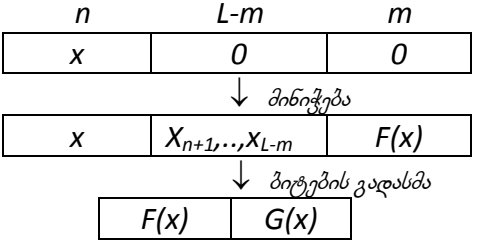
შებრუნებად სქემაში მინიჭებას ანხორციელებს გადასმა:

$$(x_{j_k}, \ldots, x_{l_k}, x_{n+k}) := (f_k)_\oplus (x_{j_k}, \ldots, x_{l_k}, x_{n+k}),$$

ე.ი. $x_{n+k} := x_{n+k} \oplus f_k(x_{j_k}, \ldots, x_{l_k})$.

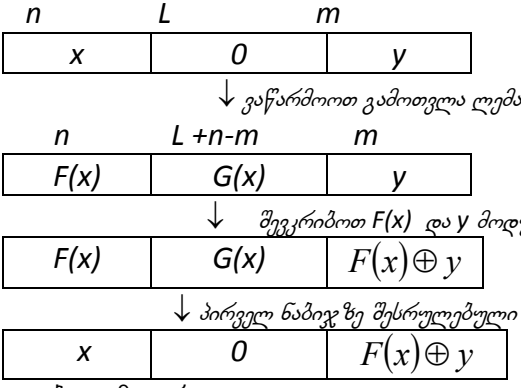
ამრიგად, თუ დამატებითი ცვლადების საწყისი მნიშვნელობა იყო 0-ის ტოლი, მათი საბოლოო მნიშვნელობა ისეთივე იქნება, როგორც იყო ბულის სქემაში. ამის შემდეგ საკმარისია ბიტებს ადგილები შევუცვალოთ, რომ მივიღოთ ლემის

დამტკიცება. სქემატურად ზემოთ მოყვანილი მსჯელობა გამოისახება შემდეგნაირად:



ლემა 2. ლემა 1-ის პირობების შესრულების შემთხვევაში შესაძლებელია $F_{\oplus}$ ფუნქციის გამოთვლა $O(L+n+m)$ ზომის შებრუნებადი სქემის საშუალებით.

ლემის დასამტკიცებლად საკმარისია $G(x)$ - უსასრულო ინფორმაციის მოსპობა, რის გასაკეთებლად ჩვენ გამოვიყენებთ სქემის შებრუნებადობას. $F_{\oplus}$-ს გამოთვლის პროცესი სქემატურად გამოისახება შემდეგნაირად:



ამით ლემის დამტკიცება დამთავრდა.

თეორემის დამტკიცება. რადგან $\{NOT, OR\}$ არის სრული ბაზისი, ეს ნიშნავს, რომ ნებისმიერი $F : \mathbf{B^n} \to \mathbf{B^m}$ ფუნქცია რეალიზებადია ბულის სქემის საშუალებით ამ ბაზისში. გამოვიყენოთ ლემა 1 და ლემა 2, მაშინ F შესაძლებელია რეალიზებული იქნას შებრუნებადი სქემით $\{NOT_{\oplus}, OR_{\oplus}, \sum_{\oplus}\}$ ბაზისში, ხოლო $OR_{\oplus}$ და $\sum_{\oplus}$ გეიტები კი გამოისახებიან ტოფოლის ელემენტების საშუალებით. ამით თეორემა დამტკიცებულია.

4. ელემენტარული გეიტები კვანტური გამოთვლებისათვის

კვანტური სქემა. როგორც ვნახეთ კვანტური სქემები ხორციელდება უნიტარული ოპერატორების საშუალებით. უნიტარული ოპერატორების უსასრულო რაოდენობა არსებობს, ამიტომ ბაზისი ან უსასრულო რაოდენობისაგან უნდა შედგებოდეს, ან უარი უნდა ვთქვათ ოპერატორის ზუსტად რეალიზებადობაზე და შევცვალოთ იგი მიახლოებითი წარმოდგენით.

ჩვენი შემდგომი მსჯელობა ამ საკითხებთან იქნება დაკავშირებული. პირველ რიგში ჩვენ შემოვიტანთ ოპერატორთა მნიშვნელოვან კლასს - *ოპერატორებს კვანტური მართვით* (მართვას ანხორციელებს პირველი ქუბიტი), შემდეგნაირად:

$$\wedge(U)|0\rangle\otimes|\xi\rangle=|0\rangle\otimes|\xi\rangle,$$
$$\wedge(U)|1\rangle\otimes|\xi\rangle=|1\rangle\otimes U|\xi\rangle.$$

ანალოგიურად, ნებისმიერი k-თვის განიმარტება ოპერატორი:

$$\wedge^k(u)|x_1,\ldots,x_k\rangle\otimes|\xi\rangle=\begin{cases}|x_1,\ldots,x_k\rangle\otimes|\xi\rangle, & \text{თუ } x_1\ldots x_n=0,\\ |x_1,\ldots,x_k\rangle\otimes U|\xi\rangle, & \text{თუ } x_1\ldots x_n=1.\end{cases}$$

მაგალითი. ვთქვათ $\sigma^x=\begin{pmatrix}0&1\\1&0\end{pmatrix}$. NOT ფუნქციას შევუსაბამოთ ოპერატორი $\sigma^x=\widehat{NOT}$, მაშინ $\Lambda(\sigma^x)=\hat{\sum}_{\oplus}$, ხოლო $\Lambda^2(\sigma^x)=\hat{T}$, ამ უკანასკნელს ვუწოდოთ *ტოფოლის კვანტური ელემენტი.*

ქვემოთ ვნახავთ, რომ ტოფოლის კვანტური ელემენტი შესაძლებელია მიღებული იქნას ორ ქუბიტზე მოქმედი ოპერატორების საშუალებით.

გავაკეთოთ რამდენიმე შენიშვნა წრფივი ალგებრიდან. $U(2)$ უნიტარული ჯგუფი მოქმედებს 3-განზომილებიან ევკლიდურ სივრცეზე. ამ მოქმედების აღსაწერად შევნიშნოთ, რომ 2×2-მატრიცები ნულოვანი კვალით ქმნიან 3-განზომილებიან ევკლიდურ სივრცეს $\langle X|Y\rangle=\frac{1}{2}\mathrm{Tr}(XY)$ სკალარული ნამრავლით. ამ სივრცის ორთონორმირებული ბაზისია პაულის მატრიცები:

$$\sigma^x=\begin{pmatrix}0&1\\1&0\end{pmatrix},\quad \sigma^y=\begin{pmatrix}0&-i\\1&0\end{pmatrix},\quad \sigma^z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}.$$

$U\in SU(2)$ უნიტარული ოპერატორი მასზე მოქმედებს შემდეგნაირად:

$$U: G\to UGU^{-1}$$

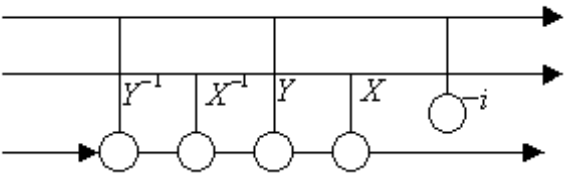
მტკიცდება, რომ ეს მოქმედებები განსაზღვრავს იზომორფიზმს:

$$U(2)/U(1) \cong SO(3),$$

სადაც $U(1)$ არის ფაზის ძვრების ქვეჯგუფი, ხოლო $SO(3)$ კი მობრუნებების ჯგუფია სამგანზომილებიან სივრცეში. ე.ი. ორთოგონალური გარდაქმნების ჯგუფი დეტერმინანტით 1. ამასთან σ^x შეესაბამება 180°-ით x ღერძის მობრუნებას კოორდინატთა სათავის მიმართ. შემოვიტანოთ მატრიცები

$$X = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}, \qquad Y = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

მაშინ, X შეესაბამება x-ის 90°-ით მობრუნება, ხოლო Y-ს კი y ღერძის მობრუნება 180°-ით. რადგან $XYX^{-1}Y = i\sigma^x$, შემდეგი სქემა



სქემა 1

გამოითვლის ტოფოლის ელემენტს $\wedge(X)$, $\wedge(Y)$ და $\wedge^2(-i)$ მმართველი ოპერატორების საშუალებით. შევნიშნოთ, რომ $\wedge^2(-i)$ არის ორი ბიტით მართული ფაზური ძვრა (i-ზე გამრავლება).

ქვემოთ მოყვანილი ორი დებულება საბაზისო გეიტების აგების საშუალებას იძლევა.

დებულება 1. ტოფოლის კვანტური ელემენტის საშუალებით შესაძლებელია საბაზისო ვექტორების გადასმა დამატებითი მეხსიერების გამოყენებით.

დებულება 2. ნებისმიერი k-თვის შესაძლებელია $\wedge^k(U)$ ოპერატორის რეალიზება ისე, რომ ოპერატორი ვამოქმედოთ მხოლოდ 2 ქუბიტზე.

ახლა გადავიდეთ სასრული ბაზისის აღწერაზე. ამ დროს გამოთვლებისათვის საჭირო ოპერატორის რეალიზაცია ხდება მიახლოებით საბაზისო ოპერატორების საშუალებით. ჩვენ შეგახსენებთ, რომ $|x\rangle$ მდგომარეობის ნორმა განმარტებით არის $\||x\rangle\| = \sqrt{\langle x|x\rangle}$. U ოპერატორის ნორმა კი მრავალი სახით შეიძლება იქნას შემოტანილი. ჩვენ გამოვიყენებთ ე.წ. ოპერატორულ ნორმას:

$$\|U\| = \sup_{|x\rangle \neq 0} \frac{\||U|x\rangle\|}{\||x\rangle\|}.$$

შევნიშნოთ, რომ $\|U\|^2$ ტოლია U^*U ოპერატორის უდიდესი საკუთრივი რიცხვის.

თუ U საძიებელი ოპერატორია, მაშინ მისი მიახლოებითი რეალიზაცია აღვნიშნოთ $\widetilde{U}$-ით.

განმარტება. ვიტყვით, რომ $\widetilde{U}$ ოპერატორი არის U-ს მიახლოებითი წარმოდგენა σ სიზუსტით, თუ $\left\|\widetilde{U}-U\right\|<\delta.$

ეს განმარტება ძალიან კარგია იმ შესანიშნავი თვისების გამო, რომ თუ $U=U_L...U_2U_1$ რამდენიმე ოპერატორის ნამრავლია, რომელთაგან თითოეულს აქვს თავისი მიახლოებითი წარმოდგენა $\widetilde{U}_k$ ოპერატორით δ_k სიზუსტით, მაშინ ამ მიახლოებათა ნამრავლი $\widetilde{U}=\widetilde{U}_L...\widetilde{U}_1$ არის U-ს წარმოდგენა $\sum\delta_k$ სიზუსტით. ეს ნიშნავს, რომ შეცდომების წრფივ დაგროვებას აქვს ადგილი:

$$\left\|\widetilde{U}_L...\widetilde{U}_1-U_L...U_1\right\|\le\sum_j\delta_j.$$

შეცდომების წრფივი კანონით დაგროვება ნებისმიერი ოპერატორისათვის არ არის დამახასიათებელი. ეს უნიტარული ოპერატორის ის შესანიშნავი თვისებაა, რომელზედაც ზემოთ გავამახვილეთ ყურადღება.

ყოველი მოდელი, რომელსაც პრეტენზია აქვს მოახდინოს გამოთვლა, შეთანხმებული უნდა იყოს გამოთვლის, როგორც ფიზიკური პროცესის მოდელთან. გამოთვლა, რომელიც აწარმოებს შეცდომების ექსპონენციალურ დაგროვებას პრაქტიკული თვალსაზრისით გამოსადეგი არ იქნება.

ისევე როგორც შებრუნებადი გამოთვლების შემთხვევაში, შემოვიტანოთ მიახლოებითი წარმოდგენის ცნება ფართო აზრით.

განმარტება. ვიტყვით, რომ $\widetilde{U}:\mathbf{P}^{\otimes n}\to\mathbf{P}^{\otimes n}$ ოპერატორის ზოგადი მიახლოება არის $\widetilde{U}:\mathbf{P}^{\otimes N}\to\mathbf{P}^{\otimes N}$ ოპერატორი σ სიზუსტით, თუ ნებისმიერი $|x\rangle$ ვექტორისათვის $\mathbf{P}^{\otimes n}$-დან ადგილი აქვს უტოლობას:

$$\left\|\widetilde{U}\left(|x\rangle\otimes\left|O^{N-n}\right\rangle\right)-U|x\rangle\otimes\left|O^{N-n}\right\rangle\right\|\le\delta\||x\rangle\|.$$

განმარტება. A ბაზისს ეწოდება სრული, თუ ნებისმიერი U ოპერატორი შესაძლებელია წარმოდგენილი იქნას კვანტური სქემით A ბაზისში ნებისმიერი მიახლოებით ფართო აზრით.

თეორემა 1. $F=\left\{H,K,\wedge\left(\delta^x\right),\wedge^2\left(\delta^x\right)\right\}$ ბაზისი სრულია, სადაც

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}, \quad K = \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}.$$

ეს თეორემა გამომდინარეობს შემდეგი ლემებიდან, რომლებსაც მოვიყვანთ დამტკიცების გარეშე.

ლემა. ვთქვათ $U : \mathbf{P}^{\otimes n} \to \mathbf{P}^{\otimes n}$ უნიტარული ოპერატორია, რომელიც აკმაყოფილებს პირობას $U|0\rangle = |0\rangle$. არსებობს $6n+1$ ზომის სქემა $F \cup \{U\}$ ბაზისში, რომელშიც შესაძლებელია $\wedge(U)$ ოპერატორის რეალიზება, ამასთან სქემაში U ოპერატორი გვხვდება მხოლოდ ერთხელ.

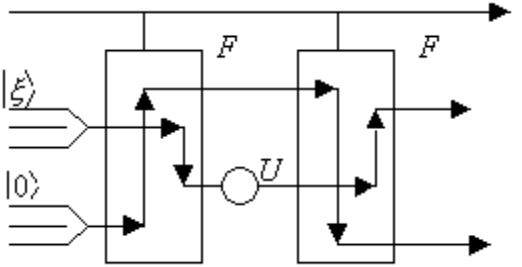
შემოვიტანოთ კიდევ ერთი საინტერესო ელემენტი, *ფრედკინის* გეიტი- $F = \wedge(\leftrightarrow)$, რომელიც მართავს ბიტების გაცვლას:

$$F : |a,b,c\rangle = \begin{cases} |0,b,c\rangle, & \text{თუ } a = 0; \\ |1,c,b\rangle, & \text{თუ } a = 1; \end{cases}$$

ტოფოლის კვანტური ელემენტის საშუალებით შესაძლებელია ფრედკინის გეიტის წარმოდგენა შემდეგნაირად:

$$F[1,2,3] = \wedge^2(\delta^x)[1,2,3]\wedge^2(\delta^x)[1,2,3].\wedge^2(\delta^x)[1,2,3].$$

ნახაზზე ნაჩვენებია სქემა U ოპერატორისათვის, რომელიც ინახავს $|0\rangle$-ს. მისგან შესაძლებელია $\wedge(U)$ შესაბამისი სქემის მიღება.



სქემა 2

ამ სქემაში, მართკუთხედებში ხდება ქუბიტების მართული გაცვლა, თუ მმართველი ქუბიტი 1-ის ტოლია, მაშინ იმ სქემის შესავალს, რომელიც U-ს გამოითვლის მიეწოდება $|\xi\rangle$, წინააღმდეგ შემთხვევაში მიეწოდება $|0\rangle$.

ახლა ჩამოვაყალიბოთ თეორემა, რომლის თანახმადაც კვანტური გამოთვლებისათვის საჭირო ნებისმიერი უნიტარული ოპერატორის მიღება შესაძლებებლია მცირე რაოდენობის ოპერატორებით, რომლებიც ერთ ან

ორ ქუბიტზე მოქმედებენ. ასეთ ოპერატორებს მიღებულია ეწოდოთ *ელემენტარული.*

თეორემა 2. $\{\delta^x, \wedge^2(R)\}$ არის სრული ბაზისი კვანტური გამოთვლებისათვის, სადაც $R = -ie^{\pi i \alpha \sigma^x}$, ხოლო α კი ირაციონალური რიცხვია.

ამ თეორემის დამტკიცება ემყარება ქვემოთ მოყვანილ დებულებებს, რომლებსაც დამოუკიდებელი მნიშვნელობაც აქვთ სხვადასხვა ტიპის ელემენტარული გეიტების აგების დროს.

დებულება 1. დავუშვათ $X, Y \in SO(3)$ არაკომუტირებადი ოპერატორებია, რომლებიც ანხორციელებენ მობრუნებას π-ს არათანაბარზომადი კუთხით. მაშინ X და Y-ით წარმოქმნილი ქვეჯგუფი ყველგან მკვრივია $SO(3)$-ში.

დებულება 2. F სტანდარტულ ბაზისზე მოჭიმული სიმრავლე ყველგან მკვრივია $U(B^{\otimes 2})/U(1)$-ში.

დებულება 3. F სტანდარტულ ბაზისში შესაძლებელია ფაზური ძვრების რეალიზება ფართო აზრით.

განმარტება. ვთქვათ $F : \boldsymbol{B}^n \to \boldsymbol{B}^m$ რაიმე ფუნქციაა. განვიხილოთ $U = U_L ... U_2 U_1 : \mathbf{P}^{\otimes N} \to \mathbf{P}^{\otimes N}$ კვანტური სქემა. ვიტყვით, რომ U სქემა გამოითვლის F**-ს,** თუ ნებისმიერი x**-**თვის სრულდება უტოლობა:

$$\sum_z \left| \langle F(x), z | U | x, O^{N-n} \rangle \right|^2 \geq 1 - \varepsilon,$$

სადაც ε $1/2$ ნაკლები რაიმე ფიქსირებული რიცხვია.

გავუკეთოთ ამ განმარტებას მცირე კომენტარი. ვამბობთ, რომ სქემა ითვლის F ფუნქციას, თუ U-თი ვმოქმედებთ $|x, O^{N-n}\rangle$ მდგომარეობაზე და "შევხედავთ" რა პირველ m ბიტს, დიდი ალბათობით "დავინახავთ" $F(x)$-ს. "შეხედვა" და "დანახვას" აქვს მკაცრი აზრი და ნიშნავს გაზომვის პროცედურას, რაზეც უკვე ვილაპარაკეთ წინა პარაგრაფში. რამდენჯერმე გამოთვლის ჩატარების შემდეგ გაზომვამ შესაძლებელია სხვადასხვა პასუხები მოგვცეს, მაშინ ავირჩევთ იმას, რომელიც გვხვდება ყველაზე უფრო ხშირად.

ელემენტარული გეიტები. კლასიკურ კომპიუტერში ყველა ბიტი დროის გარკვეულ მომენტში იმყოფება გარკვეულ მდგომარეობაში, მაგ. 00011101-ში. კვანტური კომპიუტერის მდგომარეობა აღიწერება ტალღური ფუნქციის საშუალებით:

$$\Psi = a|010011...\rangle + b|1011000\rangle + ...$$

სადაც *a* და *b* კომპლექსური რიცხვებია, ამასთანავე ალბათობა იმისა, რომ სისტემა იმყოფება $|010011...\rangle$ მდგომარეობაში არის $|a|^2$-ის ტოლი, ხოლო ალბათობა იმისა, რომ იგი იმყოფება $|111000...\rangle$ მდგომარეობაში $|b|^2$-ის ტოლია და ა.შ. Ψ ტალღური ფუნქცია გვეუბნება, რომ კომპიუტერი იმყოფება ყველა შესაძლო მდგომარეობაში, ხოლო როდესაც ხდება სისტემაზე "დაკვირვება", გაზომვა, მაშინ იგი იმყოფება ერთადერთ განსაზღვრულ მდგომარეობაში გარკვეული ალბათობით.

შემოვიტანოთ შემდეგი მატრიცები - უნიტარული ოპერატორები, რომლებიც $\mathbf{C^2}$-ის $\{|0\rangle, |1\rangle\}$ ბაზისზე მოქმედებენ შემდეგი წესით:

იგივური: $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \quad I : |0\rangle \to |0\rangle; |1\rangle \to |1\rangle;$

უარყოფა: $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \quad X : |0\rangle \to |1\rangle, |1\rangle \to |0\rangle;$

ფაზის გახლეჩვის ოპერაცია: $Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}; Y : |0\rangle \to -|1\rangle, |1\rangle \to |0\rangle;$

*1. **კონტროლირებადი არა*** (აღვნიშნოთ იგი *CNOT*-თი); ეს ოპერატორი მოქმედებს 2- ქუბიტზე. 2-ქუბიტი არის $\mathbf{C^4}$ ელემენტი და გამოისახება $\mathbf{C^4}$-ის შემდეგი ბაზისით: $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. *CNOT*-ის მოქმედება ამ საბაზისო ოპერაციებზე შემდეგნაირია:

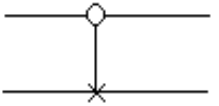
$$CNOT = \begin{cases} |00\rangle \to |00\rangle \\ |01\rangle \to |01\rangle \\ |10\rangle \to |11\rangle \\ |11\rangle \to |10\rangle \end{cases},$$

ანუ

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

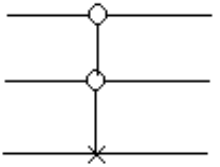
CNOT ოპერატორი მოქმედებს 2-ქუბიტზე, რომელიც ცვლის მეორე ქუბიტს თუ პირველი ქუბიტი 1-ია და არაფერი არ იცვლება, თუ პირველი ქუბიტი 0-ია.

CNOT ოპერატორის გრაფიკული გამოსახულება შემდეგია:



პატარა წრეწირი გამოხატავს მაკონტროლირებელ ბიტს, ხოლო × კი ნიშნავს ქვემდებარე ბიტის უარყოფას *(sobject bit)*

2'. ***კონტროლირებადი - კონტროლირებადი არა*** მოქმედებს 3-ქუბიტზე შემდეგი წესით: სამიდან უკანასკნელი ქუბიტის "უარყოფა" ხდება მაშინ და მხოლოდ მაშინ, როდესაც პირველი ორი ბიტი 1-ის ტოლია. გრაფიკულად $CCNOT : \mathbf{C}^3 \to \mathbf{C}^3$ გამოისახება შემდეგნაირად:



2.ადამარის ოპერატორი *(Hadamard transformation).* $H : \mathbf{C}^2 \to \mathbf{C}^2$ ოპერატორი $\mathbf{C}^2$-ის ბაზისზე მოქმედებს შემდეგნაირად:

$$H|0\rangle \to \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \quad |1\rangle \to \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

თუ *H*-ს ვამოქმედებთ *n* ბიტზე ინდივიდუალურად, მივიღებთ ყველა 2^n შესაძლო მდგომარეობების სუპერპოზიციას, რომელიც შეიძლება განვიხილოთ როგორც ნებისმიერი x რიცხვის 2-ობით თვლის სიტემაში ჩაწერის საშუალება, როდესაც $0 \le x \le 2^n - 1$:

$$(H \otimes H \otimes ...H)|00...0\rangle =$$

$$= \frac{1}{\sqrt{2^n}}((|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes ... \otimes (|0\rangle + |1\rangle) =$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle.$$

კლასიკურ გამოთვლებში კარგად ცნობილი ოპერაციები "უარყოფა" *(NOT),* "ან" *(OR)* და "და" (AND) ლოგიკური ოპერაციებიდან მხოლოდ *NOT* ოპერაციაა

შებრუნებადი. ჩვენი მიზანია ავაგოთ ამ კლასიკური ოპერაციების ანალოგი უნიტარული ოპერატოტების საშუალებით.

პირველ რიგში გავაკეთოთ შენიშვნა: თუ U_1 და U_2 უნიტარული ოპერატორებია, მაშინ $|0\rangle\langle 0|\otimes U_1 + |1\rangle\langle 1|\otimes U_2$ აგრეთვე უნიტარულია. ზემოთ განმარტებული *CNOT* და *CCNOT* ოპერატორები გამოისახებიან შემდეგნაირად:

$$CNOT = |0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes X,$$

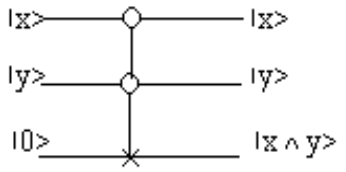
$$CCNOT = |0\rangle\langle 0|\otimes I\otimes I + |1\rangle\langle 1|\otimes CNOT.$$

CCNOT გეიტს ეწოდება *ტოფოლის* (*Toffoli)* გეიტი. ტოფოლის გეიტის საშუალებით *AND* და *NOT* გეიტები გამოისახებიან შემდეგნაირად:

$$T(|1,1,x\rangle) = |1,1,\neg x\rangle,$$

$$T(|x,y,0\rangle) = |x,y,x\wedge y\rangle.$$

ეს ნიშნავს, რომ *x*-ის "უარყოფის" მისაღებად საჭიროა მოვამზადოთ $|1,1,x\rangle$ მდგომარეობა და ვიმოქმედოთ მასზე *T* ოპერატორით. ხოლო *x* და *y* მდგომარეობების ჯამის მისაღებად საკმარისია მოვამზადოთ $|x,y,0\rangle$ მდგომარეობა და ვიმოქმედოთ მასზე *T* ოპერატორით. სქემატურად ეს გამოისახება შემდეგნაირად:



შევნიშნოთ, რომ ტოფოლის გეიტი საკმარისია ნებისმიერი კომბინატორული სქემის მისაღებად.

ქვემოთ ჩვენ შევაჯამებთ ამ პარაგრაფის ძირითად შედეგებს.

თეორემა 3. *(Deutsch,1985)*[10]. ყოველი კლასიკური გამოთვლადი ფუნქციისათვის არსებობს შებრუნებადი კვანტური გეიტებისაგან შედგენილი სქემა.

თეორემა 4. *(Bernstein, Vazirani,1997)*[12]. არსებობს კვანტური ტიურინგის მანქანა.

თეორემა 5. (იხ.[6]) ნებისმიერი $f : B^m \to B^k$ კლასიკური გამოთვლადი ფუნქცია რეალიზებადია კვანტურ კომპიუტერზე.

ამ თეორემიდან გამომდინარეობს, რომ ნებისმიერი გამოთვლადი *f* ფუნქციისათვის არსებობს ისეთი U_f ოპერატორი, რომელიც *m+n* ბიტზე მოქმედებს შემდეგი წესით:

$$U_f : |x,y\rangle \to |x, y \oplus f(x)\rangle. \qquad (1.4\text{-}1)$$

სადაც $\oplus$ არის "თანრიგობრივი გამორიცხული არა" *(bitwise exclusive OR)*.

თეორემის დამტკიცება ემყარება შემდეგ ლემას.

ლემა. (4-1) წესით განსაზღვრული U_f ოპერატორი არის უნიტარული ნებისმიერი f ფუნქციისათვის.

თეორემა 6. (*Barenco,Bennett, Cleve, Divincenzo,Margulis, Shor, Sleator, Smolin, Weifurter, 1995)*[14].

$\left\{CNOT, \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}, \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{-i\alpha} \end{pmatrix}\right\}$, სადაც $0 \le \alpha \le 2\pi$, სიმრავლე არის გეიტების უნივერსალური სიმრავლე.

კლონირების შეუძლებლობა. იმის გამო, რომ ევოლუციური პროცესის კვანტური აღწერა ხდება უნიტარული ოპერატორის საშუალებით, კვანტური მდგომარეობის კოპირება ანუ კლონირება შეუძლებელია. $|a\rangle$ კვანტური მდგომარეობის *კლონირება* ეწოდება ისეთ ოპერაციას, რომელიც $|a0\rangle$ მდგომარეობას გადაიყვანს $|aa\rangle$ მდგომარეობაში. სხვანაირად რომ ვთქვათ, არსებობს ისეთი U ოპერატორი, რომ ნებისმიერი $|a\rangle$ და $|b\rangle$ მდგომარეობებისათვის ადგილი აქვს ტოლობას:

$$U(|a0\rangle) = |aa\rangle \text{ და } U(|b0\rangle) = |bb\rangle \qquad (1.4\text{-}2)$$

ვაჩვენოთ, რომ ასეთი U ოპერატორი არ არსებობს. დავუშვათ საწინააღმდეგო, ვთქვათ არსებობს და სრულდება (4-2). განვიხილოთ მდგომარეობა $|c\rangle = \frac{1}{\sqrt{2}}(|a\rangle + |b\rangle)$, მაშინ U-ს წრფივობის გამო გვაქვს:

$$U(|c0\rangle) = \frac{1}{\sqrt{2}}(U(|a0\rangle) + U(|b0\rangle)) =$$

$$= \frac{1}{\sqrt{2}}(|aa\rangle + |bb\rangle). \qquad (1.4\text{-}3)$$

ხოლო თუ დავუშვებთ, რომ $U(|c0\rangle) = |cc\rangle$, მაშინ

$$U(|c0\rangle 0 = |cc\rangle = \frac{1}{2}(|aa\rangle + |ab\rangle + |ba\rangle + |bb\rangle) \qquad (1.4\text{-}4)$$

(4-3) და (4-4) გამოსახულებების მარჯვენა მხარეები ტოლები არ არიან, რაც ნიშნავს, რომ ჩვენი დაშვება სწორი არ არის.

კვანტური პარალელიზმი. დავუშვათ ბულის n-ცვლადზე დამოკიდებული f ფუნქციის მნიშვნელობის პოვნა გვინდა რაიმე x_0 წერტილში, სადაც $0 \le x_0 \le 2^n - 1$. ამისათვის ავიღოთ $|00...0\rangle$ მდგომარეობა და ვიმოქმედოთ მასზე ადამარის ოპერატორით:

$$H(|00...0\rangle) = \frac{1}{\sqrt{2^n}}(|00...0\rangle + |00...1\rangle + ... + |11...1\rangle) =$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle.$$

დავუმატოთ შედეგს k ბიტიანი რეგისტრი და ვიმოქმედოთ მასზე U_f ოპერატორით:

$$U_f\left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x,0\rangle\right) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} U_f(|x,0\rangle) =$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x, f(x)\rangle.$$

f ფუნქციის საძიებელ მნიშვნელობას ვღებულობთ გაზომვის შემდეგ $\frac{1}{\sqrt{2^n}}$ ალბათობით.

უნივერსალურ გეიტთა აგების გზები. ბრილინსკიმ აჩვენა [17], რომ *უნივერსალურ გეიტთა სისტემას წარმოადგენს ყველა* $\boldsymbol{C^2 \to C^2}$ *უნიტარული ოპერატორი გადახლართვის ერთ რომელიმე* $\boldsymbol{C^2 \otimes C^2 \to C^2 \otimes C^2}$ *ოპერატორთან ერთად.*

ინტერაქტიული პროგრამა, რომელიც ამოწმებს არის თუ არა 4×4-უნიტარული მატრიცი გადახლართვის ოპერატორი შეგიძლიათ ნახოთ ინტერნეტ-მისამართზე http: //www.physics.uq.edu.au/gqc/.

განვიხილოთ $S: \mathbf{C^2} \otimes \mathbf{C^2} \to \mathbf{C^2} \otimes \mathbf{C^2}$ ცხადად მოცემული უნიტარული ოპერატორი

$$S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

რომელსაც გადასმის ოპარატორი ვუწოდოთ. იგი ბიტების გადასმას ახდენს: $S|10>=|01>$ და პირიქით, $S|01>=|10>$. განვიხილოთ, აგრეთვე, შემდეგი დიაგონალური უნიტარული მატრიცი

$$D = \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & c & 0 \\ 0 & 0 & 0 & d \end{pmatrix},$$

სადაც a, b, c, d ნებისმიერი კომპლექსური რიცხვებია, რომელთა მოდულები ერთის ტოლია. იანგ-ბაქსტერის განტოლების (იხილე პარაგრაფი 2-ის ბოლო პუნქტი) უნიტარული ამონახსნებისა და S ოპერატორის ნამრავლს ვუწოდოთ ალგებრული იანგ-ბაქსტერის განტოლების ამონახსნი. ადვილად მოწმდება, რომ დიაგონალური D მატრიცი ალგებრული იანგ-ბაქსტერის განტოლების ამონახსნია, თუ $ad - bc \neq 0$. აქედან, გადახლართვის ოპერატორი იქნება მაგალითად,

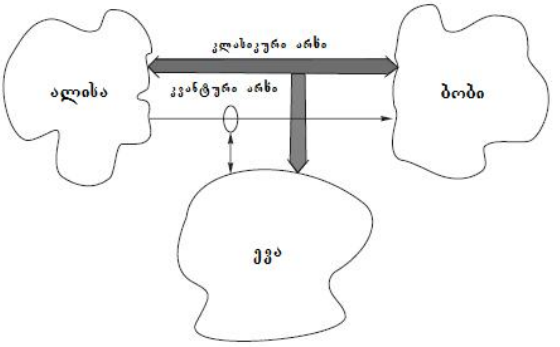
$$F = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

უნიტარული ოპერატორი. დავუშვათ $U_1, U_2: \mathbf{C^2} \to \mathbf{C^2}$ ორი უნიტარული ოპერატორია, მაშინ $U_1 \otimes U_2: \mathbf{C^2} \otimes \mathbf{C^2} \to \mathbf{C^2} \otimes \mathbf{C^2}$ არ იქნება გადახლართვის ოპერატორი და აქედან გამომდინარე ნებისმიერი უნიტარული ოპერატორი $U: \mathbf{C^2} \otimes \mathbf{C^2} \to \mathbf{C^2} \otimes \mathbf{C^2}$, რომელიც ორი ოპერატორის ტენზორული ნამრავლია, აგრეთვე არ იქნება გადახლართვის ოპარატორი. მაგალითად, $CNOT$ ოპერატორი გადახლართვის ოპერატორია და ახლახან შემოტანილ ოპერატორებს უკავშირდება შემდეგი ტოლობით: $CNOT = (H \otimes I)F(H \otimes I)^{-1}$, სადაც H ადამარის გეიტია.

კვანტური ტელეპორტაცია. ტელეპორტაციის მიზანია კვანტური მდგომარეობის შექმნა და გადაცემა. რადგან კვანტური მდგომარეობის კოპირება შეუძლებელია (წინააღმდეგ შემთხვევაში საწყისი ნაწილაკი განადგურებული იქნებოდა), ამის გამო ასეთი ნაწილაკებით გადაცემული ინფორმაცია თეორიულადაც კი შეუძლებელია არასანქცირებული მომხმარებლის ხელში მოხვდეს. 1984 წელს ბენეტმა და ბრასარდმა აღწერეს RSA–კრიპტოსისტემაზე დაფუძნებული საიდუმლო კოდის გადაცემის პირველი კვანტური სქემა.

განვიხილოთ შემთხვევა როდესაც ალისას და ბობს უნდათ შეთანხმდნენ საიდუმლო გასაღების გამოყენების თაობაზე. კავშირი ხორციელდება ჩვეულებრივი ორმხრივი კლასიკური და ცალმხრივი კვანტური არხებით. ევა ცდილობს ამ არხების მოსმენას. ალისა უგზავნის

ბობს რაღაც ნაწილაკებს (მაგალითად, ფოტონებს) კვანტური არხის საშუალებით. ბობი ზომავს ამ ნაწილაკების მდგომარეობებს. ევა ეცდება გაზომოს ნაწილაკების მდგომარეობები და შემდეგ გაუგზავნოს ისინი ბობს.



პროცესს იწყებს ალისა და უგზავნის ბობს ბიტების მიმდევრობას. თითოეული ბიტი კოდირებულია ბაზისების მეშვეობით შემდეგი წესით:

$$0 \to |\uparrow\rangle, \quad 1 \to |\rightarrow\rangle \qquad \text{ან} \qquad 0 \to |\nwarrow\rangle, \quad 1 \to |\nearrow\rangle.$$

ბობი ზომავს ფოტონების მდგომარეობას. ამ დროს ის შემთხვევით ირჩევს ბაზისს. მას შემდეგ, რაც ბიტები გადაცემულია, ბობი და ალისა ეუბნებიან ერთმანეთს რა ბაზისები იყო გამოყენებული კოდირებისთვის. ამ დამატებითი ინფორმაციის საშუალებით მათ შეუძლიათ განსაზღვრონ რომელი ბიტები იყო გადაცემული და გაშიფრული სწორად და გამოიყენონ ისინი საიდუმლო გასაღებად. საშუალოდ ეს იქნება გადაცემული ბიტების ნახევარი.

ახლა წარმოვიდგინოთ, რომ ევა ზომავს ფოტონების მდგომარეობებს, მანამ სანამ ისინი მოხვდებიან ბობთან და უგზავნის ბობს ახალ ფოტონებს იგივე მდგომარეობაში. დაახლოებით ნახევარჯერ ევა იყენებს მცდარ ბაზისს. შესაბამისად, როდესაც ბობი ზომავს გადაცემულ ქუბიტებს სწორ ბაზისში, ალბათობა იმისა, რომ მან მიიღო მცდარი მნიშვნელობა შეადგენს გადაცემული ბიტების მეოთხედს.

ნებისმიერი მოსმენა კვანტურ არხში ზრდის შეცდომების რაოდენობას. ეს შეიძლება მარტივად დადგინდეს ალისასა და ბობის მიერ მაშინ, როდესაც ისინი გაცვლიან თავიანთ ბაზისებს ან რამდენიმე მაკონტროლებელ ბიტს ღია, კლასიკური არხით. უფრო მეტიც, ამ პროცედურის შესაბამისად ევას გასაღები კოდის მეოთხედი მცდარი

იქნება. იმისათვის რომ მოხდეს ევას აღმოჩენა საკმაოდ დიდი ალბათობით, საკმარისია რომ ალისამ და ბობმა შეადარონ სულ რამდენიმე ბიტი.

განვიხილოთ $\Psi = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ ორ-ქუბიტიანი სისტემის გაზომვის პროცესი. ვზომავთ პირველ ქუბიტს სტანდარტულ $\{|0\rangle, |1\rangle\}$ ბაზისში:

$$a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle = |0\rangle\otimes(a|0\rangle + b|1\rangle) + |1\rangle\otimes(c|0\rangle + d1.$$

პირველი ბიტის გაზომვა $|a|^2 + |b|^2$ ალბათობით მოგვცემს $|0\rangle$-ს და $|c|^2 + |d|^2$ ალბათობით - $|1\rangle$-ს. იგივე პროცედურა შეესაბამება მეორე ბიტის გაზომვას.

გაზომვები გვაძლევენ საშუალებას სხვა კუთხით შევხედოთ გადახლართულ მდგომარეობებს. ნაწილაკები არ არიან გადახლართულნი, თუ ერთის გაზომვა არ მოქმედებს მეორეზე. მაგალითად, $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ გადახლართული მდგომარეობაა, რადგან ალბათობა იმისა, რომ პირველი ბიტის გაზომვა მოგვცემს $|0\rangle$-ს არის $\frac{1}{2}$ იმ პირობით, რომ მეორე ბიტი არ იყო გაზომილი მანამდე. მაგრამ, თუ მეორე ბიტი გაზომილია, მაშინ ცხადია, რომ პირველი ბიტის როგორც $|0\rangle$ მდგომარეობის გაზომვის ალბათობაა 1 ან 0 იმისდა მიხედვით, როგორ იყო გაზომილი მეორე ბიტი ($|0\rangle$ ან $|1\rangle$ შესაბამისად). $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$ არ არის გადახლართული მდგომარეობა, რადგან

$$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = |0\rangle\otimes\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

დავუბრუნდეთ ალისა და ბობის ამოცანას. დავუშვათ ორივეს აქვს $\psi = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ გადახლართული წყვილის თითო ქუბიტი. ალისა ცდილობს გაუგზავნოს ბობს $\varphi = a|0\rangle + b|1\rangle$ ქუბიტი კლასიკური არხით. ალისა ასრულებს ქუბიტის და გადახლართული წყვილის დეკოდირების პროცედურას.

საწყისი მდგომარეობა:

$$\varphi\otimes\psi = \frac{1}{\sqrt{2}}\big(a|0\rangle \otimes (|00\rangle + |11\rangle) + b|1\rangle \otimes (|00\rangle + |11\rangle)\big) = \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle).$$

ალისა მართავს პირველ ორ ქუბიტს, ხოლო ბობი კი - ბოლო ორს. ალისა მოქმედებს ამ საწყის მდგომარეობაზე თანმიმდევრობით $C_{not}\otimes I$ და $H\otimes I\otimes I$ ოპერატორებით:

$$(H\otimes I\otimes I)(C_{not}\otimes I\ )(\varphi\otimes\psi) = (H\otimes I\otimes I)(C_{not}\otimes I\ )(\varphi\otimes\psi)$$
$$= (H\otimes I\otimes I)\frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle) =$$
$$=\frac{1}{2}\big(|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle) + |10\rangle(a|0\rangle - b|1\rangle) +$$
$$11a1-b0.$$

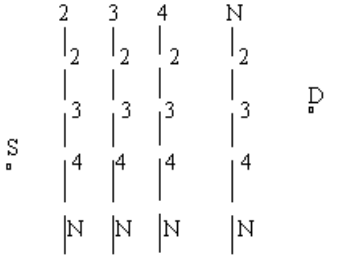
შემდეგ ალისა ზომავს პირველი ორი კუბიტის მდგომარეობას და ღებულობს ერთნაირი ალბათობით $|00\rangle$, $|01\rangle$, $|10\rangle$ ან $|11\rangle$-ს. შედეგიდან გამომდინარე ბობის კვანტური მდგომარეობა პროექტირდება შესაბამისად $a|0\rangle + b|1\rangle$, $a|1\rangle + b|0\rangle$, $a|0\rangle - b|1\rangle$ ან $a|1\rangle - b|0\rangle$ მდგომარეობებზე. ალისა უგზავნის ბობს თავისი გაზომვის შედეგს ორი კლასიკური ბიტის სახით. როდესაც ბობი ღებულობს ალისასგან ორ კლასიკურ ბიტს, მან უკვე იცის როგორ არის დაკავშირებული მისი გადახლართული წყვილის მდგომარეობა ალისას ქუბიტის საწყის მდგომარეობასთან. თავისი გადახლართული წყვილისთვის შესაბამისი გარდაქმნის გამოყენებით ბობს შეუძლია აღადგინოს ალისას ქუბიტის საწყისი φ მდგომარეობა.

შევნიშნოთ, რომ გაზომვისას ალისამ შეუქცევადად შეცვალა თავისი φ ქუბიტის მდგომარეობა. ზუსტად საწყისი მდგომარეობის დაკარგვა არის იმის მიზეზი, რომ ტელეპორტაცია არ ეწინააღმდეგება კლონირების შეუძლებლობას.

5.კომივოიაჟერის ამოცანის კვანტური ალგორითმი

განვიხილოთ *NP* - სრული ამოცანების ფიზიკური ასპექტები. *NP* - სრული ამოცანების მათემათემატიკური თეორია, რომელიც შეიცავს ამოცანის, ალგორითმის, სირთულის ცნებებს ჩვენ უკვე განვიხილეთ, მაგრამ კომპიუტერი ფიზიკური მოწყობილობაა, რის გამოც გვინდა განვიხილოთ *NP*-კლასის ამოცანების ფიზიკური ასპექტები.

განვიხილოთ კომივოიაჟერის ცნობილი ამოცანა (შემდგომში ვიხმართ აბრივიატურას-TSP, traveling-salesman-problem): მოცემულია *N* რაოდენობის



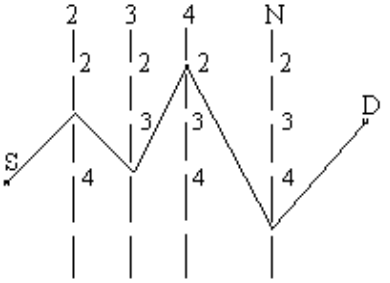
ნახ.1

ქალაქი და ქალაქთა ყოველ წყვილს შორის მანძილი d_{ij} . საჭიროა ვიპოვოთ ყველა ქალაქის შემაერთებელი უმცირესი გზა. ქვემოთ ჩვენ განვიხილავთ კერძო სახის ამოცანას, სადაც იგულისხმება, რომ ყველა d_{ij} ზემოდან შემოსაზღვრულია *L*-ით (ამოცანა კვლავ *NP*-კლასში რჩება). ამოცანის ამოხსნის ყველაზე მარტივი ალგორითმი შემდეგში მდგომარეობს: გადავნომროთ ყველა შესაძლო მარშრუტები და შემდეგ გავზომოთ მანძილები. ამოხსნის დრო ექსპონენციალურად იზრდება *N* -ის ზრდასთან ერთად, რადგან მარშრუტების რაოდენობა *N!* რიგისაა. მაგრამ არ არსებობს ამაზე უკეთესი ალგორითმი! ყველა *N!* მარშრუტის პარალელურ გადარჩევას სასრული დრო დასჭირდება, მაგრამ საჭირო იქნება *N!* პროცესორი, რის გამოც კომპიუტერის ზომა და ინფორმაციის წაკითხვის დრო გაიზრდება ექსპონენციალურად. ამრიგად, პირდაპირი პარალელიზმი დიდ ეფექტს ვერ მოგვცემს. საბოლოოდ ვასკვნით, რომ სასრულ ფიზიკურ სისტემას არ გააჩნია "ექსპონენციალურად ბევრი" შესაძლებლობა, მაგრამ ამასთან, შებრუნებული დებულებაა სამართლიანი! *კვანტურმა სისტემამ შესაძლებელია მართოს ექსპონენციალურად ბევრი მდგომარეობები.* კვანტური სისტემის ეს თვისება შესაძლებელია გამოყენებული იქნას გამოთვლებისათვის (Deutsch, Feynman). ამოცანა დავსვათ ასე: შესაძლებელია თუ არა ისეთი გამოთვლითი პრინციპების მოგონება, რომელიც *NP* კლასის ამოცანებს ამოხსნის პოლინომიალურ დროში და არსებობს თუ არა ისეთი ფიზიკური სისტემა, რომელშიც ამ გამოთვლების განხორციელება არ ეწინააღმდეგება ფიზიკურ კანონებს. კომივოიაჟერის ამოცანისათვის ჩვენ ავაგებთ ალგორითმს, რომელიც მას პოლინომიალურ დროში ამოხსნის, ხოლო შემდეგ ავაგებთ წარმოსახვით მანქანას, რომელზედაც ამ ალგორითმის განხორციელებაა შესაძლებელი.

N რაოდენობის ქალაქისათვის TSP-ს ამოსახსნელად განვიხილოთ მანქანა, რომელსაც ექნება N-1 ღერო და თითოეულ ღეროზე N-1 ნახვრეტი (ნახ.1). ყოველი ნახვრეტი ცალსახად მოიცემა (*i,j*) წყვილით. დავუშვათ S წერტილში მოთავსებულია ნაწილაკების წარმომქმნელი წყარო (მაგ. ლაზერი), ხოლო D წერტილში კი

ნაწილაკების დეტექტორი. ვთქვათ ნახვრეტებს შორის მოთავსებულია შტერნ-გერლახის მოწყობილობა. ამრიგად, ჩვენი მანქანა წარმოადგენს გარკვეული სახის მრავალნაბიჯიან ინტერფერენციულ მანქანას.

არსებობს $(N-1)^{(N-1)}$ შესაძლო ტრაექტორია, რომლითაც ნაწილაკი S წერტილთან მოხვდება *D* წერტილში. ტრაექტორია ცალსახად მოიცემა ნახვრეტების კოორდინატების მიმდევრობის ჩამოთვლით. მაგ. ნახ. 2-ზე ნაჩვენები ტრაექტორია მოიცემა შემდეგნაირად: *S (2,3), (3,4), (4,2), (5,5), D.* ნათელია, რომ ღეროების ნომერი შესაძლებელია გამოვტოვოთ და ტრაექტორია აღვწეროთ შემდეგი მიმდევრობით: *S,3,4,2,5,D.* თავის მხრივ, ეს მიმდევრობა შესაძლებელია მივიღოთ როგორც 5 ქალაქის შემაერთებელი ტრაექტორიის კოდი. ამასთან არსებობს ისეთი კოდები, რომლებიც არ შეიძლება იყოს კომივოიაჟერის მარშრუტები. მაგალითად, *S,2,2,3,5, D,* რადგან იგი შეესაბამება კომივოიაჟერის ისეთ მარშრუტს, რომლის თანახმადაც, კომივოიაჟერი ქალაქ 2-ში ორჯერ მოხვდება, ხოლო ქალაქ 4-კი საერთოდ არ გაივლის. ასეთ კოდებს ვუწოდოთ აკრძალული, ყველა დანარჩენს კი დასაშვები. საჭიროა აღვწეროთ ნაწილაკის მოძრაობის დინამიკა ისე, რომ ნაწილაკმა, რომელიც გაივლის მანქანას, იცოდეს შესაბამისი მარშრუტის სიგრძე.



ნახ.2

იმისათვის, რომ ეს პირობები შესრულდეს, საჭიროა გარკვეული თავისუფლების ხარისხის მქონე ისეთი ნაწილაკები, რომლებიც ურთიერთქმედებენ მანქანასთან. შესაძლებელია გამოვიყენოთ იზოტოპური სპინის მსგავსი შიგა თავისუფლების ხარისხი. კიდევ ერთხელ გავუსვათ ხაზი, რომ ჩვენ ვლაპარაკობთ ჰიპოთეზურ სამყაროზე და ამის გამო შეგვიძლია გამოვიგონოთ ნებისმიერი შიგა თავისუფლების ხარისხი, ისეთიც კი, რომელიც არ გვხვდება რეალურ სამყაროში არსებული ელემენტარული ნაწილაკებისათვის.

დავუშვათ ჩვენი ჰიპოთეზური ნაწილაკების შიგა მდგომარეობები აღიწერება შემდეგი კეტ-ვექტორით:

$$|k; c_2, c_3, \ldots, c_N, p\rangle,$$

სადაც $k \in \{0,1,...,NL\}$, $c_i \in \{0,1\}$, $p \in \{0,1\}$. *k* - კვანტური რიცხვი ზომავს მარშრუტის "კილომეტრაჟს", c_i კი მიუთითებს, იყო თუ არა კომივოიაჟერი *i*-ურ ქალაქში. *p* კვანტურ რიცხვს TSP - თან უშუალო კავშირი არა აქვს. იგი აღწერილი დინამიკის მქონე სისტემის რეალიზაციისათვის არის საჭირო. მანქანის მუშაობის პრინციპის აღსაწერად ყველაფერი მზადაა. განვიხილოთ ტრაექტორიის ნაწილი ორ მეზობელ *i* და *i+1* ღეროზე მოთავსებულ *m* და *n* ნახვრეტებს შორის: $(i,m) \to (i+1,n)$. დავუშვათ, რომ თუ ნაწილაკი გაივლის (i,n) ნახვრეტს, c_n კვანტური რიცხვი შეიცვლება შემდეგნაირად: $c_n = 0 \to c_n = 1$. დავუშვათ აგრეთვე, რომ ჩვენი ნაწილაკები ნახვრეტებს შორის გადაადგილების დროს მოძრაობენ არა თავისუფალ სივრცეში, არამედ გარკვეულ ველში ისე, რომ k კვანტური რიცხვი ტრაექტორიის განსახილველ (i,n) და $(i+1,m)$ ნახვრეტების შემაერთებელ მონაკვეთზე იზრდება შემდეგი კანონით:

$$k \to k + d_{nm},$$

სადაც d_{nm} არის m და n ქალაქებს შორის მანძილი.

დავუშვათ S წერტილში წარმოქმნილი ნაწილაკები იმყოფებიან $|0;0,...,0;0\rangle$ დგომარეობაში. მას შემდეგ, რაც ნაწილაკები გაივლიან მანქანას, ისინი გადავლენ

$$\sum_{\text{ტრაექტორიები}} |k;c_2,c_3,...,c_N;p\rangle_{\text{ტრაექტორია}}$$

მდგომარეობაში. ამ ჯამში ზოგიერთი ტრაექტორია შეესაბამება დასაშვებ ტრაექტორიას კომივოიაჟერისათვის. ნათელია, რომ ეს ის ტრაექტორიებია, რომელთათვისაც ყველა c_i კვანტური რიცხვები 1-ია. ასეთი ტრაექტორიებისათვის k კვანტური რიცხვის მნიშვნელობა შესაბამისი მარშრუტის სიგრძის ტოლია.

დავუშვათ ახლა D წერტილში მოთავსებულია ფილტრი, რომელიც ახშობს ყველა მდგომარეობას, გარდა იმ მდგომარეობებისა, რომელთათვისაც ყველა c_i რიცხვი 1-ის ტოლია. მაშინ მანქანის გამოსავალზე იქნება მდგომარეობა:

$$\sum_{\text{ტრაექტორიები}} |(\text{მარშრუტის სიგრძე}) \times k,1,...,1,p\rangle_{\text{ტრაექტორია}}.$$

ფილტრი შესაძლებელია იყოს შტერნ-გერლიხის ტიპის მოწყობილობების ერთობლიობა, რომლებიც გრძნობენ *c* კვანტურ რიცხვებს და აქრობენ ისეთ მდგომარეობას, რომელთათვისაც *c=0*. ამის შემდეგ საკმარისია D წერტილში მოვათავსოთ კიდევ ერთი შტერნ-გერლახის ტიპის მოწყობილობა, მხოლოდ

ამჯერად ისეთი, რომელიც მგრძნობიარე იქნება k კვანტური რიცხვის მიმართ. მან უნდა გაყოს გამომავალ ნაწილაკთა ნაკადი *NL* რაოდენობის ნაკადებად, რომელთაგან თითოეული შეესაბამებოდეს *k*-ს კონკრეტულ მნიშვნელობას. დავაყენოთ გამომავალი ნაწილაკების უკვე გაყოფილი ნაკადებისათვის დეტექტორები. $k = ML$ მახასიათებლების მქონე ნაკადი გადაიხრება მხოლოდ იმ შემთხვევაში, როდესაც არსებობს *M* სიგრძის მარშრუტი. იმ დეტექტორთა შორის, რომლებიც გადაიხრებიან, შესაძლებელია ავირჩიოთ ისეთი, რომელიც შეესაბამება მინიმალურ *k*-ს. ეს იქნება უმოკლესი გზა.

6.კვანტური ფურიეს გარდაქმნა და ნატურალური რიცხვის პერიოდი

სისტემა გასაღების ღია გავრცელებით. *NP* კლასს ეკუთვნის *დისკრეტული ლოგარითმის* გამოთვლის ამოცანა, რომელზედაც დაფუძნებულია *კრიპტოსისტემა გასაღების ღია გავრცელებით*. როგორც აღვნიშნეთ, ასეთი სისტემა იყენებს იმ გამოთვლით სირთულეს, რომელიც დაკავშირებულია გალუას ველის მიმართ ლოგარითმის გამოთვლასთან.

დავუშვათ $y = \alpha^x \bmod q$, სადაც $1 \le x \le q-1$, α რაიმე ფიქსირებული პრიმიტიული ელემენტია $GF(q)$-დან. ასეთ შემთხვევაში ვიტყვით, რომ x არის y -ის ლოგარითმი α ფუძით $GF(q)$-ში და დავწერთ: $x = \log_\alpha y$, $1 \le y \le q-1$; y-ის გამოთვლა x-ის საშუალებით ძნელი არ არის. ამისთვის საჭიროა მაქსიმუმ $2\log_2 q$ გამრავლების ოპერაცია, ხოლო x-ის გამოთვლა, როდესაც y ცნობილია, საკმაოდ რთული ამოცანაა და დამოკიდებულია q -ზე. ამჟამად არსებულ საუკეთესო ალგორითმსაც კი $\sqrt{q}$-რაოდენობის ოპერაცია ჭირდება (იხ. მაგ. [5]).

კრიპტოსისტემა აგებულია შემდეგნაირად: სისტემის თითოეული მომხმარებელი ახდენს x_i შემთხვევითი რიცხვის გენერირებას $GF(q)$-დან და ინახავს მას "საიდუმლოდ". გამოთვლის $y_i = \alpha^{x_i} \bmod q$-ს და აქვეყნებს მას (ეს რიცხვი ინახება ყველასთვის ხელმისაწვდომ ფაილში). როდესაც i და j მომხმარებელს სურთ ერთმანეთს გაუცვალონ საიდუმლო შეტყობინება, ისინი გასაღებად იყენებენ რიცხვს - $k_{ij} = \alpha^{x_i x_j} \bmod q$. i მომხმარებელი გამოითვლის k_{ij} -ს მას შემდეგ, რაც მიიღებს ხელმისაწვდომ (საჭირო,ღია) y_j -ს. ის იყენებს შემდეგ ტოლობას:

$$k_{ij} = y_j^{x_i} \ mod\ q = (\alpha^{x_j})^{x_i} \ mod\ q = \alpha^{x_i x_j} \ mod\ q$$

.

ანალოგიურად, j მომხმარებელი ფორმულით $k_{ij} = y_i^{x_j} \ mod\, q$ გამოთვლის k_{ij}-ს. სხვა მომხმარებელმა k_{ij} უნდა გამოთვალოს ხელმისაწვდომი y_i და y_j რიცხვების საშუალებით და $k_{i,j} = y_i^{\log_\alpha y_j} \bmod q$ ტოლობის გამოყენებით.

ამრიგად, თუ $GF(q)$ ველში ლოგარითმის გამოთვლა შესაძლებელია, მაშინ საიდუმლო სისტემის გახსნაც იქნება შესაძლებელი. აქვე შევნიშნოთ, რომ ასეთი კრიპტოსისტემის მდგრადობა ჯერ-ჯერობით დამტკიცებული არ არის. ეს მხოლოდ ემპირიული ფაქტია.

RSA კრიპტოგრაფიული სისტემა ღია გასაღებით (RSA -არის კრიპტოსისტემის ავტორების გვარების Rivest,Shamir,Adleman აბრივიატურა [15]). ამ სისტემაში გამოიყენება ასეთი იდეა: საკმაოდ დიდი (მაგ. 100 ბიტიანი) რიცხვის მარტივ მამრავლებად დაშლა რთული ამოცანაა!

A მომხმარებელი შემთხვევით ირჩევს საკმაოდ დიდ P და Q რიცხვებს და ამრავლებს მათ: $N = P \cdot Q$, ამის შემდეგ იგი N რიცხვს ხელმისაწვდომს ხდის, ხოლო P და Q რიცხვებს კი - საიდუმლოდ ინახავს. P და Q-ს საშუალებით გამოითვლება ეილერის $\Phi(N)$ ფუნქცია, რომელიც განმარტებით არის იმ მთელ რიცხვთა რაოდენობის ტოლი, რომლებიც N-თან თანამარტივნი არიან და ნაკლები არიან N-ზე. ცნობილია, რომ

$$\Phi(N) = (P-1)(Q-1).$$

შემდეგ იგი შემთხვევით $]2, \Phi(N)-1[$ ინტერვალიდან იღებს რაიმე რიცხვს და ხდის ხელმისაწვდომს.

შეტყობინება იგზავნება ისეთი $M_1, M_2, \ldots$ რიცხვების მიმდევრობით, რომელთაგან ყოველი M_i მოთავსებულია $]0, N-1[$ ინტერვალში. მათი გაფილტვრა ხდება ფორმულით $c = m^e \bmod N$, სადაც c არის დაშიფრული ტექსტი.

$\Phi(N)$ გასაიდუმლოებული რიცხვის საშუალებით A მომხმარებელი გამოითვლის ისეთ d-ს, რომელიც აკმაყოფილებს ტოლობას:

$$ed = 1 \bmod \Phi(N).$$

თუ e და $\Phi(N)$ თანამარტივები არ არიან, მაშინ ასეთი d არ არსებობს, მაგრამ ალგორითმი ამას "გაიგებს" და ავირჩევთ სხვა e-ს. $ed = 1 \bmod \Phi(N)$ ექვივალენტურია ტოლობისა:

$$ed = k\Phi(N) + 1$$

რადგან $x^{k\Phi(N)+1} = x \bmod N$ ტოლობა სრულდება ნებისმიერი x-თვის $]0, N-1[$-დან და ნებისმიერი k-თვის, გაშიფვრა ადვილი ხდება, კერძოდ საჭიროა c-ს ახარისხება d ხარისხში:

$$c^d = m^{ed} = m^{k\Phi(N)+1} = m \bmod n;$$

მანამ, სანამ არ მოიძებნება ეფექტური m^e-ს პოვნის ალგორითმი d-ს გამოთვლის გარეშე, ასეთი კრიპტოსისტემა იქნება მდგრადი.

დისკრეტული ლოგარითმის გამოსათვლელად არსებობს ეფექტური კვანტური ალგორითმი, რომლის რეალიზებაც შესაძლებელია მხოლოდ კვანტურ კომპიუტერზე. ქვემოთ ჩვენ განვიხილავთ ამ ალგორითმს.

ამოცანა. მოცემულია შედგენილი N ნატურალური რიცხვი. ვიპოვოთ N-ის გამყოფი ე.ი. ისეთი N_1, რომელიც განსხვავებულია 1-სა და N-საგან და აკმაყოფილებს პირობას $N_1 | N$ (რაც იკითხება შემდეგნაირად: N_1 ყოფს N-ს).

N_1-ის საპოვნელი ეფექტური ალგორითმის მოძებნას, როდესაც N არის 2-ის რაიმე ხარისხი, დიდი პრაქტიკული მნიშვნელობა აქვს, რადგან ასეთი ეფექტური ალგორითმის არ არსებობა, როგორც უკვე აღვნიშნეთ, არის *RSA* კრიპტოსისტემების მდგრადობის გარანტი.

განმარტება. აღვნიშნოთ $\mathbf{Z}_N^*$-ით N-თან თანამარტივ რიცხვთა სიმრავლე $\mathbf{Z}_N$-დან:

$$\mathbf{Z}_N^* = \{x \in \mathbf{Z}_N : (x, N) = 1\}.$$

$\mathbf{Z}_N^*$ არის ჯგუფი $x.y = (xy) mod\, N$ ოპერაციის მიმართ. $\mathbf{Z}_N^*$-ის ელემენტების რაოდენობა აღვნიშნოთ $\Phi(N)$-ით (ეს *ეილერის ფსი ფუნქციაა,* რომელზედაც უკვე ვილაპარაკეთ).

განმარტება. $x \in \mathbf{Z}_N^*$ ელემენტის რიგი, აღვნიშნოთ იგი $ord_N(x)$-ით, არის ის მინიმალური r-ნატურალური რიცხვი, რომლისთვისაც სრულდება ტოლობა $x^r \equiv 1 (mod\, N)$.

ცნობილია, რომ თუ $N = PQ$ არის კენტი (სადაც P და Q მარტივი რიცხვებია), მაშინ შემთხვევით აღებული $x \in \mathbf{Z}_N^*$ რიცხვის რიგი - $k = ord_N(x)$, $\frac{1}{2}$-ზე მეტი ალბათობით არის ლუწი და $x^{\frac{r}{2}} \equiv \pm 1 (mod\, N)$. ვთქვათ $y = x^{\frac{r}{2}}$, მაშინ

$y^2 \equiv 1(mod\ N)$ და $y \neq 1(mod\, N)$. სხვა სიტყვებით $N \mid y^{2-1}$, მაგრამ N არ ყოფს $(y \pm 1)$, მაშასადამე $(y+1, N)$ და $(y-1, N)$ რიცხვებიდან ერთი მაინც განსხვავებულია 1-სა და N-გან. ამრიგად, ვიპოვეთ N-ის არატრივიალური გამყოფი. აქვე შევნიშნოთ, რომ უდიდესი საერთო გამყოფის პოვნა შეგვიძლია ევკლიდეს ალგორითმის საშუალებით. ამრიგად, N შედგენილი რიცხვის გამყოფის პოვნა დაიყვანება $x \in \boldsymbol{Z}_N^*$-დან აღებული ნებისმიერი რიცხვის პერიოდის პოვნაზე, ამ ამოცანას კი კვანტური ფურიეს გარდაქმნა ხსნის ეფექტურად.

ზემოთ მოყვანილი მსჯელობის შედეგია აგრეთვე ის ფაქტი, რომ თუ ცნობილია $x \in \boldsymbol{Z}_N^*$ შემთხვევით აღებული რიცხვის რიგი, მაშინ ჩვენ შეგვიძლია დიდი ალბათობით ვიპოვოთ არატრივიალური ფესვი ერთიდან მოდულით N (ე.ი. ისეთი ფესვი, რომელიც 1-სა და -1-საგან განსხვავებულია).

კვანტური ფურიეს გარდაქმნა. ნებისმიერი q რიცხვისათვის ვთქვათ $\boldsymbol{Z}_q = \{0, \ldots, q-1\}$. ყოველი $a \in \boldsymbol{Z}_q$-თვის განვმარტოთ ფუნქცია $\chi_a : \boldsymbol{Z}_q \to \boldsymbol{C}$ შემდეგნაირად:

$$\chi_a(y) = e^{2\pi i \frac{ay}{q}} \tag{1.6-1}$$

$\{|a\rangle : a \in \boldsymbol{Z}_q\}$ ბაზისს ვუწოდოთ სტანდარტული. განვიხილოთ სიმრავლე $\{|\chi_a\rangle : a \in \boldsymbol{Z}_q\}$ ასეთ მდგომარეობათა სიმრავლეს ეწოდება ფურიეს ბაზისი. ყოველი a-თვის $\boldsymbol{Z}_q$-დან $|\chi_a\rangle$ მდგომარეობა განისაზღვრება შემდეგნაირად:

$$|\chi_a\rangle = \frac{1}{\sqrt{q}} \sum_{y \in \mathbf{Z}_q} \chi_{\mathbf{a}}(y) |y\rangle \tag{1.6-2}$$

კვანტური ფურიეს გარდაქმნა *(QFT)* არის უნიტარული ოპერატორი, რომელიც სტანდარტულ ბაზისს გადაიყვანს ფურიეს ბაზისში:

$$QFT : |a\rangle \to |\chi_n\rangle \tag{1.6-3}$$

ჩვენ საქმე გვექნება მხოლოდ სწრაფ კვანტურ ფურიეს გარდაქმნასთან (რომელსაც კვლავ *QFT*-თი აღვნიშნავთ) და ისევე როგორც კლასიკური სწრაფი ფურიეს გარდაქმნის შემთხვევაში დავუშვათ, რომ $q = 2^m$. ვთქვათ

$$a \in \boldsymbol{Z}_{2^m} = \{0, 1, \ldots, 2^m - 1\}.$$

ჩავწეროთ a თვლის ორობით სისტემაში

$$a = 2^{m-1} a_1 + 2^{m-2} a_2 + \ldots + 2^1 a_{m-1} + 2^0 a_m \tag{1.6-4}$$

(6-4) წარმოდგენას ბინარული წარმოდგენა ეწოდება. (6-1),(6-2) მიიღებს სახეს:

$$|a\rangle \xrightarrow{QFT} \sum_{y=0}^{2^m-1} e^{\frac{2\pi i a y}{2^m}} |y\rangle. \qquad (1.6\text{-}5)$$

უშუალო გადამრავლებით ადვილად დავრწმუნდებით, რომ ადგილი აქვს ტოლობას:

$$e^{\frac{2\pi i a y}{2^m}} |y_1 \ldots y_m\rangle = e^{2\pi i (0.a_m) y_1} |y_1\rangle e^{2\pi i (0.a_{m-1}a_m) y_2} |y_2\rangle \ldots e^{2\pi i (0.a_1 a_2 \ldots a_m) y_m} |y_m\rangle \qquad (1.6\text{-}6)$$

სადაც $\frac{a}{2^m} = 0.a_1 a_2 \ldots a_m$ და გამოყენებულია a-ს (6-4) ბინარული წარმოდგენა.

(6-6) ტოლობის გამოყენებით $|a\rangle$ დაიშლება შემდეგნაირად:

$$|a\rangle = \left(|0\rangle + e^{2\pi i (0.a_m)} |1\rangle\right)\left(|0\rangle + e^{2\pi i (0.a_{m-1}a_m)} |1\rangle\right) \ldots \left(|0\rangle + e^{2\pi i (0.a_1 \ldots a_m)} |1\rangle\right) \qquad (1.6\text{-}7)$$

შემოვიტანოთ შემდეგი ოპერატორი: $R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{pmatrix}$. ვაჩვენოთ, რომ ნახ.1-ზე მოცემული სქემა გამოითვლის (6-5) ტოლობით მოცემულ $|a\rangle$ მდგომარეობას.

◁ მართლაც, $|a\rangle = |a_1 \ldots a_m\rangle$-ის პირველ ქუბიტზე ვიმოქმედოთ ადამარის H ოპერატორზე და მივიღებთ:

$$|a\rangle \xrightarrow{H} \left(|0\rangle + e^{2\pi i (0.a_1)}\right) |a_2 \ldots a_m\rangle$$

მოვდოთ მაკონტროლებელი R_2 ოპერატორი:

$$\left(|0\rangle + e^{2\pi i (0.a_1)} |a_2 \ldots a_m\rangle\right) \xrightarrow{R_2} \left(|0\rangle + e^{2\pi i (0.a_1 a_2)} |1\rangle\right) |a_2 \ldots a_m\rangle.$$

შემდეგ ვიმოქმედოთ მასზე მაკონტროლებელი R_3 ოპერატორით და მივიღებთ მდგომარეობას:

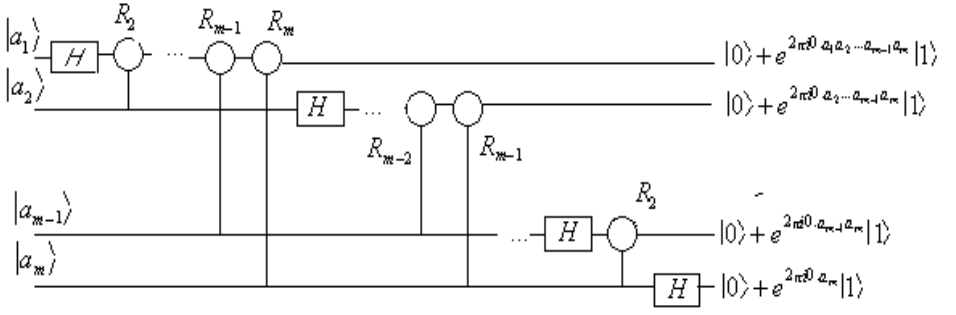
$$\left(|0\rangle + e^{2\pi i (0.a_1 a_2 a_3)} |1\rangle\right) |a_2 \ldots a_m\rangle$$

და ა.შ. საბოლოოდ გვექნება:

$$\left(|0\rangle + e^{2\pi i (0.a_1 \ldots a_m)} |1\rangle\right) |a_2 \ldots a_m\rangle.$$

ამის შემდეგ მეორე ქუბიტზე ვიმოქმედოთ კვლავ H ოპერატორით, შედეგს ექნება შემდეგი სახე:

$$\left(|0\rangle + e^{2\pi i (0.a_1 \ldots a_m)} |1\rangle\right)\left(|0\rangle + e^{2\pi i (0.a_2)} |1\rangle\right) |a_3 \ldots a_m\rangle,$$



სქემა 1.

გამოვიყენოთ ყველა მაკონტროლებელი R_k ოპერატორები R_2-დან დაწყებული R_{m-1} ჩათვლით და მივიღებთ:

$$\left(|0\rangle + e^{2\pi i(0.a_1 \ldots a_m)}|1\rangle\right)\left(|0\rangle + e^{2\pi i(0.a_2)}|1\rangle\right)|a_3 \ldots a_m\rangle$$

გავაგრძელებთ ამგვარად და საბოლოოდ გვექნება შემდეგი მდგომარეობა:

$$\left(|0\rangle + e^{2\pi i(0.a_1 \ldots a_m)}|1\rangle\right)\left(|0\rangle + e^{2\pi i(0.a_2 \ldots a_m)}|1\rangle\right)..\left(|0\rangle + e^{2\pi i(0.a_m)}|1\rangle\right).$$

თუ მაკონტროლებელ R_k ოპერატორს, რომელიც 2^m სიგრძის რეგისტრის l და j ქუბიტებზე მოქმედებს, აღვნიშნავთ S_{lj}-თი:

$$S_{l,j} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{\frac{i\pi}{2l-j}} \end{pmatrix},$$

მაშინ კვანტური ფურიეს გარდაქმნა მიიღება

$$H_0 S_{0,1} \ldots S_{0,m-1} H_1 \ldots H_{m-3} S_{m-3,m-2} S_{m-3,m-1} H_{m-2} S_{m-2,m-1} H_{m-1} \qquad (1.6\text{-}8)$$

ოპერატორების კომბინაციით ბიტების გადანაცვლების შემდეგ.

ზემოთ მოყვანილი მსჯელობიდან გამომდინარეობს შემდეგი დებულება:

დებულება. დავუშვათ ცნობილია (6-7) ნამრავლში შემავალი თითოეული მდგომარეობა

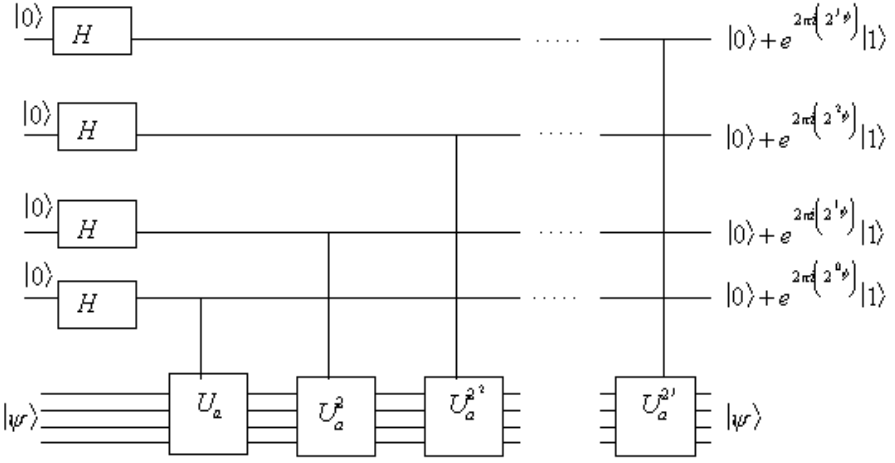
$$\left(|0\rangle + e^{2\pi i(0.a_m)}|1\rangle\right),\ \left(|0\rangle + e^{2\pi(0.a_{m-1}a_m)}|1\rangle\right),\ldots,\left(|0\rangle + e^{2\pi i(0.a_1 \ldots a_m)}|1\rangle\right),$$

მაშინ შესაძლებელია $a_1,\ldots,a_m$ რიცხვების გამოთვლა.

◁ დებულების დასამტკიცებლად საკმარისია შევნიშნოთ, რომ (6-3)-ით განსაზღვრული *QFT* გარდაქმნა, რომელიც ხორციელდება (6-8) ოპერატორით, შებრუნებადია, ამიტომ $|a_1...a_m\rangle$ მდგომარეობის მისაღებად საჭიროა გამოვიყენოთ $(QFT)^{-1}$ ▷.

დავუშვათ U უნიტარული ოპერატორია, რომელიც n-ქუბიტზე მოქმედებს და $|\psi\rangle$ არის U-ს საკუთრივი ვექტორი $e^{2\pi i\phi}$, $0 \le \phi < 1$ საკუთრივი მნიშვნელობით. განვიხილოთ შემდეგი სცენარი: ვთქვათ ცნობილი არ არის U, $|\psi\rangle$ და $e^{2\pi i\phi}$, მაგრამ მოცემულია მოწყობილობა, რომელიც არის მაკონტროლებელი - U, მაკონტროლებელი - U^{2^1}, მაკონტროლებელი U^{2^2} და ა.შ. ვთქვათ აგრეთვე, არსებობს $|\psi\rangle$ მდგომარეობის წარმომქმნელი მოწყობილობა. ამ მონაცემებით ჩვენი მიზანია მივიღოთ m თანრიგიანი შეფასება ϕ-თვის.

შემდეგი სქემა



სქემა 2.

წარმოქმნის მდგომარეობას:

$$\left(|0\rangle + e^{2\pi i 2^{m-1}\phi}|1\rangle\right)\left(|0\rangle + e^{2\pi i 2^{m-2}\phi}|1\rangle\right)..\left(|0\rangle + e^{2\pi i\phi}|1\rangle\right) = \sum_{y=0}^{2^m-1} e^{2\pi i\phi y}|y\rangle. \qquad (1.6\text{-}9)$$

უკვე ვნახეთ, რომ თუ $\phi = 0.a_1...a_m$-ს, მაშინ $|a_1...a_m\rangle$ მდგომარეობა (და მაშასადამე ϕ) შეიძლება მივიღოთ შებრუნებული კვანტური ფურიეს გარდაქმნით,

ხოლო თუ ϕ არ წარმოიდგინება $\phi = \frac{a}{2^m}$ სახით, მაშინ ასეთი ϕ-თვის ფურიეს შებრუნებული გარდაქმნა გვაძლევს ϕ-ს საუკეთესო m-თანრიგიან აპროქსიმაციას $4/\pi^2 = 0.405...$ ალბათობით. ჩავთვალოთ, რომ ასეთ პირობებში $\phi = \frac{a}{2^m} + \delta$, სადაც $0 < |\delta| \le \frac{1}{2^{m+1}}$. გამოვიყენოთ (6-9)-თვის შებრუნებული კვანტური ფურიეს გარდაქმნა და მივიღებთ:

$$\frac{1}{2^m}\sum_{x=0}^{2^m-1}\sum_{y=0}^{2^m-1} e^{-\frac{2\pi i xy}{2^m}} e^{2\pi i\phi y}\left|x\right\rangle = \frac{1}{2^m}\sum_{x=0}^{2^m-1}\sum_{y=0}^{2^m-1} e^{-\frac{2\pi i xy}{2^m}} .e^{2\pi i\left(\frac{a}{2^m}+\delta\right)y}\left|x\right\rangle,$$

სადაც $a_1...a_m$-ს კოეფიციენტი იქნება:

$$\frac{1}{2^m}\sum_{y=0}^{2^m-1}\left(e^{2\pi i\delta}\right)^y = \frac{1}{2^m}\left(\frac{1-\left(e^{2\pi i\delta}\right)2^m}{1-e^{2\pi i\delta}}\right).$$

რადგან $|\delta| \le \frac{1}{2^{m+1}}$, ამიტომ $2\pi\delta 2^m \le \pi$ და აქედან $\left|1-e^{2\pi i\delta 2^m}\right| \ge \frac{2\pi\delta 2^m}{\pi/2} = 4\delta 2^m$, აგრეთვე $\left|1-e^{2\pi i\delta}\right| \le 2\pi\delta$. ამრიგად, ალბათობა იმისა, რომ $a_1...a_m$ მდგომარეობა იქნება დამზერილი მდგომარეობის გაზომვის შემდეგ ტოლია

$$\left|\frac{1}{2^m}\left(\frac{1-\left(e^{2\pi i\delta}\right)2^m}{1-e^{2\pi i\delta}}\right)\right|^2 \ge \left(\frac{1}{2^m}\left(\frac{4\delta 2^m}{2\pi\delta}\right)\right)^2 = \frac{4}{\pi^2}.$$

შევნიშნოთ, რომ ალგორითმი შეიცავს m მაკონტროლებელ $-U^{2^k}$ ოპერაციას და კიდევ $O\left(m^2\right)$ სხვა ოპერაციას.

განვიხილოთ რიგის პოვნის ამოცანა. მოცემულია a და N ურთიერთთანამარტივი დადებითი რიცხვები და $a < N$. ჩვენს მიზანს შეადგენს ვიპოვოთ ისეთი უმცირესი დადებითი r რიცხვი, რომ $a^r \bmod N = 1$.

დავუშვათ, შეგვიძლია შევქმნათ

$$\left|\psi_1\right\rangle = \sum_{j=0}^{r-1} e^{-\frac{2\pi i j}{r}}\left|a^j \bmod N\right\rangle$$

მდგომარეობა. განვიხილოთ ისეთი უნიტარული U გარდაქმნა, რომელიც $\left|x\right\rangle$-ს გადასახავს $\left|ax \bmod N\right\rangle$-ში. ვთქვათ, $\left|\psi_1\right\rangle$ არის U-ს საკუთრივი ვექტორი $e^{2\pi i\left(\frac{1}{r}\right)}$

საკუთრივი მნიშვნელობით. ვთქვათ, აგრეთვე, რომ რომელიმე j-თვის შესაძლებელია მაკონტროლებელი U^{2^j} გეიტის შექმნა $O(n^2)$ რაოდენობის ელემენტარული გეიტის საშუალებით. გამოვიყენოთ წინა პუნქტში განვითარებული მეთოდები და მივიღებთ, რომ $\frac{1}{r}$ შეგვიძლია მივიღოთ $2n$ თანრიგის სიზუსტით საკმაოდ დიდი ალბათობით.

ზემოთ მოყვანილი მეთოდის სუსტი მხარეა ის, რომ არ არსებობს $|\psi_1\rangle$ მდგომარეობის შექმნის ეფექტური მეთოდი. დავუშვათ, გვაქვს მოწყობილობა, რომელიც წარმოქმნის

$$|\psi_k\rangle = \sum_{j=0}^{r-1} e^{-\frac{2\pi i k j}{r}} |a^j \bmod N\rangle$$

მდგომარეობას, სადაც k არის შემთხვევით არჩეული რიცხვი $\{1,\ldots,r\}$ რიცხვებიდან. პირველ რიგში ვაჩვენებთ, რომ ეს, აგრეთვე, საკმარისია r-ის ეფექტურად გამოთვლისათვის, ხოლო შემდეგ შევქმნით ასეთ მდგომარეობას.

ყოველი k-თვის $\{1,\ldots,r\}$ – დან $|\psi_k\rangle$ მდგომარეობის საკუთრივი მნიშვნელობაა $e^{2\pi i\left(\frac{k}{r}\right)}$ და ჩვენ შეგვიძლია კვლავ გამოვიყენოთ წინა პუნქტის ტექნიკა, რისი საშუალებითაც ეფექტურად გამოვითვლით $\frac{k}{n}$-ს $2n$-თანრიგის სიზუსტით. აქედან შეგვიძლია $\frac{k}{r}$ რიცხვი წარმოვადგინოთ უწყვეტი წილადის სახით. თუ აღმოჩნდა, რომ $(k,r)=1$, მაშინ მივიღებთ r-ს, წინააღმდეგ შემთხვევაში კი r-ის გამყოფს მივიღებთ. შემოწმება იმისა, რომ მართლაც სასურველი რიცხვი მივიღეთ თუ არა, შესაძლებელია $a^r \bmod N$-ის გამოთვლით. თუ r რიგია, მაშინ უნდა შესრულდეს ტოლობა: $a^r \bmod N = 1$. თუ აღმოჩნდა, რომ ეს ტოლობა არ სრულდება, იგივე პროცედურას შევასრულებთ სხვა $|\psi_k\rangle$ მდგომარეობისათვის, ამიტომ საჭიროა $O(\log(\log(N))) = O(\log n)$ ცდის ჩატარება იმაში დასარწმუნებლად, რომ k და r თანამარტივნი არიან.

თუ ორი დამოუკიდებელი ცდის შემდეგ მივიღებთ k_1/r და k_2/r რიცხვებს, r-ის გამოსაცნობად საკმარისია, რომ k_1 და k_2 თანამარტივები იყვნენ r-თან. ალბათობა იმისა, რომ ეს მართლაც ასეა, შემოსაზღვრულია ქვემოდან შემდეგი რიცხვით:

$$1-\sum_{\text{P არის მარტივი}}\Pr[p \text{ ყოფს } k_1]\Pr[p \text{ ყოფს } k_2]\geq 1-\sum_{P\text{არის მარტივი}}\frac{1}{p^2}\geq 0.54.$$

დავუშვათ არ გვაქვს სპეციალური მოწყობილობა შემთხვევითი საკუთრივი ვექტორის შესაქმნელად და დაკვირვებადი მდგომარეობაა $|1\rangle=\sum_{k=1}^{r}|\psi_k\rangle$, რომელიც ადვილია შესაქმნელად. გამოვიყენოთ ზემოთ მოყვანილი ალგორითმი, მხოლოდ $|\psi_k\rangle$ მდგომარეობა შევცვალოთ $|1\rangle$ მდგომარეობით. მაკონტროლებელი რეგისტრი გავზომოთ $|\psi_1\rangle,...,|\psi_r\rangle$ ორთონორმირებული ბაზისის მიმართ. რადგან ეს ორთონორმირებული ბაზისი შედგენილია U ოპერატორის საკუთრივი ვექტორებისაგან, ამიტომ გაზომვის ოპერაცია (ოპერატორი) კომუტირებს ყველა მაკონტროლირებელ U^{2j} ოპერაციასთან, ამიტომ შედეგი იგივე იქნება, იმის მიუხედავად, გამოთვლის დაწყებამდე გამოვიყენებთ ამ ოპერაციას, თუ გამოთვლის შემდეგ. აქედან გამოდის, რომ თუ $|1\rangle$-ით შევცვლით შემთხვევით აღებულ $|\psi_k\rangle$-ს, შედეგი იგივე დარჩება.

ამით ჩვენ დავასრულეთ რიგის პოვნის ალგორითმის ყველა საფეხური.

7. დოიჩის ამოცანა

კვანტურ გამოთვლებში შავი ყუთი მოიცემა U_f უნიტარული ოპერატორით, რომელსაც ისე როგორც კლასიკური გამოთვლების თეორიაში, *ორაკულს* უწოდებენ.

განვიხილოთ დოიჩის ე.წ. XOR-ამოცანა: *საჭიროა გავარკვიოთ* $f:\boldsymbol{B}\to\boldsymbol{B}$ *ფუნქცია მუდმივია თუ არა.* კლასიკურ შემთხვევაში საჭიროა გამოითვალოს f ფუნქცია 2-ჯერ. ანუ თუ ჩვენ გვაქვს მოწყობილობა, რომელიც ერთი "ჩართვით" გამოითვლის f-ის კონკრეტულ მნიშვნელობას, მაშინ საჭიროა ჩვენი მოწყობილობა 2-ჯერ ჩავრთოთ. კვანტურ შემთხვევაში კი ამოცანის ამოსახსნელად საჭიროა ჩვენი მოწყობილობის კვანტური ანალოგის მხოლოდ ერთხელ ჩართვა.

ამოცანა. ვთქვათ $f:\boldsymbol{Z}_{2N}\to\boldsymbol{Z}_2$. ვიპოვოთ ჭეშმარიტი დებულება.

A. f არ არის მუდმივი ფუნქცია (ე.ი. $f(x_1,...,x_{2N})=0$ ან $f(x_1,...,x_{2N})=1$ ნებისმიერი $x_1,...,x_{2N}\in\boldsymbol{Z}_{2N}$-სათვის).

B. f ფუნქციის მნიშვნელობათა $f(0),...,f(2N-1)$ მიმდევრობა არ შეიცავს ზუსტად N რაოდენობის 0-ს.

◁ განვიხილოთ შემდეგი უნიტარული ოპერატორი

$$S|i,j\rangle = (-1)^j |i,j\rangle. \qquad (1.7\text{-}1)$$

და მოვამზადოთ მდგომარეობა

$$|\Phi\rangle = \frac{1}{\sqrt{2N}} \sum_{i=0}^{2N-1} |i,0\rangle \qquad (1.7\text{-}2)$$

(7-1) ოპერაციას კვანტური კომპიუტერი N-ისა და f-ისაგან დამოუკიდებლად შეასრულებს ფიქსირებული ნაბიჯების შემდეგ, ხოლო (7-2) მდგომარეობა მიიღება $|0,0\rangle$ საწყისი მდგომარეობიდან f-ისაგან დამოუკიდებლად $O(ln(u))$ ნაბიჯით.

თუ $2N$ არის 2-ის რაიმე ხარისხი, მაშინ ყოველი i-ს მნიშვნელობა მიიღება ელემენტარული ერთბიტიანი

$$|x\rangle \to \frac{1}{\sqrt{2}}\left(|x\rangle + (-1)^x |1-x\rangle\right), \quad x \in \mathbf{Z}_2$$

გარდაქმნით ყოველი ბიტისათვის $log_2(2N)$ რაოდენობის ბიტიდან.

დავუშვათ U_f კვანტური ორაკულია და მეხსიერების ჩვენთვის საინტერესო ნაწილი იმყოფება $|\Phi\rangle$ მდგომარეობაში. ვიმოქმედოთ მასზე თანმიმდევრობით U_f, S, U_f ოპერატორებით, მაშინ (7-1) და (7-2) –ის გამოყენებით მივიღებთ:

$$|\Phi\rangle \to \frac{1}{\sqrt{(2N)}} \sum_{i=0}^{2N-1} |i, f(i)\rangle \to \frac{1}{2N} \sum_{i=0}^{2N-1} (-1)^{f(i)} |i, f(i)\rangle \to \frac{1}{2N} \sum_{i=0}^{2N-1} (-1)^{f(i)} |i,0\rangle \equiv \psi \qquad (1.7\text{-}3)$$

გამოვთვალოთ $|\langle \Phi | \Psi \rangle|$ სიდიდე:

$$|\langle \Phi | \Psi \rangle| = \frac{1}{2N} \left| \sum_{i=0}^{2N-1} (-1)^{f(i)} \right| \qquad (1.7\text{-}4)$$

(7-4) ტოლობის მარჯვენა მხარე 0-ის ტოლია, თუ ჩვენი ამოცანის B გამონათქვამი მცდარია და 1-ის ტოლია თუ A გამონათქვამია მცდარი. ამრიგად, თუ (1.7-3) ოპერაციების შესრულების შემდეგ ჩვენ გავზომავთ $|\phi\rangle\langle\phi|$ პროექციას და მივიღებთ 0-ს, ეს ნიშნავს, რომ $|\psi\rangle$ არ ყოფილა $|\phi\rangle$-ს პარალელური და ამრიგად A გამონათქვამი ჭეშმარიტია, ხოლო თუ შედეგი 1-ის ტოლია, მაშინ $|\psi\rangle$

არ არის ორთოგონალური $|\phi\rangle$ მდგომარეობის და ამრიგად, B გამონათქვამია ჭეშმარიტი.

შედეგი აუცილებლად იქნება 0 ან 1, რადგან ისინი (0 და 1) არიან პროექტირების ოპერატორის (ნებისმიერი ხილული მდგომარეობის) საკუთრივი რიცხვები. ამრიგად, ჩვენს მიერ შესრულებულმა პროცედურებმა არ შეიძლება არ მოგვცეს ჭეშმარიტი მნიშვნელობა A ან B გამონათქვამისათვის.

$|\phi\rangle\langle\phi|$ შესაძლებელია გამოითვალოს $O(ln\,N)$ ნაბიჯში. გამოთვლისათვის საჭიროა 1) გამოვიყენოთ $|0,0\rangle$ საწყისი მდგომარეობიდან $|\phi\rangle$ მდგომარეობის მიღების ოპერატორის შებრუნებული ოპერატორი. 2) გამოვთვალოთ $|0,0\rangle\langle 0,0|$. გამოთვლა წარმოებს ყოველი ბიტისათვის ცალ-ცალკე.

(7-3)-ში U_f ორაკულის გამოძახება ხდება მხოლოდ 2-ჯერ. საუკეთესო შემთხვევაში კლასიკური და სტოქასტიკური გამოთვლების შემთხვევაში კი $3-2^{-N+1}$-ჯერ გამოძახებაა საჭირო გამოთვლის ყოველ ნაბიჯზე.

8. გროვერის ალგორითმი. მონაცემთა მოუწესრიგებელ ბაზაში მოცემული თვისების მქონე ელემენტის პოვნა

დავუშვათ მონაცემთა ბაზა შედგება N ელემენტისაგან. ყველაზე ეფექტურ კლასიკურ ალგორითმში გადაისინჯება თანმიმდევრობით მონაცემთა ბაზის ელემენტები და შემოწმდება: აკმაყოფილებს თუ არა მოცემულ პირობას თითოეული ამორჩეული ელემენტი. თუ რომელიმე ელემენტს საჭირო თვისება გააჩნია, მაშინ ძიება მთავრდება, თუ არა, გადავდივართ შემდეგ ელემენტზე, მხოლოდ შემოწმებულები ისეთ ადგილზე თავსდება, რომ ხელმეორედ აღარ იქნას შემოწმებული. ნათელია, რომ საჭირო ელემენტის პოვნამდე საშუალოდ $N/2$ ელემენტის შემოწმებაა საჭირო.

ვაჩვენებთ, რომ თუ სისტემის შესავალზე და გამოსავალზე მოდებულია მდგომარეობათა სუპერპოზიცია, მაშინ საჭირო ელემენტის მოძებნა მოხდება $O(\sqrt{N})$ კვანტურ-მექანიკური ბიჯის შემდეგ $O(N)$ კლასიკური ბიჯის მაგივრად. ყოველი კვანტური ბიჯი შედგება უნიტარული ოპერაციისაგან. პირველ რიგში განვიხილავთ ამ ოპერაციებს.

აქ კიდევ ერთხელ ჩამოვაყალიბებთ კვანტური ალგორითმის არსს. კვანტურ კომპიუტერში ლოგიკური სქემები და ბიჯები (დროის გარკვეულ ინტერვალში) არსებითად იმყოფებიან სუპერპოზიციის მდგომარეობაში კვანტური

მექანიკის აზრით. კვანტური ოპერაციები, რომელთა კონტროლირებადი შესრულება ხდება, ყოველ ბიჯზე მოქმედებს მეხსიერების ბიტების მცირე ნაწილზე. ძებნის კვანტური ალგორითმიც, რომელსაც ჩვენ ვიკვლევთ, არის ისეთი უნიტარული ოპერატორების მიმდევრობა, რომლებიც მოქმედებენ სუფთა მდგომარეობებზე. ამ მდგომარეობათა განსაზღვრა შესაძლებელია გაზომვის პროცედურით (რომელიც მათემატიკურად კვლავ უნიტარული ოპერატორია). გამოვიყენებთ სამ უნიტარულ ოპერაციას:

1. ოპერატორი, რომელიც მოამზადებს ისეთ მდგომარეობას, რომელიც თანაბარი ალბათობით გვხვდება სისტემის N-საბაზისო მდგომარეობიდან ერთ-ერთში;
2. ადამარის ოპერატორი;
3. მდგომარეობის ფაზის შერჩევით მობრუნება.

როგორც უკვე აღვნიშნეთ, ადამარის H ოპერატორი $|0\rangle$ და $|1\rangle$ მდგომარეობაზე ისეთნაირად მოქმედებს, რომ მიღებული ორივე მდგომარეობის ამპლიტუდა $\frac{1}{\sqrt{2}}$-ის ტოლია, ხოლო $|1\rangle$ მდგომარეობის ფაზა შებრუნებულია.

ფაზის ანალოგი კლასიკურ ალბათურ ალგორითმებში არ არსებობს. ის ჩნდება კვანტურ მექანიკაში, რადგან ალბათობის ამპლიტუდა კომპლექსური რიცხვია. ისეთ სისტემაში, რომლის მდგომარეობა აღიწერება n ბიტის საშუალებით (ე.ი. გვაქვს $N = 2^n$ შესაძლო მდგომარეობა), ჩვენ შეგვიძლია განვახორციელოთ H გარდაქმნა დამოუკიდებლად ცალკეულ ბიტებზე და ამით თანმიმდევრულად შეგვიძლია შევცვალოთ სისტემის მდგომარეობა. მატრიცის განზომილება, რომელიც ამ ოპერაციას შეესაბამება, იქნება $2^n \times 2^n$. (იხ. პარაგრაფი 4, ელემენტარული გეიტები კვანტური გამოვლისათვის).

მდგომარეობის ფაზის შერჩევით მობრუნებას ანხორციელებს ოპერატორი:

$$\begin{pmatrix} e^{i\phi_1} & 0 \\ 0 & e^{i\phi_2} \end{pmatrix},$$

სადაც ϕ_1 და ϕ_2 ნებისმიერი ნამდვილი რიცხვებია. ამ გარდაქმნის დროს გადასვლის ამპლიტუდა არ იცვლება.

დავუშვათ სისტემას აქვს $N = 2^n$ მდგომარეობა, რომლებიც აღვნიშნოთ $S_1,...,S_N$-ით. დავუშვათ არსებობს ერთადერთი მდგომარეობა, მაგალითად S_j, რომელიც აკმაყოფილებს პირობას $C(S_j) = 0.$ ამოცანა მდგომარეობს S_j-ის გამოცნობაში.

ეს ამოცანა შეიძლება განხილული იქნას, როგორც მონაცემთა ბაზაში მიცემული თვისების მქონე ელემენტის ძიების ამოცანა. ამ შემთხვევაში C ფუნქცია იქნება მეხსიერების უჯრის შიგთავსის მდგომარეობის განმსაზღვრელი პროცედურა. ბევრი გამოთვლითი ამოცანა შესაძლებელია ამ ფორმით იქნას ჩამოყალიბებული.

ნაბიჯი 1. გადავიყვანოთ სისტემა სუპერპოზიციის მდგომარეობაში:

$$\left(1/\sqrt{N}, 1/\sqrt{N}, \ldots, 1/\sqrt{N}\right).$$

ამრიგად, ყოველი N მდგომარეობიდან ყველას ექნება ერთნაირი ამპლიტუდა. ამ სუპერპოზიციის მიღება შეიძლება $O(\log N)$ ნაბიჯში.

ნაბიჯი 2. გავიმეოროთ შემდეგი უნიტარული ოპერაცია $O(N)$-ჯერ.

ა) ვთქვათ სისტემა იმყოფება რაიმე S მდგომარეობაში: თუ $C(S)=1$, შევცვალოთ ფაზა π რადიანით, თუ $C(S)=0$, დავტოვოთ სისტემა შეუცვლელი.

ბ) გამოვიყენოთ $D=\begin{pmatrix} -1+\frac{2}{N} & \frac{2}{N} \\ \frac{2}{N} & -1+\frac{2}{N} \end{pmatrix}$ დიფუზიის ოპერატორი, (რომელიც სამი ელემენტარული მატრიცის საშუალებით მიიღება, იხ. ლემა ქვემოთ).

ნაბიჯი 3. მოვახდინოთ მიღებული მდგომარეობის გაზომვა. ეს მდგომარეობა იქნება საძიებელი S_j მდგომარეობა არანაკლებ 0.5-ის ტოლი ალბათობით.

მეორე ბიჯი არის ალგორითმის ძირითადი ნაწილი. ეს ციკლი იტერაციის ყოველ ბიჯზე $\frac{1}{\sqrt{N}}$-ით ზრდის საძებნი მდგომარეობის ამპლიტუდას. ამიტომ $O(\sqrt{N})$-ჯერ ამ ოპერაციის შესრულების შემდეგ მივიღებთ მდგომარეობას ალბათობით $O(1)$.

იმისათვის, რომ ვაჩვენოთ ამპლიტუდა მართლაც ყოველ ბიჯზე $O\left(\frac{1}{\sqrt{N}}\right)$-ით გაიზრდება, საჭიროა ვაჩვენოთ, რომ D დიფუზია არის *ინვერსია საშუალოს მიმართ*. ჩვეულებრივი ინვერსია ეს არის ფაზის მობრუნება, რომელიც უნიტარულია.

მართლაც, ვთქვათ $a=\frac{1}{N}\sum_{i=1}^{N} a_i$, სადაც a_i არის i-ური მდგომარეობის ამპლიტუდა. D ოპერატორის მოქმედების შედეგად თითოეული მდგომარეობის

ფაზა იზრდება (მცირდება) იმდენით, რამდენითაც ნაკლები იყო შესაბამისი ფაზა a_i-ზე ოპერატორის მოქმედებამდე. ამაში დავრწმუნდებით უშუალო ჩასმით, რაც ამტკიცებს ჩვენს დებულებას.

ლემა. $D = HRH,$ სადაც R არის ფაზის მობრუნების ოპერატორი, ხოლო H კი ადამარის ოპერატორი.

დამტკიცება უშუალოდ ჩასმით მიიღება.

თავი II

კვანტური კომპიუტერის ფიზიკური რეალიზაცია

9. ამოცანის დასმა

კვანტური ნაწილაკების სისტემის კოჰერენტული დინამიკა ყოველთვის ინტენსიური კვლევის საგანს წარმოადგენდა. ამასთან, 80-იანი წლებიდან მოყოლებული, ასეთი სისტემების ინფორმატიკულმა შესაძლებლობებმაც დიდი ყურადღება მიიპყრო [2.1-2.4]. შეიქმნა თანამედროვე საბუნებისმეტყველო მეცნიერების მნიშვნელოვანი მიმართულება–კვანტური ინფორმაციის თეორია. გაჩნდა კვანტური გამოთვლის პროცესზე დაფუძნებული კომპიუტერის შექმნის შესაძლებლობა.

კვანტური გამოთვლის პროცესი უნდა მიმდინარეობს შექცევადი კვანტური პროცესების საფუძველზე (უნიტარული გარდაქმნები), ანუ ფაზის რელაქსაციისა და დისიპაციური პროცესების გარეშე, ხოლო გამოთვლის შედეგების აღქმისათვის, ანუ გამოთვლის შედეგის წასაკითხად, აუცილებელია გაზომვის ჩატარება, რაც კვანტური სისტემის კლასიკურ ხელსაწყოსთან ურთიერთქმედებით ხორციელდება და ბუნებით დისიპაციური პროცესია.

კვანტური გამოთვლების ჩასატარებლად აუცილებელია სამი ძირითადი ელემენტი. უპირველეს ყოვლისა, გარემოსაგან იზოლირებული ორდონიანი კვანტური ნაწილაკების სისტემა (იგულისხმება ნაწილაკთა სისტემა+ვაკუუმი), რომელმაც უნდა შეინარჩუნოს კოჰერენტულობა მთელი გამოთვლის პროცესის განმავლობაში. მეორე, გარეშე კოჰერენტული წყარო, რომელიც კვანტურ ნაწილაკებთან კოჰერენტული ურთიერთქმედების საშუალებით ლოგიკური ოპერაციების განხორციელების საშუალებას მოგვცემს. მესამე, კვანტური გამოთვლების შედეგის ამოსაკითხად, სისტემის კვანტური მდგომარეობების გასაზომი მოწყობილობა.

სადღეისოდ კვანტური გამოთვლების ერთ-ერთი ყველაზე უფრო პოპულარული სქემაა ლოკალიზებული, რადიაციულად გაციებული იონების ურთიერთქმედების პროცესი კონტროლირებად ლაზერული

გამოსხივების იმპულსებთან [2.5-2.9]. უფრო კონკრეტულად კი, კოჰერენტული ურთიერთქმედების შედეგად, იონებში განსაზღვრული სპექტროსკოპიულ გადასვლების რეალიზაციაზე. სწორედ ასეთი ტიპის სქემების რეალიზაციის შესაძლებლობებს ეძღვნება ჩვენი მიმოხილვა.

10. კვანტური სისტემის აღწერა

10.1. ურთიერთქმედების წარმოდგენა

კვანტური გამოთვლებისას მიმდინარე ფიზიკური პროცესების ანალიზისათვის გამოყენებული იქნება ურთიერთქმედების (დირაკის) წარმოდგენა [2.10, 2.11]. ჩვენი ამოცანისათვის ეს მიდგომა ძალზე მოსახერხებელია. ამაში რომ დავრწმუნდეთ თავდაპირველად ნაწილაკისა და გამოსხივების ურთიერთქმედება შრედინგერის სურათით განვიხილოთ. ამ შემთხვევაში კვანტური ნაწილაკის მდგომარეობის დინამიკა დროზე დამოკიდებული $|\psi(t)\rangle$ ტალღური ვექტორით, და დროში უცვლელი $\hat{H}$ ჰამილტონის ოპერატორით აღიწერება

$$\frac{\partial}{\partial t}|\psi(t)\rangle = -\frac{i}{\hbar}\hat{H}\,|\psi(t)\rangle\,. \qquad (2.10-1)$$

ვინაიდან შრედინგერის სურათში $\hat{H}$ დროზე არ არის დამოკიდებული, ამიტომ (10-1) განტოლების ამონახსნს შემდეგი სახე ექნება

$$|\psi(t)\rangle = \exp\left(-\frac{i\hat{H}t}{\hbar}\right)|\psi(0)\rangle\ , \qquad (2.10-2)$$

სადაც $|\psi(0)\rangle$–სისტემის საწყისი მდგომარეობის ვექტორია. გადავიდეთ ურთიერთქმედების წარმოდგენაზე. ნებისმიერ შემთხვევაში სრული სისტემის H ჰამილტონიანი $\hat{H}_A$ თავისუფალი კვანტური ნაწილაკის, $\hat{H}_F$ ელექტრომაგნიტური ველის და მათი ურთიერთქმედების $\hat{H}_I$ ჰამილტონიანების ჯამის სახით შეგვიძლია წარმოვადგინოთ: $\hat{H} = \hat{H}_0 + \hat{H}_I$, სადაც $\hat{H}_0 \equiv \hat{H}_A + \hat{H}_F$ და ვივარაუდოთ, რომ ატომი გადატანით მოძრაობას არ ასრულებს. ამ შემთხვევაში $\hat{H}_0$ დროზე არ არის დამოკიდებული და მდგომარეობის ვექტორი შრედინგერის სურათის შესაბამის ვექტორს ასე უკავშირდება:

$$|\psi_I(t)\rangle = \exp\left(\frac{i\hat{H}_0 t}{\hbar}\right)|\psi(t)\rangle\ , \qquad (2.10-3)$$

ხოლო ურთიერთქმედების წარმოდგენის ოპერატორი შრედინგერის სურათის ოპერატორს – შემდეგი გამოსახულებით

$$\hat{O}_I(t) = \exp\left(\frac{i\hat{H}_0 t}{\hbar}\right)\hat{O}\exp\left(-\frac{i\hat{H}_0 t}{\hbar}\right)\ . \qquad (2.10-4)$$

ჩავსვათ (10-3) გამოსახულება (10-1) განტოლებაში, მივიღებთ

$$\frac{\partial}{\partial t}\,|\psi_I(t)\rangle = -\frac{i}{\hbar}\exp\left(\frac{i\hat{H}_0 t}{\hbar}\right)\hat{H}_I\exp\left(-\frac{i\hat{H}_0 t}{\hbar}\right)|\psi_I(t)\rangle. \qquad (2.10-5)$$

ეს გამოსახულება კი სისტემის დინამიკას აღწერს ურთიერთქმედების წარმოდგენაში. მართლაც (10-4)-ის თანახმად

$$\hat{V}_I(t) = \exp\left(\frac{i\hat{H}_0 t}{\hbar}\right)\hat{H}_I\exp\left(-\frac{i\hat{H}_0 t}{\hbar}\right) \qquad (2.10-6)$$

შრედინგერის სურათის $\hat{H}_I$ ურთიერთქმედების ოპერატორია და შესაბამისი ჩანაცვლების შემდეგ მივიღებთ სისტემის მდგომარეობის განტოლებას ურთიერთქმედების (დირაკის) წარმოდგენაში

$$\frac{\partial}{\partial t}\,|\psi_I(t)\rangle = -\frac{i}{\hbar}\hat{V}_I(t)\,|\psi_I(t)\rangle\ . \qquad (2.10-7)$$

(10-7)-ის თანახმად სისტემის მდგომარეობის ცვლილება, შრედინგერის (10-1) სურათისაგან განსხვავებით, მხოლოდ ურთიერთქმედებისას ხორციელდება. შესაბამისად ამ წარმოდგენაში სისტემის ევოლუცია თვალსაჩინო ხდება. ეს კი მნიშვნელოვნად აადვილებს სხადასხვა ლოგიკური სქემების რეალიზაციის შესაძლებლობების ანალიზს.

10.2 ელექტრომაგნიტური გამოსხივების კლასიკურობის პირობა

ასევე მნიშვნელოვნად ამარტივებს გამოთვლებს ნივთიერებისა და ელექტრომაგნიტური გამოსხივების ურთიერთქმედების ნახევრადკლასიკური მიდგომა თუ ამით პროცესის ფიზიკური სურათი არსებითად არ მახინჯდება. როდესაც კვანტურ სისტემაზე (იონი) ზემოქმედებს ელექტრომაგნიტური გამოსხივება, გარკვეულ შემთხვევებში შესაძლებელი ხდება ამ ველის კლასიკურ ელექტრომაგნიტურ ტალღად წარმოდგენა, ანუ ურთიერთქმედების ნახევრადკლასიკური მიდგომის (მიახლოვების) გამოყენება [2.12, 2.13]. ამ შემთხვევაში იკვანტება მხოლოდ იონის თავისუფლების ხარისხები, ველი კი კლასიკურია. ვინაიდან, როგორც უკვე აღვნიშნეთ, ნახევრადკლასიკური მიდგომა ასევე საგრძნობლად ამარტივებს გამოთვლებს, ამიტომ მნიშვნელოვანია განვსაზღვროთ ის პირობები, როდესაც იგი სამართლიანია. ამრიგად, უნდა განვსაზღვროთ ელექტრომაგნიტური ველის კლასიკურობის პირობა.

როგორც ცნობილია, კვანტურ თეორიაში $\hat{q}$ კოორდინატისა და $\hat{p}$ იმპულსის ოპერატორები ურთიერთშეუღლებულ სიდიდეებს წარმოადგენენ

$$[\hat{q},\hat{p}] = i\hbar\,. \qquad (2.10-8)$$

ელექტრომაგნიტური ველის ერთი მოდის შემთხვევაში, რომელიც ერთეულოვანი მასის მქონე ჰარმონიული ოსცილატორით აღიწერება, კოორდინატს შეესაბამება ვექტორ-პოტენციალის-$\hat{A}$, ხოლო იმპულსს კი– ელექტრული ველის დაძაბულობის-$\hat{E}$ ოპერატორები. ამ შემთხვევაში ელექტრომაგნიტური ველის კლასიკურობის პირობა შემდეგი სახისაა [2.14]

$$\lim_{\hbar\to 0}(\Delta q\cdot\Delta p)\to 0\,. \qquad (2.10-9)$$

ადვილად დავრწმუნდებით რომ ეს პირობა მხოლოდ ელექტრომაგნიტური ველის კოჰერენტული მდგომარეობებისათვის სრულდება

$$|\alpha\rangle=\exp\left(-\frac{1}{2}|\alpha|^2\right)\sum_n\frac{\alpha^n}{(n!)^{1/2}}\,|n\rangle, \qquad (2.10-10)$$

რომელიც სტაციონარული მდგომარეობების სპეციალური სახის სუპერპოზიციას წარმოადგენს. კოჰერენტული მდგომარეობის შემთხვევა-ში

$$\Delta q_\alpha=(\hbar/2\omega)^{1/2},\;\;\Delta p_\alpha=(\hbar\omega/2)^{1/2},\;\;\Delta q_\alpha\cdot\Delta p_\alpha=\hbar/2 \qquad (2.10-11)$$

და შესაბამისად როდესაც $\hbar\to 0$ ვიღებთ, რომ $\Delta q_\alpha=\Delta p_\alpha=0$, რაც კლასიკურ მოძრაობას შეესაბამება (ატომ-ფოტონურ ურთიერთქმედებებში კოჰერენტული გამოსხივების კლასიკური ხასიათის გამოვლენის მკაცრი დამტკი-ცება იხილე [2.13]-ში, ამოცანა 17) ელექტრომაგნიტური ველის კლასიკუ-რობის რაოდენობრივი მახასიათებლის მისაღებად კოჰერენტული გამოსხივების კონკრეტული წყარო განვიხილოთ, კერძოდ–ლაზერის გამოსხივება, რომელიც ფართოდ გამოიყენება კვანტურ გამოთვლებთან დაკავშირებული ექსპერიმენტებში.

ლაზერის გამოსხივების, ანუ $\hbar(\omega_{\rm L}\pm\Delta\omega_{\rm L}/2)$ ფოტონების კვაზიმონოქრომატული ნაკადის $(\Delta\omega_{\rm L}/\omega_{\rm L}\ll 1)$, კლასიკურობა შემდეგი პროცედურით განისაზღვრება [2.12]. კარგადაა ცნობილი, რომ სრული კვანტური მიდგომისას, კვანტური სისტემის მიერ ფოტონის შთანთქმისა და გამოსხივების ამპლიტუდები შესაბამისად $(n_{\mathbf{k}\alpha})^{1/2}$ და $(n_{\mathbf{k}\alpha}+1)^{1/2}$-ის პროპორციულნი არიან. ამ გამოსახულებებში $n_{\mathbf{k}\alpha}$ წარმოადგენს α პოლარიზაციისა და $\mathbf{k}$ ტალღური ვექტორის მქონე ფოტონების რიცხვს. ველი კლასიკურად შეგვიძლია ჩავთვალოთ თუ ორივე პროცესის ალბათობა ტოლია, ანუ თუ $n_{\mathbf{k}\alpha}\gg 1$. ამის შემდეგ უნდა განისაზღვროს ელექტრული ველის დაძაბულობის ის მნიშვნელობები, რომლებიც

მოცემულ პირობას აკმაყოფილებენ. როგორც ცნობილია, მოცულობის ერთეულში ოსცილატორების რაოდენობა შემდეგი გამოსახულებით განისაზღვრება: $\Delta\mathbf{k}/(2\hbar)^3 \propto \omega_{\mathrm{L}}^2\,\Delta\omega_{\mathrm{L}}/c^3$. თუ ჩავთვლით რომ თითოეულ ოსცილატორზე მოდის ერთნაირი ფოტონების $n_{\mathbf{k}\alpha}$ რიცხვი და თითოეული ფოტონის ენერგია $\hbar\omega_{\mathrm{L}}$-ს ტოლია, მივიღებთ რომ ამ მოცულობაში დაგროვილი სრული ენერგია $\hbar\omega_{\mathrm{L}}^3\Delta\omega_{\mathrm{L}}/c^3$-ის ტოლია. მეორეს მხრივ ეს სიდიდე შეგვიძლია განვიხილოთ როგორც E^2. ამრიგად, $n_{\mathbf{k}\alpha} \gg 1$ პირობა ელექტრული ველის დაძაბულობის მნიშვნელობას შემდეგ ექვივალენტურ პირობას ადებს

$$E \gg (\hbar\omega_{\mathrm{L}}^3\Delta\omega_{\mathrm{L}}/c^3)^{1/2} \propto (\hbar c\Delta\lambda_{\mathrm{L}}/\lambda^5)^{1/2}. \qquad (2.10-12)$$

ამ გამოსახულებაში λ_{L} ლაზერის გამოსხივების ტალღის სიგრძეა, ხოლო $\Delta\lambda_{\mathrm{L}}$ გამოსხივების ხაზის სიგანე. ლაზერის გამოსხივების ტიპიური სიდიდეებისათვის ($\lambda_{\mathrm{L}} = 500\,\mathrm{nm}$ და $\Delta\lambda_{\mathrm{L}} \sim 0.01\,\mathrm{nm}$), $E \gg 1\ \mathrm{V/cm}$. ეს პირობა ყოველთვის სრულდება კვანტურ გამოთვლებში გამოყენებული ლაზერული წყაროებისათვის და საერთოდ ლაზერებისათვის თუ მათ ოპერირების ზღურბლზე არ განვიხილავთ.

კიდევ ერთხელ უნდა აღინიშნოს, რომ ელექტრომაგნიტური ველის კლასიკურობის პირობა $(n_{\mathbf{k}\alpha} \gg 1)$ და შესაბამისად (10-12) გამოსახულება სამართლიანია მხოლოდ ველის კოჰერენტული მდგომარეობებისათვის. ელექტრომაგნიტური ველის სხვა მდგომარეობებისათვის, მაგალითად ისეთის, როგორიცაა ფოკის მდგომარეობები, (10-12) გამოსახულების გამოყენება არ არის მართებული.

11. ქუბიტის დინამიკური მახასიათებლები

განვიხილოთ თუ რას წარმოადგენს ფიზიკური სისტემა რომელმაც კვანტური ბიტის, ანუ ქუბიტის ფუნქცია უნდა შეასრულოს. ვინაიდან ჩვენ შემდგომში საქმე სპექტროსკოპიულ გადასვლებთან გვექნება, ამიტომ ლოგიკურ ელემეტად ორდონიანი ატომი (ან იონი) ავირჩიოდ [2.2, 2.4, 2.10]. ხოლო პროცესორად – იდენტური N რაოდენობის ორდონიანი ატომების მძივი. ამ პარაგრაფში მხოლოდ ლოგიკურ ელემენტს, ანუ ორდონიან ატომურ ნაწილაკს განვიხილავთ.

რა თქმა უნდა, ორდონიანი ატომი ბუნებაში არ არსებობს, მაგრამ ოპტიკური რეზონანსის პირობებში [2.15] სწორედ რეალური ატომის (იონის) ორი ენერგეტიკული მდგომარეობა, განსაზღვრავს რა კვანტური

სისტემის დინამიკას, ქმნის ორდონიან სისტემას. ეს კი თავის მხრივ წარმოადგენს ქუბიტის კარგ მოდელს.

ნახ. 11.1

ორდონიანი ქვანტური სისტემა ნახ.11.1-ზეა მოყვანილი. მას გააჩნია ორი ენერგეტიკული დონე (შესაბამისად $\hbar\omega_0$ და $\hbar\omega_1$ ენერგიის მნიშვნელობებით), რომლებიც $\hbar\omega_{10}$-ის ტოლი ენერგიით არიან ერთმანეთისაგან დაცილებულნი. $|0\rangle$ და $|1\rangle$ კვანტური მდგომარეობების ვექტორები $\widehat{H}_A$ შეუშფოთებელი ატომის (იონის) ჰამილტონის ოპერატო-რის საკუთარ მდგომარეობების ვექტორებს წარმოადგენენ, ხოლო მათი საკუთარი მნიშვნელობები კი შესაბამისად ტოლია:

$$\widehat{H}_A\,|0\rangle = \hbar\omega_0\,|0\rangle,$$

(211-1)

$$\widehat{H}_A\,|1\rangle = \hbar\omega_1\,|1\rangle.$$

როგორც ვხედავთ, მოცემული ჰამილტონის ოპერატორი ($\widehat{H}_A$) მხოლოდ ენერგეტიკულ სპექტრს განსაზღვრავს, ხოლო ჩვენ კი ორდონიანი სისტემის - ქუბიტის კვანტური დინამიკა გვაინტერესებს. ამიტომ, დინამიკის აღწერის მიზნით, როგორც ეს ელექტრომაგნიტური ველის დაკვანტვისას ხდება, შემოვიტანოთ ორი არაერმიტული ოპერატორი $\hat{b}$ და $\hat{b}^+$. პირველი მათგანი ამცირებს, ხოლო მეორე კი ზრდის კვანტური სისტემის ენერგიას $\hbar\omega_{10}$ სიდიდით. ვინაიდან სისტემას ორი ენერგეტიკული დონე გააჩნია, ამიტომ $\hat{b}^+$-ის ზემოქმედება უფრო დიდი ენერგიის მქონე დონეზე და შეაბამისად $\hat{b}$-ს ზემოქმედება უფრო მცირე ენერგიის მქონე დონეზე ნულის ტოლია. ყოველივე ზემოთქმული მათემატიკურად ასე გამოისახება:

$$\hat{b}\,|1\rangle = |0\rangle\,,\quad \hat{b}^+\,|1\rangle = 0,$$

(2.11-2)

$$\hat{b}\,|0\rangle = 0\,,\quad \hat{b}^{+}\,|0\rangle = \,|1\rangle.$$

ამ ოპერატორების ხელმეორედ ზემოქმედების შედეგად კი მივიღებთ:

$$\hat{b}\hat{b}^{+}\,|1\rangle = 0\,,\quad \hat{b}^{+}\hat{b}\,|1\rangle = \,|1\rangle,$$

(2.11-3)

$$\hat{b}\hat{b}^{+}\,|0\rangle = \,|0\rangle\,,\quad \hat{b}^{+}\hat{b}\,|0\rangle = 0.$$

ამ გამოსახულებაში $\hat{b}\hat{b}^{+}$ და $\hat{b}^{+}\hat{b}$ შესაბამისად ქვედა და ზედა დონეების *დასახლების* ოპერატორებია 0 და 1 საკუთარი მნიშვნელობებით. ამაში ადვილად დავრწმუნდებით თუ (11-3) გამოსახულების წევრებს მარცხნიდან $\langle 1|$ და $\langle 0|$ მდგომარეობების ვექტორებზე გავამრავლებთ და საკუთარი ვექტორების ორთონორმირების პირობას გავითვალისწინებთ ($\langle\lambda|\lambda'\rangle = \delta_{\lambda\lambda'},\ \lambda,\lambda' = 0,1$):

$$\langle 1|\hat{b}\hat{b}^{+}|1\rangle = 0,\qquad \langle 1|\hat{b}^{+}\hat{b}|1\rangle = 1,$$

(2.11-4)

$$\langle 0|\hat{b}\hat{b}^{+}|0\rangle = 1,\qquad \langle 0|\hat{b}^{+}\hat{b}|0\rangle = 0.$$

ასევე ცხადია, რომ ორჯერ $\hat{b}$ ან $\hat{b}^{+}$ ოპერატორით ზემოქმედება ნებისმიერ მდგომარეობის ვექტორზე ნულის ტოლია. მართლაც, (11-2) გამოსახულებაში განვახორციელებთ ხელმეორედ ზემოქმედებას, მივიღებთ:

$$\hat{b}\hat{b}\,|1\rangle \to \hat{b}\,|0\rangle = 0\,,\ \hat{b}^{+}\hat{b}^{+}\,|1\rangle \to \hat{b}^{+}0 = 0,$$
$$\hat{b}\hat{b}\,|0\rangle \to \hat{b}0 = 0\,,\ \hat{b}^{+}\hat{b}^{+}\,|0\rangle \to \hat{b}^{+}\,|1\rangle = 0,$$

ანუ საზოგადოდ,

$$\hat{b}^{2} = 0 = \left(\hat{b}^{+}\right)^{2}. \qquad (2.11-5)$$

$\hat{b}$ და $\hat{b}^{+}$ ოპერატორების განხილულ თვისებებს შეგვიძლია თავი მოვუყაროთ შემდეგ ანტიკომუტაციურ თანაფარდობებში:

$$\{\hat{b},\hat{b}\} = 0 = \{\hat{b}^{+},\hat{b}^{+}\},$$

(2.11–6)

$$\{\hat{b},\hat{b}^{+}\} = 1\,,$$

სადაც $\{\hat{A},\hat{B}\} \equiv \hat{A}\hat{B} + \hat{B}\hat{A}$, რაც დამახასიათებელია ფერმიონების ალგებრისათვის.

ყოველივე ამის შემდეგ ორდონიანი ატომის (იონის) შინაგანი თავისუფლების ხარისხების შესაბამისი ოპერატორები $\hat{b}$ და $\hat{b}^{+}$ ოპერატორებით გამოვსახოთ. თუ გამოვიყენებთ ერთეულოვან ოპერატორს

$$\sum_{\lambda=0}^{1} |\lambda\rangle\langle\lambda| = 1\,, \qquad (2.11-7)$$

მაშინ ნებისმიერი ოპერატორისათვის გვექნება შემდეგი თანაფარდობა:

$$\hat{O} = \left(\sum_{\lambda=0}^{1} |\lambda\rangle\langle\lambda|\right)\hat{O}\left(\sum_{\lambda=0}^{1} |\lambda\rangle\langle\lambda|\right). \qquad (2.11-8)$$

(11-2), (11-3) და (11-8) გამოსახულებების გამოყენებით მივიღებთ:

$$\hat{b} = |0\rangle\langle 1|$$
$$\hat{b}^{+} = |1\rangle\langle 0| \qquad (2.11–9)$$
$$\hat{b}\hat{b}^{+} = |0\rangle\langle 0|$$
$$\hat{b}^{+}\hat{b} = |1\rangle\langle 1|$$

ამ გამოსახულებაში მოყვანილი ბოლო ორი ოპერატორი ჩვენთვის უკვე ცნობილი ქვედა ($|0\rangle$) და ზედა ($|1\rangle$) დონეების *დასახლების* ოპერატორებია. ჩვენთვის ძალზე მნიშვნელოვანია პირველი ორი ოპერატორი, რომლებზეც აქცენტი არ გაგვიკეთებია. ისინი შესაბამისად ენერგეტიკულ მდგომარეობებს შორის *გადასვლის* ოპერატორებია. სწორედ ეს ოპერატორები განსაზღვრავენ ორდონიანი კვანტური სისტემის დინამიკას: $|0\rangle\langle 1|$ და $|1\rangle\langle 0|$ ოპერატორების ზემოქმედებით ელექტრონი ერთი ენერგეტიკული მდგომარეობიდან მეორეში გადადის. ჩვენი შემდგომი ამოცანაა (11-9) ოპერატორებით ორდონიანი ატომის (იონის) ენერგეტიკული და დინამიკური ოპერატორების გამოსახვა.

(11-8) პროცედურისა და (11-1) შრედინგერის სტაციონარული განტოლების გამოყენებით, ამასთან (11-9) გამოსახულებების გათვალისწინებით, ორდონიანი სისტემის $\hat{H}_A$ ენერგიის ოპერატორი შემდეგ სახეს მიიღებს:

$$\hat{H}_A = \hbar\omega_0 |0\rangle\langle 0| + \hbar\omega_1 |1\rangle\langle 1| = \hbar\omega_0\hat{b}\hat{b}^{+} + \hbar\omega_1\hat{b}^{+}\hat{b}. \qquad (2.11-10)$$

ერთელექტრონულ არარელატივისტურ მიახლოვებაში, რომელიც, როგორც წესი, სამართლიანია კვანტურ გამოთვლებში გამოყენებული ატომური ნაწილაკებისათვის, $|0\rangle$ და $|1\rangle$ მდგომარეობის ვექტორები ზოგადად ასე შეგვიძლია გამოვსახოთ:

$$|n, \ell, m\rangle, \qquad (2.11-11)$$

სადაც n–ძირითადი, ხოლო ℓ და m შესაბამისად ორბიტალური და მაგნიტური კვანტური რიცხვებია.

მეორე მნიშვნელოვანი სიდიდე რომელიც ორდონიან ქვანტურ სისტემას, კერძოდ კი მის დინამიკას ახასიათებს, ეს მისი m რიგის

მულტიპოლური მომენტის $\widehat{M}^{(m)}$ ოპერატორია. ჩვენ შემდგომში მხოლოდ ელექტრული დიპოლური და ელექტრული კვადრუპოლური გადასვლებით დაკავშირებულ დონეებს განვიხილავთ და შესაბამისი $\widehat{M}_E^{(m)}$, სადაც $m = 1,2$, ოპერატორებით ვიმოქმედებთ. (11-8) პროცედურისა და შემდგომ (11-7) და (11-9) გამოსახულებების გამოყენებით მივიღებთ:

$$\begin{aligned}\widehat{M}_E^{(m)} &= (|1\rangle\langle 1| + |0\rangle\langle 0|)\,\widehat{M}_E^{(m)}\,(|1\rangle\langle 1| + |0\rangle\langle 0|)\\ &= M_{E;11}^{(m)}\,|1\rangle\langle 1| + M_{E;00}^{(m)}\,|0\rangle\langle 0| + M_{E;01}^{(m)}\,|0\rangle\langle 1| + M_{E;10}^{(m)}|1\rangle\langle 0|\\ &= M_{E;11}^{(m)}\hat{b}^{+}\hat{b} + M_{E;00}^{(m)}\hat{b}\hat{b}^{+} + M_{E;01}^{(m)}\hat{b} + M_{E;10}^{(m)}\hat{b}^{+},\end{aligned}$$

სადაც $M_{E;ij}^{(m)} \equiv \left\langle i\middle|\widehat{M}_E^{(m)}\middle|j\right\rangle$, $(i,j = 0,1)$–ელექტრული მულტიპოლური მომენტის ოპერატორის მატრიცულ ელემენტს წარმოადგენს. თუ ვივარაუდებთ, რომ ატომს $|0\rangle$ და $|1\rangle$ მდგომარეობებში მუდმივი მულტიპოლური მომენტი არ გააჩნიათ, ანუ $\left\langle 0\middle|\widehat{M}_E^{(m)}\middle|0\right\rangle = \left\langle 1\middle|\widehat{M}_E^{(m)}\middle|1\right\rangle = 0$, მაშინ

$$\widehat{M}_E^{(m)} = M_{E;01}^{(m)}\,|0\rangle\langle 1| + M_{E;10}^{(m)}|1\rangle\langle 0| = M_{E;01}^{(m)}\hat{b} + M_{E;10}^{(m)}\hat{b}^{+}\,. \quad (2.11-12)$$

აქამდე, ოპერატორებს მხოლოდ დროის ფიქსირებულ მომენტში ვიხილავდით. ოპერატორის დროზე დამოკიდებულება რომ გავითვალისწინოთ ამისათვის

$$\frac{d}{dt}\hat{O} = \frac{1}{i\hbar}\left[\hat{O}, \hat{H}_A\right] \quad (2.11-13)$$

ჰაიზენბერგის განტოლებით ვისარგებლოდ. შესაბამისად მულტიპოლური მომენტის ოპერატორისათვის (11-12) გამოსახულებისა და (11-6) კომუტაციური თანაფარდობების გათვალისწინებით მივიღებთ:

$$\frac{d}{dt}\,\widehat{M}_E^{(m)} = -i\omega_{10}\left(M_{E;01}^{(m)}\,|0\rangle\langle 1| - M_{E;10}^{(m)}|1\rangle\langle 0|\right)$$

$$= -i\omega_{10}\left(M_{E;01}^{(m)}\hat{b} + M_{E;10}^{(m)}\hat{b}^{+}\right). \quad (2.11-14)$$

ურთიერთქმედების წარმოდგენაში $\hat{b}$ და $\hat{b}^{+}$ ოპერატორები ასევე დროზე დამოკიდებულნი არიან და (10-4) გამოსახულების თანახმად

$$\hat{b}(t) = \exp\left(\frac{i\widehat{H}_A t}{\hbar}\right)\hat{b}(0)\exp\left(-\frac{i\widehat{H}_A t}{\hbar}\right),$$

$$\hat{b}^+(t) = \exp\left(\frac{i\widehat{H}_A t}{\hbar}\right)\hat{b}^+(0)\exp\left(-\frac{i\widehat{H}_A t}{\hbar}\right), \qquad (2.11-15)$$

თუ ოპერატორულ ექსპონენტას მწკრივის სახით წარმოვადგენთ, ოპერატორის მწკრივად გაშლის თეორემის თანახმად,

$$\exp(x\hat{A})\ \hat{B}\exp(-x\hat{A}) = \hat{B} + x[\hat{A},\hat{B}] + \frac{x^2}{2!}\left[\hat{A},[\hat{A},\hat{B}]\right] + \cdots,$$

მაშინ (11-10) გამოსახულებისა და (11-6) კომუტაციური თანაფარდობების გამოყენებით მივიღებთ:

$$\hat{b}(t) = \hat{b}(0)\exp(-i\omega_{10}t),$$

$$\hat{b}^+(t) = \hat{b}^+(0)\exp(i\omega_{10}t). \qquad (2.11-16)$$

(11-16) გამოსახულების (11-12)-სა და (11-14)-ში ჩასმის შედეგად კი მივიღებთ:

$$\widehat{M}_E^{(m)}(t) = M_{E;01}^{(m)}\,|0\rangle\langle 1|e^{-i\omega_{10}t} + M_{E;10}^{(m)}|1\rangle\langle 0|e^{i\omega_{10}t}$$

$$= M_{E;01}^{(m)}\hat{b}(0)e^{-i\omega_{10}t} + M_{E;10}^{(m)}\hat{b}^+(0)e^{i\omega_{10}t}\,. \qquad (2.11-17)$$

ატომური ნაწილაკის ელექტრული დიპოლმომენტის ოპერატორი

$$\hat{d} \equiv \widehat{M}_E^{(1)} = \sum_n -e_n\,\hat{r}_n \qquad (2.11-18)$$

სიდიდით განისაზღვრება, სადაც $\hat{r}_n$ ატომის$-e$ მუხტის მქონე n–ური ელექტრონის მდებარეობის ოპერატორია. საზოგადოდ, დიპოლური გადასვლები შემდეგ შერჩევის წესებს ემორჩილება:

$$\Delta\ell = \pm 1;\ \ \Delta m = 0, \pm 1\,. \qquad (2.11-19)$$

ამ ფორმით შერჩევის წესები ერთელექტრონულ მიახლოებაში გამოსახება, ანუ როდესაც $\hat{d} = -e\hat{r}$. ერთელექტრონული მიახლოება კი გულისხმობს რომ გარეშე ელექტრომაგნიტურ ველთან ატომური ნაწილაკის–ქუბიტის მხოლოდ გარე შრის ერთი სავალენტო ელექტრონი ურთიერთქმედებს. მეტწილად სწორედ ასეთი ნაწილაკები გამოიყენება კვანტური პროცესორის შესაქმნელად (მაგალითად, იხილე [2.6]-[2.9]).

ერთელექტრონულ მიახლოვებაში ელექტრული დიპოლმომენტისათვის (11-17) გამოსახულება შემდეგ სახეს მიიღებს:

$$\begin{aligned}\hat{d}(t) &= d_{01}\,|0\rangle\langle 1|e^{-i\omega_{10}t} + d_{10}|1\rangle\langle 0|e^{i\omega_{10}t} \\ &= d_{01}\hat{b}(0)e^{-i\omega_{10}t} + d_{10}\hat{b}^{+}(0)e^{i\omega_{10}t} \\ &= \langle 0|\hat{d}|1\rangle\,|0\rangle\langle 1|e^{-i\omega_{10}t} + \langle 1|\hat{d}|0\rangle|1\rangle\langle 0|e^{i\omega_{10}t}\end{aligned}$$

$$= \langle 0|\hat{d}|1\rangle\hat{b}(0)e^{-i\omega_{10}t} + \langle 1|\hat{d}|0\rangle\hat{b}^{+}(0)e^{i\omega_{10}t}, \quad (2.11-20)$$

სადაც

$$d_{ij} \equiv \langle i|\hat{d}|j\rangle = -e\langle i|\hat{r}|j\rangle, \qquad i,j = 0,1 \qquad (2.11-21)$$

დიპოლმომენტის ოპერატორის მატრიცულ ელემენტს წარმოადგენს. $\hat{r}$ სიდიდე ნამდვილი ვექტორია თუ სპექტროსკოპული გადასვლისას მაგნტური კვანტური რიცხვი, m, ინახება, ანუ $\Delta m = 0$, ხოლო $\Delta m = \pm 1$ გადასვლებისათვის ის კომლექსური სიდიდეა [2.16].

ელექტრული კვადრუპოლური მომენტის ოპერატორი

$$\hat{Q} \equiv \hat{M}_E^{(2)} = \frac{1}{2}\sum_n -e_n\,\hat{r}_n\,\hat{r}_n\ , \qquad \hat{r}_n\hat{r}_n \equiv\ |\hat{r}_n\rangle\langle\hat{r}_n|\ , \qquad (2.11-22)$$

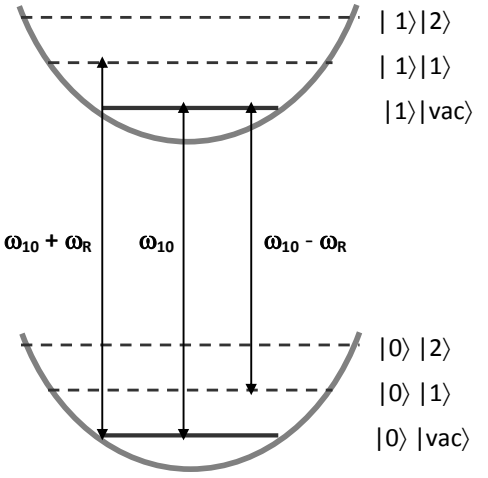
აგრეთვე ორდონიანი კვანტურ სისტემის დინამიკას ახასიათებს. დიდი კოჰერენტულობის დროის გამო ის კვანტური გამოთვლების პროცესში მთავარ როლს ასრულებს. ამ სახის გადასვლები კვანტური გამოთვლებისათვის განსაკუთრებით მნიშვნელოვანია. ორდონიანი სისტემა, რომლის დინამიკას კვადრუპოლური ურთიერთქმედება განსაზღვრავს, დიპოლურთან შედარებით გაცილებით დიდი დროის განმავლობაში ინარჩუნებს კოჰერენტულობას. მაგალითად, თუ ატომის ან იონის ორი დონე $\hbar\omega_{10} = 1.24\,eV$ (ნახ.11.1) ტოლი ენერგიით განსხვავდებიან, მაშინ კვადრუპოლური ურთიერთქმედების კოჰერენტულობის დრო დაახლოებით 10^6-ჯერ აღემატება დიპოლურისას. ურთიერთქმედების ტიპებს უფრო დეტალურად შემდგომ განვიხილავთ. აქ კი მხოლოდ კვადრუპოლური გადასვლებისათვის შერჩევის წესებს მოვიყვანთ:

$$\Delta\ell = 0, \pm 2; \ \ \Delta m = 0, \pm 1, \pm 2\,. \qquad (2.11-23)$$

ამრიგად, ჩვენ მივიღეთ ის ოპერატორები რომლებიც თავისუფალი ორდონიანი კვანტური სისტემის ევოლუციას აღწერენ. სწორედ ელექტროდიპოლური და ელექტრული კვადრუპოლური ურთიერთქმედებები განსაზღვრავენ ქუბიტის დინამიკას, როდესაც მასზე ოპტიკური დიაპაზონის ელექტრომაგნიტური გამოსხივება ზემოქმედებს.

12. კვანტური ნაწილაკების კრებული - ატომური იონების წრფივი მძივი

წინა პარაგრაფში ჩვენ განვიხილეთ იზოლირებული ქუბიტი და მისი დინამიკური მახასიათებლები. ბუნებრივია რომ კვანტური



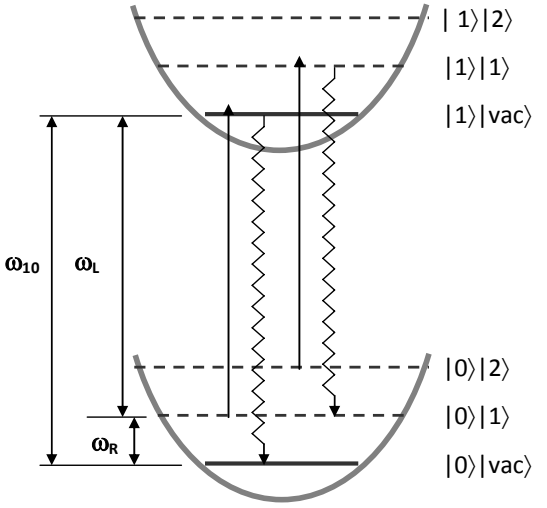
ნახ. 12.1

ჩაჭერილი იონების ენერგეტიკული დონეები. კონკრეტულობისათვის განხილულია რხევის მასათა ცენტრის მოდა. ელექტრონული დონეები აღნიშნულია უწყვეტი ხაზით, ხოლო ელექტრონულ-რხევითი პუნქტირით. ასევე მოყვანილია რაბის გადასვლების (ოსცილაციების) რეალიზაციის შესაძლო სქემები.

აუცილებელია ასეთი ქუბიტების კრებული. თანაც ამ ქუბიტებს შორის უნდა არსებობდეს ინფორმაციული კავშირის რეალიზაციის შესაძლებლობა. ეს კი მაშინაა შესაძლებელი თუ მათ კოლექტიური თავისუფლების ხარისხი გააჩნიათ–მაგალითად, თუ ისინი კოჰერენტულად ირხევიან გარეშე ელექტრომაგნიტურ ველში.

ორდონიან კვანტური ნაწილაკების კრებულის მისაღებად გამოვიყენოთ ატომური იონები. ასეთი სისტემა სივრცეში ლოკალიზებისა (პოტენციალურ ველში) და რადიაციული გაცივების (ლაზერის გამოსხივებით) შემდეგ გარკვეულ პირობებში წარმოქმნის კრისტალურ სტრუქტურას – იონების წრფივ მძივს [2.5, 2.15, 2.6], ანუ სტრუქტურას, რომლის გადატანითი მოძრაობა მკაცრად შეზღუდულია კოორდინატთა ორი ღერძის მიმართ (მაგალითად, y და z მიმართულებე-

ბით). ჩავთვალოთ, რომ მძივის თითოეული იონი x მიმართულებით სუსტად ურთიერთქმედებდეს პოტენციალურ ველთან, რომლის ცვლადი ჰარმონიული კომპონენტი რადიოსიხშირული



ნახ. 12.2

ჩაჭერილი იონების ენერგეტიკული დონეები და გაცივების სქემა. კლაკნილი ხაზებით აღნიშნულია სპონტანური გადასვლები. აქაც, ელექტრონული დონეები აღნიშნულია უწყვეტი ხაზით, ხოლო ელექტრონულ-რხევითი პუნქტირით.

დიაპაზონისაა [2.18]. ასეთი სახის ურთიერთქმედების შემთხვევაში იონების მძივი ისეთ კვანტურ სისტემას წარმოქმნის, რომელიც შედგება კოლექტიურად მერხევი კარგად გარჩევადი იონებისაგან, ანუ თითოეული იონის ენერგეტიკულ სპექტრში თითოეულ ელექტრონულ დონეს გააჩნია რხევითი ექვიდისტანტური სტრუქტურა. ენერგეტიკული მანძილი რხევით დონეებს შორის (ფონონი) $\sqrt{\mu_p}\,\hbar\omega_R$-ის ტოლია, სადაც ω_R პოტენციალური ველის ჰარმონიული კომპონენტის რხევის სიხშირეა, ხოლო μ_p ($\mu_p \geq 0$) დამოკიდებულია რხევის ტიპზე, ანუ რხევით მოდაზე (თვალსაჩინოებისათვის იხილე ნახ.12.1 და ნახ. 12.2).

დავუშვათ, რომ იონების წრფივი მძივი შედგება N იდენტური იონისაგან. როგორც უკვე აღვნიშნეთ იონებს გადატანითი მოძრაობი-

სათვის გააჩნიათ მხოლოდ x მიმართულება. შესაძლებელია თითოელი იონის ფიზიკურად გარჩევა და შესაბამისად მათი გადანომვრა. მარცხნიდან მარჯვნივ გადანომრილი m-ური იონის მდებარეობა აღვნიშნოთ $x_m(t)$-ით. მაშინ მძივში თითოეული იონის მოძრაობა განპირობებული იქნება ჰარმონიული პოტენციალითა და იონებს შორის მოქმედი კულონური ურთიერთქმედებით. შესაბამისად იონების მძივის პოტენციური ენერგია ასე გამოისახება

$$V = \sum_{m=1}^{N} \frac{1}{2} M\, \omega_R^2\, x_m^2(t) + \sum_{\substack{n,m=1 \\ m\neq n}}^{N} \frac{Z^2 e^2}{8\pi\varepsilon_0} \frac{1}{|x_n(t) - x_m(t)|}, \qquad (2.12-1)$$

სადაც M–იონის მასაა, e–ელექტრონის მუხტი, Z–იონიზაციის ხარისხი, ε_0 კი ვაკუუმის დიელექტრიკული მუდმივა. ამ გამოსახულებაში პირველი წევრი შეესაბამება ჰარმონიული რხევების ენერგიას, ხოლო მეორე წევრი კულონურ ურთიერთქმედებას. დავუშვათ, რომ იონები საკმარისად ცივია, ისე რომ m–ური იონის მოძრაობა აპროქსიმირდება $x_m^{(0)}$ წონასწორობის მდებარეობიდან მცირე $q_m(t)$ წანაცვლებით

$$x_m(t) \approx x_m^{(0)} + q_m(t)\,. \qquad (2.12-2)$$

ამ მიახლოებაში იონების გადატანითი მოძრაობა შეგვიძლია აღვწეროთ ნორმალური კოორდინატებითა და შესაბამისად ნორმალური რხევის ტიპებით (მოდებით).

12.1. იონების წონასწორობის მდებარეობები

m–ური იონის წონასწორობის მდებარეობა

$$\left[\frac{\partial V}{\partial x_m}\right]_{x_m = x_m^{(0)}} = 0 \qquad (2.12-3)$$

განტოლებით განისაზღვრება. თუ შემოვიღებთ სიგრძის შემდეგ ერთეულს

$$\ell = \left(\frac{Z^2 e^2}{4\pi\varepsilon_0 M \omega_R^2}\right)^{1/3}, \qquad (2.12-4)$$

მაშინ (12-3) განტოლება სიგრძის ახალ ერთეულებში საბოლოოდ ასე გამოისახება

$$u_m - \sum_{n=1}^{m-1} \frac{1}{(u_m - u_m)^2} + \sum_{n=m+1}^{N} \frac{1}{(u_m - u_m)^2} = 0, \;\; m = 1, 2 \cdots N, \; (2.12-5)$$

სადაც $u_m = x_m^{(0)}/\ell$. (12.5) გამოსახულება წარმოადგენს არაწრფივ ალგებრულ განტოლებათა სისტემას. $N = 2$ და $N = 3$ შემთხვევებისათვის განტოლებათა სისტემა ანალიზურად, კვადრატურებში იხსნება, ხოლო N-ის დიდი მნიშვნელობებისათვის რიცხვითი მეთოდებით [2.6].

12.2. იონების წრფივი მძივის რხევითი მოძრაობა

(12-2) მიახლოების თანახმად, მძივში იონები წონასწორობის წერტილების სიახლოვეს მცირე ამპლიტუდებით ირხევიან. ამ რხევების ხასიათი განპირობებულია იონებს შორის კულონური ურთიერთქმედებითა და გარეშე პოტენციური ველით. შესაბამისად, სისტემის ლაგრანჟიანი შემდეგი სახისაა

$$L = \frac{M}{2}\sum_{m=1}^{N}(\dot{q}_m)^2 - \frac{1}{2}\sum_{n,m=1}^{N} q_n q_m \left[\frac{\partial^2 V}{\partial x_n \partial x_m}\right]_0 . \qquad (2.12-6)$$

მოცემულ გამოსახულებაში წარმოებულები აღებულია $q_n = q_m = 0$ მნიშვნელობისათვის, ანუ წონასწორობის წერტილებისათვის (განტოლებაში ეს აღნიშნულია ”0” ინდექსით). ამასთან, უარყოფილია $O(3)$ რიგის წევრები. მოცემული განტოლების ამონახსნს აქვს შემდეგი სახე:

$$L = \frac{M}{2}\left[\sum_{m=1}^{N}(\dot{q}_m)^2 - \omega_{\mathrm{R}}\sum_{n,m=1}^{N} A_{nm} q_n q_m\right], \qquad (2.12-7)$$

სადაც

$$A_{nm} = \begin{cases} 1 + \sum\limits_{\substack{p=1 \\ p\neq m}}^{N} \dfrac{1}{\left|u_m - u_p\right|^3} & if \quad n = m\,, \\ -\dfrac{2}{|u_m - u_n|^3} & if \quad n \neq m\,. \end{cases} \qquad (2.12-8)$$

უკანასკნელ გამოსახულებაში A_{nm} ნამდვილი, სიმეტრიული და დადებითად განსაზღვრული მატრიცაა. შესაბამისად, იონების მძივის მდგომარეობების $\boldsymbol{b}_m^{(p)}(p = 1,2\cdots,N)$ საკუთრივი ვექტორები შემდეგი გამოსახულებით განისაზღვრებიან

$$\sum_{n=1}^{N} A_{nm}\,\boldsymbol{b}_n^{(p)} = \mu_p \boldsymbol{b}_m^{(p)} (p = 1,2\cdots, N), \qquad (2.12-9)$$

სადაც $\mu_p \geq 0$. მათი გადანომვრა ხორციელდება საკუთარი მნიშვნელობების ზრდის მიხედვით. ამასთან, საკუთრივი ვექტორები ნორმირებულნი არიან შემდეგი პირობებით

$$\sum_{p=1}^{N} \boldsymbol{b}_n^{(p)} \boldsymbol{b}_m^{(p)} = \delta_{nm}\,, \qquad (2.12-10)$$

$$\sum_{n=1}^{N} \boldsymbol{b}_n^{(p)} \boldsymbol{b}_n^{(q)} = \delta_{pq}\,. \qquad (2.12-11)$$

მაგალითად, უმცირესი (μ_1) საკუთრივი მნიშვნელობის შესაბამისი საკუთრივი ვექტორი შემდეგი სახისაა

$$\boldsymbol{b}^{(1)} = \frac{1}{\sqrt{N}}\{1,1,\cdots 1\}, \qquad \mu_1 = 1\,. \qquad (2.12-12)$$

მომდევნო საკუთარი ვექტორი

$$\boldsymbol{b}^{(2)} = \frac{1}{(\sum_{m=1}^{N} u_m^2)^{1/2}}\{u_1, u_2, \cdots u_N\}, \qquad \mu_2 = 3\,. \qquad (2.12-13)$$

მაღალი რიგის საკუთრივი ვექტორები, საზოგადოდ, რიცხვითი მეთოდებით გამოითვლებიან [2.6]. (12-11) და (12-12)–დან აგრეთვე გამომდინარეობს, რომ

$$\sum_{m=1}^{N} \boldsymbol{b}_m^{(p)} = 0, \quad \text{თუ } p \neq 1. \qquad (2.12-13)$$

12.3. იონების მძივის რხევითი მოძრაობა ნორმალურ კოორდინატებში

გამოვსახოთ მძივში იონების მოძრაობა ნორმალურ კოორდინატებში:

$$Q_p(t) = \sum_{m=1}^{N} \boldsymbol{b}_m^{(p)} q_m(t). \qquad (2.12-15)$$

ნორმალური კოორდინატებისათვის (12-7) ლაგრანჟიანი შემდეგ სახეს მიიღებს:

$$L = \frac{M}{2}\sum_{p=1}^{N}\left[\dot{Q}_p^2 - \omega_{\mathrm{R}p}^2 Q_p^2\right], \qquad (2.12-16)$$

სადაც

$$\omega_{\mathrm{R}p} = \sqrt{\mu_p}\,\omega_{\mathrm{R}}\,. \qquad (2.12-17)$$

ამ გამოსახულების თანახმად, Q_p მოდები ერთმანეთთან არ ურთიერთქმედებენ და შესაბამისად კანონიკურად შეუღლებული იმპულსისათვის გვექნება $P_p = M\dot{Q}_p$. ამ შენიშვნების გათვალისწინებით, იონის რხევითი მოძრაობის ჰამილტონიანი შემდეგი სახით დაიწერება:

$$\widehat{H} = \frac{1}{2M}\sum_{p=1}^{N} P_p^2 + \frac{M}{2}\sum_{p=1}^{N} \omega_{\mathrm{R}p}^2 Q_p^2\,. \qquad (2.12-18)$$

ჰამილტონიანის წარმოდგენის შემდეგ შეგვიძლია დავკვანტოთ იონების რხევითი მოძრაობა. ამისათვის შემოვიტანოთ კოორდინატისა და იმპულსის შესაბამისი ოპერატორები

$$Q_p \to \hat{Q}_p = i\sqrt{\frac{\hbar}{2M\omega_{\mathrm{R}p}}}\left(\hat{a}_p - \hat{a}_p^{+}\right), \qquad (2.12-19)$$

$$P_p \to \hat{P}_p = \sqrt{\frac{\hbar M\omega_{\mathrm{R}p}}{2}}\left(\hat{a}_p + \hat{a}_p^{+}\right), \qquad (2.12-20)$$

$\hat{Q}_p$-სა და $\hat{P}_p$-სათვის სამართლიანია შემდეგი ტოლობა: $\left[\hat{Q}_p, \hat{P}_q\right] = i\hbar\delta_{pq}$, ხოლო $\hat{a}_p^{+}$ გაჩენისა და $\hat{a}_p$ გაქრობის ოპერატორებისათვის კი $\left[\hat{a}_p^{+}, \hat{a}_q\right] = \delta_{pq}$. ასეთ აღნიშვნებში m-ური იონის რხევითი მოძრაობა წონასწორობის მიდამოში, ურთიერთქმედების წარმოდგენაში, შემდეგი ოპერატორით აღიწერება:

$$\hat{q}_m(t) = \sum_{p=1}^{N} \boldsymbol{b}_m^{(p)}\,\hat{Q}_p(t) =$$

$$i\sqrt{\frac{\hbar}{2M\omega_{\mathrm{R}}N}}\sum_{p=1}^{N} s_m^{(p)}\left[\hat{a}_p\exp\left(-i\omega_{\mathrm{R}p}t\right) - \hat{a}_p^{+}\exp\left(i\omega_{\mathrm{R}p}t\right)\right], \qquad (2.12-21)$$

სადაც ურთიერთქმედების $s_m^{(p)}$ კონსტანტა შემდეგი გამოსახულებით განისაზღვრება:

$$s_m^{(p)} = \frac{\sqrt{N}\,\boldsymbol{b}_m^{(p)}}{\mu_p^{1/4}}\,. \qquad (2.12-22)$$

როგორც უკვე აღვნიშნეთ, განხილული ურთიერთქმედების შემთხვევაში იონების მძივი ისეთ კვანტურ სისტემას წარმოქმნის, რომ მის ენერგეტიკულ სპექტრში თითოეულ ელექტრონულ დონეს გააჩნია რხევითი ექვიდისტანტური სტრუქტურა. თუ განვიხილავთ შემთხვევას,

როდესაც $p = 1$, მაშინ (12-12) და (12-17) გამოსახულებების თანახმად ენერგეტიკული მანძილი რხევით დონეებს შორის (ფონონი) $\hbar\omega_{\mathrm{R}}$-ის ტოლია, სადაც ω_{R} პოტენციური ველის ჰარმონიული კომპონენტის რხევის სიხშირეა. ასეთი რხევის ტიპს *მასათა ცენტრის* მოდა (CM-მოდა) ეწოდება. ამ შემთხვევაში სისტემა, როგორც მყარი სხეული, ω_{R} სიხშირით ირხევა და

$$s_m^{(1)} = 1\,, \qquad \omega_{R1} = \omega_{\mathrm{R}}\,. \qquad (2.12-23)$$

როდესაც $p = 2$, მაშინ (12-13) და (12-17) გამოსახულებების თანახმად ენერგეტიკული მანძილი რხევით დონეებს შორის (ფონონი) $\sqrt{3}\,\omega_{\mathrm{R}}$-ის ტოლია. ასეთი ტიპის რხევას *სუნთქვით* მოდას უწოდებენ. ამ დროს მძივის თითოეული იონი ირხევა ამპლიტუდით, რომელიც ცენტრიდან შესაბამისი წონასწორობის წერტილების მდებარეობის პროპორციულია. ამ შემთხვევაში

$$s_m^{(2)} = \frac{\sqrt{N}\,\boldsymbol{b}_m^{(p)}}{\sqrt[4]{3}\,(\sum_{m=1}^{N} u_m^2)^{1/2}}\,u_m\,, \quad \omega_{R2} = \sqrt{3}\,\omega_{\mathrm{R}}\,. \qquad (2.12-24)$$

12.4. დასკვნა

ამრიგად, თუ თითოეულ იონში რეზონანსული მეთოდით ორი ელექტრონული დონეს გამოვყოფთ, შესაბამისად $|0\rangle$-ს და $|1\rangle$-ს და იონების მძივში მასათა ცენტრის მოდას აღვძრავთ, მაშინ მის შთანთქმის სპექტრში სამი მაქსიმუმის დამზერა გახდება შესაძლებელი: ცენტრალური მაქსიმუმი ω_{10} სიხშირეზე და გვერდითი მაქსიმუმები $\omega_{10} - \omega_{\mathrm{R}}$ და $\omega_{10} + \omega_{\mathrm{R}}$ სიხშირეებზე. ცენტრალურ მაქსიმუმს $|0\rangle|vac\rangle \leftrightarrow |1\rangle|vac\rangle$ გადასვლა შეესაბამება, ხოლო გვერდით მაქსიმუმებს შესაბამისად $|0\rangle|1phonon\rangle \leftrightarrow |1\rangle|vac\rangle$ და $|0\rangle|vac\rangle \leftrightarrow |1\rangle 1phonon\rangle$ გადასვლები (ნახ.12.1). ამ გადასვლების რეზონანსული ლაზერული გამოსხივებით აღძვრისას შესაძლებელია სხვადასხვა ლოგიკური ოპერაციების განხორციელება. კონკრეტული ლოგიკური ოპერაციის განხორციელება დამოკიდებულია ორდონიანი სისტემისა (ქუბიტის) და რეზონანსული ლაზერული გამოსხივების ურთიერთქმედების სპეციფიკაზე. ეს სპეციფიკა მომდევნო პარაგრაფშია განხილული.

13. ქუბიტის ურთიერთქმედება კლასიკურ ელექტრომაგნიტურ ველთან

13.1. ელექტროდიპოლური და ელექტრული კვადრუპოლური ურთიერთქმედება

იონის ოპტიკური ელექტრონი, რომელიც ურთიერთქმედებს ლაზერულ გამოსხივებასთან, იმყოფება ამ ველის ვექტორულ პოტენციალში. როგორც უკვე არაერთგზის აღვნიშნეთ, ელექტრომაგნიტური ველის პარამეტრები და კონკრეტული იონი ისე უნდა შეირჩნენ, რომ ურთიერთქმდების პროცესმა რაც შეიძლება დიდი ხნის მანძილზე შეინარჩუნოს კოჰერენტული ხასიათი. ამ შემთხვევაში ყველაზე ოპტიმალურია ელექტრული კვადრუპოლური ურთიერთქმედების რეალიზაცია. იგი გაცილებით აღემატება ურთიერთქმედების დროით ელექტროდიპოლურ ურთიერთქმედებას. რაც შეეხება იონების გაცივების პროცესს (რომელსაც აქ არ განვიხილავთ. იხილე ნახ. 12.2) და იონების ჯაჭვზე ჩატარებული ოპერაციების შედეგების წაკითხვას, აქ კი უკვე ენიჭება უპირატესობა ელექტროდიპოლურ ურთიერთქმედებას.

განვიხილოდ m-ური ქუბიტი, რომელიც სივრცის ფიქსირებულ x_m წერტილში კლასიკურ ელექტრომაგნიტურ ველთან ურთიერთქმედებს. ელექტრომაგნიტური ველი $\boldsymbol{A}$ ვექტორ-პოტენციალით აღვწეროთ. ამასთან, ურთიერთქმედების ჰამილტონიანში უგულვებელვყოდ, ჩვენს შემთხვევაში უმნიშვნელო, $e\boldsymbol{A}^2/2m$ წევრი. მაშინ ქუბიტის ველთან ურთიერთქმედების ჰამილტონიანს შემდეგი სახე ექნება:

$$\hat{V}_I(t) = -\frac{e}{m}\hat{\boldsymbol{p}}(t)\cdot\boldsymbol{A}(x_m,t)\,. \qquad (2.13-1)$$

თუ $\boldsymbol{A}(x_m,t)$ ვექტორ-პოტენციალი x_m-ის მახლობლობაში არ იცვლება, მაშინ კვანტური ნაწილაკის კანონიკური იმპულსი ტოლია:

$$\hat{\boldsymbol{p}}(t) = m\dot{\hat{\boldsymbol{r}}}(t) = -\frac{m}{e}\dot{\hat{\boldsymbol{d}}}(t). \qquad (2.13-2)$$

ეს ელექტროდიპოლური მიახლოვებაა, რომლის ჰამილტონიანი (13-2) ოპერატორული ტოლობის გამოყენებით შემდეგ სახეს იღებს:

$$\hat{V}_I^{(ED)}(t) = \dot{\hat{\boldsymbol{d}}}(t)\cdot\boldsymbol{A}(x_m,t). \qquad (2.13-3)$$

თუ კვანტურ ნაწილაკს სპეციალურ პირობებს შევურჩევთ, შესაძლებელი ხდება ელექტროდიპოლური ურთიერთობის გამორთვა. ამ შემთხვევაში მნიშვნელოვანი ხდება ველის მცირე სივრცული ცვლილებები, რომელიც დიპოლური ურთიერთქმედების დროს უმნიშვნელო იყო. ველის სივრცულ ცვლილებებზე დამოკიდებული ურთიერთქმედებებიდან ჩვენი მიზნები-

სათვის ყველაზე მნიშვნელოვანი ელექტრული კვადრუპოლური ურთიერთქმედებაა. განვიხილოთ ეს პროცესი. თუ $\boldsymbol{A}(x_m,t)$ ვექტორ-პოტენციალს x_m-ის მახლობლობაში r-ის მიმართ გავშლით მწკრივად

$$\boldsymbol{A}(x_m+\boldsymbol{r},t)=\boldsymbol{A}(x_m,t)+\left(\boldsymbol{r}\cdot\boldsymbol{\nabla}_{x_m}\right)\boldsymbol{A}(x_m,t)+\cdots. \qquad (2.13-4)$$

და (13-1) ჰამილტონიანში ელექტროდიპოლურ ურთიერთქმედებას გამოვრიცხავთ, მაშინ ურთიერთქმედების ჰამილტონიანი ელექტრული კვადრუპოლური ურთიერთქმედებისათვის შემდეგ სახეს მიიღებს:

$$\hat{V}_I^{(EQ)}(t)=\frac{1}{2}\dot{\hat{\boldsymbol{d}}}\cdot\dot{\hat{\boldsymbol{r}}}\cdot\boldsymbol{\nabla}_{x_m}\boldsymbol{A}(x_m,t), \qquad (2.13-5)$$

ან

$$\hat{V}_I^{(EQ)}(t)=\sum_{i,j}-e\hat{q}_{ij}\frac{\partial}{\partial\hat{r}_i}A_j(x_m,t), \quad i,j=x,y,z, \qquad (2.13-6)$$

სადაც $\hat{q}_{ij}$ – კვადრუპოლური ტენზორია:

$$\hat{q}_{ij}=\frac{1}{2}\left(\hat{r}_i\hat{r}_j-\frac{1}{3}\delta_{ij}\hat{r}_i^2\right). \qquad (2.13-7)$$

ახლა კი ლაზერის გამოსხივების ველში ელექტროდიპოლური და ელექტრული კვადრუპოლური გადასვლებით გამოწვეული სპექტროსკოპიული გადასვლები განვიხილოთ.

13.2. ელექტროდიპოლური და ელექრტული კვადრუპოლური გადასვლები ლაზერის გამოსხივების ველში

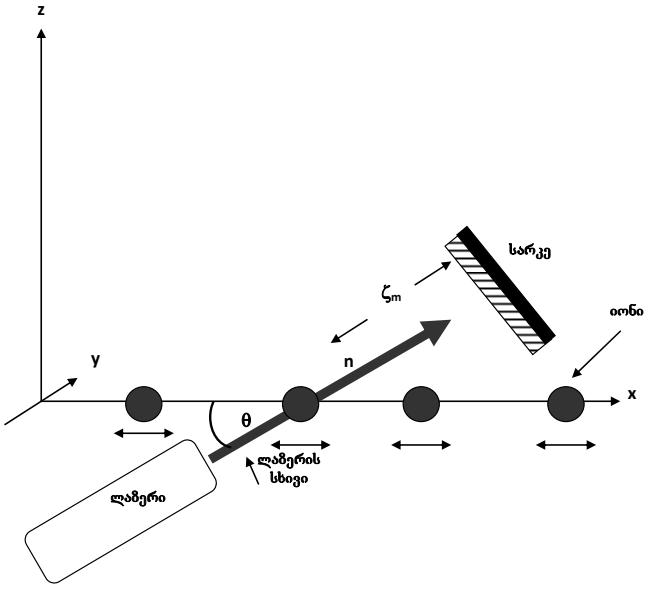
(13-3)-დან გამომდინარე და (11-20) გამოსახულებების დახმარებით, $\hat{V}_I^{(ED)}$ ელექტროდიპოლური ურთიერთქმედების ჰამილტონიანი ურთიერთქმედების წარმოდგენაში შემდეგ სახეს მიიღებს:

$$\hat{V}_I^{(ED)}(t)=i\omega_{10}\left(\boldsymbol{d}_{01}|0\rangle\langle 1|e^{-i\omega_{10}t}-\boldsymbol{d}_{10}|1\rangle\langle 0|e^{i\omega_{10}t}\right)A_i(x_m,t). \quad (2.13\text{-}8)$$

თუ ამ გამოსახულებაში დიპოლური გადასვლების მატრიცულ ელემენტებს (11-21) ფორმით გამოვსახავთ, მაშინ

$$\hat{V}_I^{(ED)}(t)=$$
$$-ie\omega_{10}\left(\langle 0|\hat{r}_i|1\rangle|0\rangle\langle 1|e^{-i\omega_{10}t}-\langle 1|\hat{r}_i|0\rangle|1\rangle\langle 0|e^{i\omega_{10}t}\right)A_i(x_m,t), \quad i=x,y,z. \qquad (2.13-9)$$

(13-7), (11-17) და (11-21) გამოსახულებების საშუალებით ელექტრული კვადრუპოლური გადასვლებისათვის მივიღებთ შემდეგი სახის ჰამილტონიანს:



ნახ. 13.1

იონების მძივზე ლაზერის სხივის ზემოქმედების ზოგადი სურათი. ლაზერის სხივი წარმოქმნის მდგარი ტალღის კონფიგურაციას.

$$\hat{V}_I^{(EQ)}(t) = -\frac{ie\omega_{10}}{2}\left(\langle 0|\hat{r}_i\hat{r}_j|1\rangle|0\rangle\langle 1|e^{-i\omega_{10}t} - \langle 1|\hat{r}_i\hat{r}_j|0\rangle|1\rangle\langle 0|e^{i\omega_{10}t}\right)\partial_i A_j(x_m,t),$$

$$i,j = x,y,z. \qquad (2.13-10)$$

(13-9) და (13-10) გამოსახულებებში $A_j(x_m,t)$–ვექტორ-პოტენციალის j-ური კომპონენტია, ∂_i–i-ური მიმართულებით დიფერენცირების ოპერატორს აღნიშნავს, $\hat{r}_i$–სავალენტო ელექტრონის მდებარეობის ოპერატორის i-ური კომპონენტია.

შემდგომი ანალიზისათვის ელექტრომაგნიტური ველის კონფიგურაცია უნდა დავაკონკრეტოთ. შემთხვევას, რომელსაც ჩვენ განვიხილავთ, ლაზერის გამოსხივების ველს, პარაგრაფ 10.2-ში ჩატარებული ანალიზზე დაყრდნობით, შეგვიძლია მივცეთ კლასიკური ბრტყელი ელექტრომაგნიტური ტალღის სახე.

ელექტრომაგნიტური ველის კონფიგურაცია

ქუბიტზე ზემოქმედებისათვის გამოვიყენოთ ლაზერის სხივის მდგარი ტალღის კონფიგურაცია. ამის მისაღწევად ლაზერის სხივს გავრცელების გზაზე, რომელიც $\boldsymbol{n}$ ერთეულოვანი ვექტორით აღიწერება, დავახვედროთ ამრეკლი ზედაპირი – სარკე (ნახ. 13.1). შესაბამისად, სარკისაკენ მოძრავი და მისგან არეკვლილი მსრბოლი ტალღების ზედდება მოგვცემს ველის შემდეგ კონფიგურაციებს:

$$A_i(x_m,t) = -\boldsymbol{\epsilon}_i \frac{E}{\omega_L}\sin\left[k\hat{\zeta}_m(t)\right] e^{i\omega_L t} + \text{c. c.}, \qquad (2.13-11)$$

$$\partial_i A_j(x_m,t) = -n_i\boldsymbol{\epsilon}_j \frac{E}{c}\cos\left[k\hat{\zeta}_m(t)\right] e^{i\omega_L t} + \text{c. c.}. \qquad (2.13-12)$$

(13-11) წარმოადგენს ელექტრული დიპოლის, ხოლო (13-12) ელექტრული კვადრუპოლის მიერ "დანახულ" ველს. ამ გამოსახულებებში E – ელექტრული ველის ამპლიტუდაა, ω_L – ლაზერის გამოსხივების სიხშირე, $k=\omega_L/c$ – ტალღური რიცხვია, $\hat{\zeta}_m(t)$ – მანძილია m-ური კვანტური ნაწილაკიდან სარკის ზედაპირამდე.

ქუბიტების განლაგება მდგარი ტალღის ველში

მდგარი ტალღის ველში ქუბიტზე ზემოქმედებისათვის ორი პოზიცია შევარჩიოთ: *(i)* მდგარი ტალღის კვანძები, სადაც ველის დაძაბულობა ნულს უტოლდება და *(ii)* მდგარი ტალღის ბურცობები, სადაც ველის დაძაბულობა მაქსიმალურია. პირველი პირობა ასე ჩაიწერება:

$$\hat{\zeta}_m(t) = \ell\lambda_L + \cos\theta\ \hat{q}_m(t), \qquad (2.13-13)$$

ხოლო მეორე კი -

$$\hat{\zeta}_m(t) = \frac{(2\ell-1)\lambda_L}{2} + \cos\theta\ \hat{q}_m(t). \qquad (2.13-14)$$

ამ გამოსახულებებში ℓ – ნებისმიერი მთელი რიცხვია, θ – იონების კოლექტიური რხევის მიმართულებასა და ლაზერის სხივის მიმართულებას შორის კუთხეა, λ_L – ლაზერის გამოსხივების ტალღის სიგრძეა. $\cos\theta\ \hat{q}_m(t)$ სიდიდე (12-21) თანახმად ტოლია

$$\cos\theta\ \hat{q}_m(t) = \frac{i}{k\sqrt{N}}\eta\sum_{p=1}^{N} s_m^{(p)}\left(\hat{a}_p e^{-i\omega_{\mathrm{R}p}t} - \hat{a}_p^{+} e^{i\omega_{\mathrm{R}p}t}\right), \qquad (2.13-15)$$

სადაც

$$\eta = \sqrt{\hbar\, k^2 \cos^2\theta / 2M\omega_{\mathrm{R}} N} \qquad (2.13-16)$$

სიდიდეს ლემბისა და დიკეს პარამეტრს უწოდებენ.

ამრიგად, ჩვენ გაგვაჩნია ყველა მონაცემი იმისათვის, რომ შევისწავლოთ ელექტრომაგნიტურ ველში მოთავსებული ქუბიტისა და ქუბიტების მძივის დინამიკა.

14. ქუბიტისა და ქუბიტების მძივის დინამიკა ლაზერის გამოსხივების ველში

14.1. ეფექტური ურთიერთქმედების ჰამილტონიანები

ამრიგად, (13-11) და (13-12) გამოსახულებების (13.9) და (13.10) გამოსახულებებში შეტანით ელექტროდიპოლური და ელექტრული კვადრუპოლური ურთიერთქმედების ჰამილტონიანები მიიღებენ შემდეგ სახეს:

$$\begin{aligned}&\hat{V}_I^{(ED)}(t) = \\ &i\frac{\omega_{10}}{\omega_L} eE\boldsymbol{\epsilon}_i\big[\langle 0|\hat{r}_i|1\rangle|0\rangle\langle 1|e^{it(\omega_L-\omega_{10})} - \\ &\langle 1|\hat{r}_i|0\rangle|1\rangle\langle 0|e^{it(\omega_L+\omega_{10})}\big]\sin\big[k\hat{\zeta}_m(t)\big] + c.c.,\end{aligned} \qquad (2.14-1)$$

$$\begin{aligned}&\hat{V}_I^{(ED)}(t) = \\ &i\frac{eE\omega_{10}}{2c}\boldsymbol{\epsilon}_i n_j\big[\langle 0|\hat{r}_i\hat{r}_j|1\rangle|0\rangle\langle 1|e^{it(\omega_L-\omega_{10})} - \\ &\langle 1|\hat{r}_i\hat{r}_j|0\rangle|1\rangle\langle 0|e^{it(\omega_L+\omega_{10})}\big]\cos\big[k\hat{\zeta}_m(t)\big] + c.c..\end{aligned} \qquad (2.14-2)$$

(14-1) და (14-2) ჰამილტონიანებში გამოვიყენოთ მბრუნავი ტალღის მიახლოება (Rotating Wave Approximation). ეს მიახლოება სამართლიანი იქნება თუ კვაზირეზონანსული ლაზერული გამოსხივებით m-ურ ქუბიტზე ვიმოქმედებთ. რაც იმას ნიშნავს, რომ ლაზერის კვანტის ენერგია დაახლოებით ტოლია ქუბიტის დონეებს შორის ენერგეტიკული მანძილისა, ანუ:

$$\hbar\omega_L \cong \hbar\omega_{10}\,, \qquad (2.14-3)$$

და შესაბამისად (14-1) და (14-2) ურთიერთქმედებების ჰამილტონიანებში $(\omega_L + \omega_{10})$ სწრაფადოსცილირებადი წევრები შეგვიძლია უგულვებელ-ყოთ. მივიღებთ

$$\hat{V}_I^{(ED)}(t) = \hbar\Omega_0^{(ED)} \sin\left[k\hat{\zeta}_m(t)\right] |0\rangle\langle 1| e^{i(t\Delta-\phi)} + h.a., \qquad (2.14-4)$$

$$\hat{V}_I^{(EQ)}(t) = i\hbar\Omega_0^{(EQ)} \cos\left[k\hat{\zeta}_m(t)\right] |0\rangle\langle 1| e^{i(t\Delta-\phi)} + h.a., \qquad (2.14-5)$$

სადაც შემოტანილია შემდეგი აღნიშვნები:

$$\Omega_0^{(ED)} \equiv \left|\frac{eE}{\hbar}\langle 0|\hat{r}_i|1\rangle \boldsymbol{\epsilon}_i\right|,$$
$$\Omega_0^{(EQ)} \equiv \left|\frac{eE\omega_{10}}{2\hbar c}\langle 0|\hat{r}_i\hat{r}_j|1\rangle \boldsymbol{\epsilon}_i n_j\right|, \qquad (2.14-6)$$

$$\phi \equiv \arg\left\{\Omega_0^{(ED)}\right\}, \arg\left\{\Omega_0^{(EQ)}\right\}, \qquad (2.14-7)$$

$$\Delta \equiv \omega_L - \omega_{10}\,. \qquad (2.14-8)$$

$\Omega_0^{(ED)}$ და $\Omega_0^{(EQ)}$ სიდიდეები რაბის სიხშირეებს წარმოადგენენ (ენერგეტიკულ დონეებს შორის ელექტრონის კოჰერენტული ოსცილაციების სიხშირე).

როგორც უკვე ვნახეთ, ცივი იონი x ღერძის გასწვრივ მცირე რხევით მოძრაობას ასრულებს (იხილე (12-2) და მიმდებარე ტექსტი). ამასთან, შემდგომში იონების კოლექტიური მოძრაობიდან მხოლოდ მასათა ცენტრის მოძრაობას ანუ CM- მოდას განვიხილავთ, ხოლო ამ რეჟიმში კი ცივი იონის რხევის ამპლიტუდა მნიშვნელოვნად მცირეა ტალღის სიგრძეზე (ლემბისა და დიკეს რეჟიმი [2.16]), რაც საშუალებას გვაძლევს სარკის მოძრაობით იონი შერჩევით მდგარი ტალღის კვანძში ან ბურცობში მოვათავსოთ. რა ხდება თითოეულ ასეთ წერტილში? ამის გასარკვევად ველის ვექტორ-პოტენციალის სივრცული ნაწილი მდგარი ტალღის კვანძსა და ბურცობში $\hat{q}_m(t)$-ის მიმართ მწკრივად გავშალოთ და წრფივი წევრებით შემოვისაზღვროთ. (13-11)-(13-13) გამოსახულებების გათვალისწინებით კვანძებში მივიღებთ:

$$\sin\left[k\hat{\zeta}_m(t)\right] = \sin\{k[\ell\lambda_L + \cos\theta\ \hat{q}_m(t)]\}$$
$$\approx \sin(k\ell\lambda_L) + k\cos\theta\ \hat{q}_m(t)\cos(k\ell\lambda_L), \qquad (2.14-9)$$

$$\cos\left[k\hat{\zeta}_m(t)\right] = \cos\{k[\ell\lambda_L + \cos\theta\ \hat{q}_m(t)]\} \approx$$
$$\approx \cos(k\ell\lambda_L) - k\cos\theta\ \hat{q}_m(t)\sin(k\ell\lambda_L), \qquad (2.14\text{-}10)$$

ვინაიდან (14-9) გამოსახულების მარჯვენა მხარის მეორე წევრი სარკის მოტრიალებით, ანუ $\cos\theta$-ს ცვლილებით, ყოველთვის შეგვიძლია ნულის ტოლი გავხადოთ, ამიტომ ველის კვანძებში მოსახვედრად (14-9)-ის მარჯვენა მხარის პირველი წევრისათვის უნდა შესრულდეს $k\ell\lambda_L = \ell\pi$ პირობა და აქედან გამომდინარე კი (14-1) და (14-2) გამოსახულებები კვანძებში შემდეგ სახეზე დავლენ:

კვანძები:

$$\begin{cases} \sin\left[k\hat{\zeta}_m(t)\right] = k\cos\theta\ \hat{q}_m(t)\cos(\ell\pi) \\ \cos\left[k\hat{\zeta}_m(t)\right] = \cos(\ell\pi) \end{cases}. \qquad (2.14-11)$$

ამრიგად, (14-11) გამოსახულებების გათვალისწინებით (14-4) ელექტრო-დიპოლური და (14-5) ელექტული კვადრუპოლური ურთიერთქმედების ჰამილტონიანები შემდეგ სახეს მიიღებენ:

$$\hat{V}_I^{(ED)}(t) = \hbar\Omega_0^{(ED)} k\cos\theta\ \hat{q}_m(t)|0\rangle\langle 1|e^{i(t\Delta-\phi+\ell\pi)} + h.a., \quad (2.14-12)$$

$$\hat{V}_I^{(EQ)}(t) = \hbar\Omega_0^{(EQ)}|0\rangle\langle 1|e^{i[t\Delta-\phi-(\ell+1/2)\pi]} + h.a., \qquad (2.14-13)$$

აქ ვისარგებლეთ კარგად ცნობილი გამოსახულებებით:

$$\cos(\ell\pi) = \exp(i\ell\pi),\ i\cos(\ell\pi) = \exp\left[i\left(\ell+\frac{1}{2}\right)\pi\right]. \qquad (2.14-14)$$

ამრიგად, მდგარი ტალღის კვანძში ქუბიტის დინამიკას განსაზღვრავს ორი სახის ოპერატორი. ელექტრული კვადრუპოლური ურთიერთქმედების ოპერატორი ზემოქმედებს მხოლოდ ქუბიტის შიგა თავისუფლების ხარისხებზე ანუ ქუბიტის ინდივიდუალურ ელექტრონულ დონეებზე, ხოლო ელექტროდიპოლური ურთიერთქმედების ოპერატორი კი ქუბიტის ელექტრონულ-რხევითი დონის საშუალებით ქუბიტების კოლექტიური თავისუფლების ხარისხზეც მოქმედებს. ამ ურთიერთქმე-დებებს სიმარტივისათვის შემდგომში U და V ტიპის ურთიერთქმედებებს ვუწოდებთ [2.5, 2.6] და ჰამილტონიანებს შესაბამის ნიშნაკებს მივაწერთ. (13-15) გამოსახულების გათვალისწინებით მივიღებთ:

$$\hat{V}_U^{(ED)}(t) =$$
$$i\frac{\hbar\Omega_0^{(ED)}}{\sqrt{N}}\eta\ \sum_{p=1}^{N} s_m^{(p)}\left(\hat{a}_p e^{-i\omega_{\mathrm{R}p}t} - \hat{a}_p^{+} e^{i\omega_{\mathrm{R}p}t}\right)|0\rangle\langle 1|e^{i(t\Delta-\phi+\ell\pi)} + h.a., \qquad (2.14-15)$$

$$\hat{V}_I^{(EQ)}(t) = \hbar\Omega_0^{(EQ)}|0\rangle\langle 1|e^{i[t\Delta-\phi-(\ell+1/2)\pi]} + h.a., \qquad (2.14-16)$$

ახლა მდგარი ტალღის ბურცობებში მოთავსებულ ქუბიტებზე მოქმედი ეფექტური ოპერატორები ვიპოვოთ. ამისათვის (13-11), (13-12) და (13-14) გამოსახულებებით ვისარგებლოთ. მათი საშუალებით ბურცობებში ველის სივრცული ნაწილისათვის შემდეგ გამოსახულებებს მივიღებთ:

$$\sin\left[k\hat{\zeta}_m(t)\right] = \sin\{k[(\ell - 1/2)\lambda_L + \cos\theta\ \hat{q}_m(t)]\}$$

$$\approx \sin[k(\ell - 1/2)\lambda_L] + k\cos\theta\ \hat{q}_m(t)\cos[k(\ell - 1/2)\lambda_L], \qquad (2.14-17)$$

$$\cos\left[k\hat{\zeta}_m(t)\right] = \cos\{k[(\ell - 1/2)\lambda_L + \cos\theta\ \hat{q}_m(t)]\}$$

$$\approx \cos[k(\ell - 1/2)\lambda_L] - k\cos\theta\ \hat{q}_m(t)\sin[k(\ell - 1/2)\lambda_L], \quad (2.14-18)$$

ვინაიდან ბურცობებისათვის სრულდება პირობა: $k(\ell - 1/2)\lambda_L = (\ell - 1/2)\pi$, ამიტომ (14-17) და (14-18) გამოსახულებები ბურცობებში შემდეგ სახეზე დავლენ:

ბურცობები:

$$\begin{cases} \sin\left[k\hat{\zeta}_m(t)\right] = -\cos(\ell\pi), \\ \cos\left[k\hat{\zeta}_m(t)\right] = k\cos\theta\ \hat{q}_m(t)\cos(\ell\pi). \end{cases} \qquad (2.14-19)$$

ამრიგად, (14-4), (14-5), (14-19) გამოსახულებებისა და (13-15)-ის გავითვალისწინებით ბურცობებში ელექტროდიპოლური და ელექტრული კვადრუპოლური ურთიერთქმედების ჰამილტონიანები მიიღებენ შემდეგ სახეს:

$$\hat{V}_V^{(ED)}(t) = \hbar\Omega_0^{(ED)}\,|0\rangle\langle 1|e^{i(t\Delta-\phi+\ell\pi)} + h.a., \quad (2.14-20)$$

$$\hat{V}_U^{(EQ)}(t) = i\frac{\hbar\Omega_0^{(EQ)}}{\sqrt{N}}\eta\ \sum_{p=1}^{N} s_m^{(p)}\left(\hat{a}_p e^{-i\omega_{\mathrm{R}p}t} - \hat{a}_p^{+}e^{i\omega_{\mathrm{R}p}t}\right)|0\rangle\langle 1|e^{i[t\Delta-\phi-(\ell+1/2)\pi]} + h.a.. \qquad (2.14-21)$$

ამრიგად, თუ ოპერატორებს ურთიერთქმედების ტიპის მიხედვით დავალაგებთ კვანტური გამოთვლითი პროცესის ასამოქმედებლად დაგვჭირდება შემდეგი ორი ტიპის ოპერატორი:

$$\hat{V}(t) = \begin{cases} \hat{V}_V^{(ED)}(t) \\ \text{or} \\ \hat{V}_V^{(EQ)}(t) \end{cases} =$$

$$= \begin{cases} \hbar\Omega_0^{(ED)} \, |0\rangle\langle 1| e^{i(t\Delta - \phi + \ell\pi)} + h.a. \\ \text{or} \\ \hbar\Omega_0^{(EQ)} \, |0\rangle\langle 1| e^{i[t\Delta - \phi - (\ell+1/2)\pi]} + h.a. \end{cases} = \hbar\Omega_0 |0\rangle\langle 1| e^{i(t\Delta - \phi_V)} + h.a. \qquad (2.14-22)$$

და

$$\hat{U}(t) = \begin{cases} \hat{V}_U^{(ED)}(t) \\ \text{or} \\ \hat{V}_U^{(EQ)}(t) \end{cases} =$$

$$= \begin{cases} i\dfrac{\hbar\Omega_0^{(ED)}}{\sqrt{N}}\eta \sum_{p=1}^{N} s_m^{(p)} \left(\hat{a}_p e^{-i\omega_{\mathrm{R}p}t} - \hat{a}_p^+ e^{i\omega_{\mathrm{R}p}t}\right)|0\rangle\langle 1| e^{i(t\Delta - \phi + \ell\pi)} + h.a. \\ \text{or} \\ i\dfrac{\hbar\Omega_0^{(EQ)}}{\sqrt{N}}\eta \sum_{p=1}^{N} s_m^{(p)} \left(\hat{a}_p e^{-i\omega_{\mathrm{R}p}t} - \hat{a}_p^+ e^{i\omega_{\mathrm{R}p}t}\right)|0\rangle\langle 1| e^{i[t\Delta - \phi - (\ell+1/2)\pi]} + h.a. \end{cases}$$

$$= i\hbar\Omega_0 \tfrac{\eta}{\sqrt{N}} \textstyle\sum_{p=1}^{N} s_m^{(p)} \left(\hat{a}_p e^{-i\omega_{\mathrm{R}p}t} - \hat{a}_p^+ e^{i\omega_{\mathrm{R}p}t}\right)|0\rangle\langle 1| e^{i(t\Delta - \phi_U)} + h.a.. \qquad (2.14-23)$$

სარკის მოძრაობით ერთი ტიპის ოპერატორის მოქმედება შეიცვლება მეორე ტიპის ოპერატორის მოქმედებით. ამასთან თუ ქუბიტზე პირველი ზემოქმედებისას საწყისი ფაზა ნებისმიერია, შემდგომი ზემოქმედებისას ფაზა ფიქსირდება, რაც აუცილებლად უნდა გავითვალისწინოთ. ეს პროცესების კოჰერენტულობითაა გამოწვეული.

14.2. პროცესორში ქუბიტის დინამიკა

ინდივიდუალურ ქუბიტზე ზემოქმედების მოსახდენად $\hat{V}$ ტიპის ოპერატორით ვსარგებლობთ. სიმარტივისათვის განვიხილოთ ზუსტი

რეზონანსის შემთხვევა, ანუ როდესაც $\Delta = 0$. ამ შემთხვევაში (14-22)-დან ვიღებთ:

$$\hat{V}(t) = \hbar\Omega_0|0\rangle\langle 1|e^{-i\phi_V} + h.a.. \qquad (2.14-24)$$

ამრიგად, მივიღეთ $\hat{V}$-ტიპის ურთიერთქმედების ოპერატორის ზოგადი გამოსახულება, რომელიც ზუსტი რეზონანსის შემთხვევაში ქუბიტის კვანტურ დინამიკას აღწერს. ურთიერთქმედების წარმოდგენაში (იხილე პარაგრაფი 10) ქუბიტის დინამიკის განტოლებას და ტალღურ ფუნქციას შემდეგი სახე ექნებათ:

$$\frac{\partial}{\partial t}|\psi_I(t)\rangle = -\frac{i}{\hbar}\hat{V}(t)|\psi_I(t)\rangle\,, \qquad (2.14-25)$$

$$|\psi_I(t)\rangle = a_0(t)|0\rangle + a_1(t)|1\rangle. \qquad (2.14-26)$$

(14-24) და (14-26) გამოსახულებების ჩასმით (14-25) მოძრაობის განტოლებაში, საკუთრივი ვექტორების ორთონორმირების პირობის გათვალისწინებით ($\langle\lambda|\lambda'\rangle = \delta_{\lambda\lambda'}$) $a_0(t)$ და $a_1(t)$ კოეფიციენტებისათვის შემდეგ განტოლებათა სისტემას მივიღებთ:

$$\frac{d}{dt}a_0(t) = -i\Omega_0 a_1(t)e^{-i\phi_V},$$

$$\frac{d}{dt}a_1(t) = -i\Omega_0 a_0(t)e^{i\phi_V}. \qquad (2.14-27)$$

ამ განტოლებათა სისტემიდან ვიღებთ ჰარმონიული ოსცილატორის განტოლებას:

$$\frac{d^2}{dt^2}a_0(t) + \Omega_0^2 a_0(t) = 0, \qquad (2.14-28)$$

რომლის ამონახსნი კარგად არის ცნობილი და მას შემდეგი სახე აქვს:

$$a_0(t) = A\cos\Omega_0 t + B\sin\Omega_0 t.$$

ამ ამონახსნის (14-27)-ის პირველ განტოლებაში ჩასმის შედეგ ვიღებთ:

$$a_1(t) = (iA\sin\Omega_0 t - iB\cos\Omega_0 t)e^{i\phi_V}$$

$t = 0$ პირობიდან ვიღებთ, რომ:

$$A = a_0(0), \qquad B = ia_1(0)\,e^{-i\phi_V},$$

საიდანაც ვპოულობთ (14-26) სუპერპოზიციის კოეფიციენტებს:

$$a_0(t) = a_0(0)\cos\ {}_0t + ia_1(0)\,e^{-i\phi_V}\sin\ {}_0t\,, \qquad (2.14-29)$$

$$a_1(t) = a_1(0)\cos\ {}_0t + ia_0(0)e^{i\phi_V}\sin\ {}_0t\,, \qquad (2.14-30)$$

ან მატრიცული სახით:

$$\begin{pmatrix} a_0(t) \\ a_1(t) \end{pmatrix} = \begin{pmatrix} \cos\ {}_0t & i\,e^{-i\phi_V}\sin\ {}_0t \\ i\,e^{i\phi_V}\sin\ {}_0t & \cos\ {}_0t \end{pmatrix}\begin{pmatrix} a_0(0) \\ a_1(0) \end{pmatrix}. \qquad (2.14-31)$$

ამრიგად, თუ m-ური ქუბიტის $|0\rangle$ მდგომარეობაზე რეზონანსული ლაზერული გამოსხივების იმპლუსით ვიმოქმედებთ, მაშინ ფაზისა და

იმპულსის ხანგრძლივობის შერჩევით პრინციპში შესაძლებელი ხდება $|0\rangle$ და $|1\rangle$ მდგომარეობების ნებისმიერი სუპერპოზიციის მიღება. ასეთი სახის ოპერაცია გამხოლოებულ ქუბიტზე წარმოებულ ექვივალენტურ უნიტარულ გარდაქმნებს წარმოადგენს:

$$\hat{V}_m(\Theta,\phi_V):\ \begin{matrix} |0\rangle_m \to \cos\Theta\,|0\rangle_m - \ i\,e^{i\phi_V}\sin\Theta\ |1\rangle_m \\ |1\rangle_m \to \cos\Theta\,|1\rangle_m - i\,e^{-i\phi_V}\sin\Theta\,|0\rangle_m \end{matrix} \qquad (2.14-32)$$

სადაც შემოტანილია შემდეგი აღნიშვნა:

$$\Theta \equiv \Omega_0 t\,. \qquad (2.14-33)$$

14.3. პროცესორში ქუბიტების მძივის დინამიკა

ამჯერად, რეზონანსული ლაზერული გამოსხივებით იონური მძივის კოლექტიური თავისუფლების ხარისხებზე ვიმოქმედოთ, ანუ განვახორციელოთ U-ტიპის ურთიერთქმედება. როგორც უკვე აღვნიშნეთ (იხილე პარაგრაფი 12) ამ შემთხვევაშიც შესაძლებელია ორი ენერგეტი-კული დონის გამოყოფა, რომელთაგან ერთი დონე მაინც ელექტრონულ-რხევითი უნდა იყოს. U-ტიპის ურთიერთქმედების განსახორციელებლად უნდა გამოვიყენოთ (14-23) ჰამილტონიანი:

$$\widehat{U}(t) = i\hbar\ {}_0\frac{\eta}{\sqrt{N}}\sum_{p=1}^{N} s_m^{(p)}\left(\hat{a}_p e^{-i\omega_{\mathrm{R}p}t} - \hat{a}_p^{+} e^{i\omega_{\mathrm{R}p}t}\right)|0\rangle\langle 1|e^{i(t\Delta-\phi_U)} + h.a.. \qquad (2.14-34)$$

U-ტიპის ურთიერთქმედებისათვის ქუბიტის დინამიკის განტოლებას და ტალღურ ფუნქციას შემდეგი სახე ექნებათ:

$$\frac{\partial}{\partial t}|\varphi_I(t)\rangle = -\frac{i}{\hbar}\widehat{U}(t)|\varphi_I(t)\rangle\,, \qquad (2.14-35)$$

$$|\varphi_I(t)\rangle = a_0(t)|0\rangle|vac\rangle + a_1(t)|1\rangle|vac\rangle + \sum_{p=1}^{N} a_{0p}(t)|0\rangle|1p\rangle + \sum_{p=1}^{N} a_{1p}(t)|1\rangle|1p\rangle\,. \qquad (2.14-36)$$

(14-36) სახით მოცემული ტალღური ფუნქცია შეესაბამება ორი ელექტრონული და მრავალი ელექტრონულ-რხევითი დონის მქონე კვანტურ ნაწილაკს. მდგომარეობა მნიშვნელოვნად გამარტივდება თუ განვიხილავთ იონების მძივის მხოლოდ მასათა ცენტრის (CM) მოდას. ამ შემთხვევაში პარაგრაფ 12-ში მიღებული შედეგების თანახმად (გამოსახუ-ლება (12-23)) $s_m^{(1)} = 1, \omega_{\mathrm{R}1} = \omega_{\mathrm{R}}$ შესაბამისად გვაქვს:

$$\widehat{U}(t) = i\hbar\Omega_0\frac{\eta}{\sqrt{N}}\left(\hat{a}_p e^{-i\omega_{\mathrm{R}}t} - \hat{a}_p^{+} e^{i\omega_{\mathrm{R}}t}\right)|0\rangle\langle 1|e^{i(t\Delta-\phi_U)} + \mathrm{h.a.}, \qquad (2.14-37)$$

ხოლო (14-36) ტალღური ფუნქცია კი, ზემოთქმულის გათვალისწინებით, შემდეგ სახეს მიიღებს:

$$|\varphi_I(t)\rangle = a_0(t)|0\rangle|vac\rangle + a_1(t)|1\rangle|vac\rangle + a_{0p}(t)|0\rangle|1p\rangle + a_{1p}(t)|1\rangle|1p\rangle. \quad (2.14-38)$$

თუ ლაზერის სიხშირეს ისე შევარჩევთ, რომ $\Delta = -\omega_{\mathrm{R}}$, მაშინ (14-37) შეგვიძლია დავაგვწეროთ

$$\widehat{U}(t) = i\hbar\Omega_0 \frac{\eta}{\sqrt{N}} \left(\hat{a}_p e^{-i2\omega_{\mathrm{R}}t} - \hat{a}_p^+\right)|0\rangle\langle 1|e^{-i\phi_U} + \text{h. a.} \qquad (2.14-39)$$

სახით. თუ უგულვებელვყოფთ ორფონონური მდგომარეობების აღგზნების შესაძლებლობას ($2\omega_{\mathrm{R}}$-ის შემცველ წევრებს), მაშინ (14-39) გამოსახულება მნიშვნელოვნად გამარტივდება და საბოლოოდ მივიღებთ:

$$\widehat{U}(t) = -i\hbar\Omega_0 \frac{\eta}{\sqrt{N}} \hat{a}_p^+|0\rangle\langle 1|e^{-i\phi_U} + i\hbar\Omega_0 \frac{\eta}{\sqrt{N}} \hat{a}_p|1\rangle\langle 0|e^{i\phi_U},$$

ან კიდევ უფრო კომპაქტურად

$$\widehat{U}(t) = -i\hbar\Omega_1 \hat{a}_p^+|0\rangle\langle 1|e^{-i\phi_U} + i\hbar\Omega_0 \frac{\eta}{\sqrt{N}} \hat{a}_p|1\rangle\langle 0|e^{i\phi_U}, \quad \Omega_1 \equiv \frac{\eta}{\sqrt{N}}, \qquad (2.14-40)$$

ხოლო შესაბამის ტალღურ ფუნქციას კი შემდეგი სახე ექნება:

$$|\varphi_I(t)\rangle = a_{0p}(t)|0\rangle|1p\rangle + a_1(t)|1\rangle|vac\rangle. \qquad (2.14-41)$$

(14-40) ჰამილტონიანი და (14-41) ტალღური ფუნქცია ჩავსვათ (14-35) მოძრაობის განტოლებაში. ამის შემდეგ მიღებული განტოლება მარცხნიდან თანმიმდევრობით გავამრავლოთ $\langle 1p|\langle 0|$ და $\langle vac|\langle 1|$-ზე, ამასთან გავითვალისწინოთ ტალღური ფუნქციების ორთონორმირების პირობა და ბოზონური ოპერატორების შემდეგი თვისებები: $\hat{a}_p^+|vac\rangle = |1p\rangle$, $\hat{a}_p|1p\rangle = |vac\rangle$. ამ ოპერაციების ჩატარების შემდეგ $a_{0p}(t)$ და $a_1(t)$ კოეფიციენტებისათვის შემდეგი განტოლებათა სისტემა გვექნება:

$$\frac{d}{dt}a_{0p}(t) = -\Omega_0 \frac{\eta}{\sqrt{N}} a_1(t)e^{-i\phi_U},$$

$$\frac{d}{dt}a_1(t) = \Omega_0 \frac{\eta}{\sqrt{N}} a_{0p}(t)e^{i\phi_U}. \qquad (2.14-42)$$

საიდანაც,

$$\frac{d^2}{dt^2}a_{0p}(t) + \frac{\eta^2}{N}\Omega_0^2 a_{0p}(t) = 0\,. \qquad (2.14-43)$$

მე-14 პარაგრაფის მე-2 პუნქტში ჩატარებული პროცედურის ანალოგიურად ვპოულობთ (14-41) სუპერპოზიციის კოეფიციენტებს:

$$a_{0p}(t) = a_{0p}(0)\cos\Omega_1 t - a_1(0)\, e^{-i\phi_U}\sin\Omega_1 t\,, \qquad (2.14-44)$$

$$a_1(t) = a_1(0)\cos\Omega_1 t + a_{0p}(0) e^{i\phi_U}\sin\Omega_1 t\,, \qquad (2.14-45)$$

ან მატრიცული ფორმით:

$$\begin{pmatrix} a_{0p}(t) \\ a_1(t) \end{pmatrix} = \begin{pmatrix} \cos\Omega_1 t & e^{-i\phi_U}\sin\Omega_1 t \\ i\, e^{i(\frac{\pi}{2}-\phi_U)}\sin\Omega_1 t & \cos\Omega_1 t \end{pmatrix} \begin{pmatrix} a_{0p}(t) \\ a_1(0) \end{pmatrix}\,. \qquad (2.14-46)$$

ამრიგად, გამოსახულებას, რომელიც რეზონანსულ ლაზერულ ველში აღწერს m-ური ქუბიტის კვანტურ დინამიკას კოლექტიური ფონონური მოდის აღგზნებით, აქვს შემდეგი სახე:

$$\widehat{U}_m(\Xi,\phi_U):\ \begin{matrix} |0\rangle|1p\rangle_m \ \to \cos\Xi\,|0\rangle|1p\rangle_m - ie^{i\phi'_U}\sin\Xi\,|1\rangle|vac\rangle_m\,, \\ |1\rangle|vac\rangle_m \to \cos\Xi\,|1\rangle|vac\rangle_m - ie^{-i\phi'_U}\sin\Xi\,|0\rangle|1p\rangle_m, \end{matrix} \qquad (2.14-47)$$

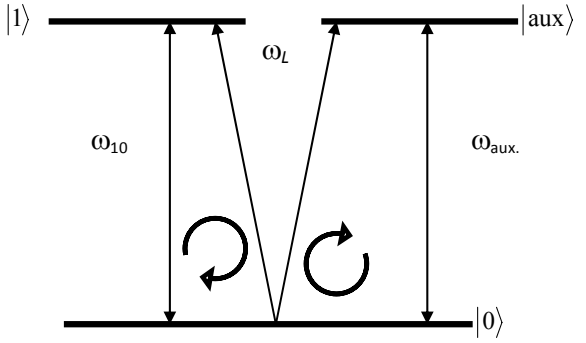
სადაც,

$$\Xi \equiv \Omega_0 t\,,\ \ \phi'_U = \frac{\pi}{2} - \phi_U. \qquad (2.14-48)$$

14.4. ურთიერთქმედება დამხმარე დონის საშუალებით

ზოგიერთი ლოგიკური ოპერაციების შესასრულებლად აუცილებელი ხდება ქუბიტის საკუთარი მდგომარეობების მხოლოდ ერთი ბაზისური ვექტორის შეცვლა ისე, რომ მეორე უცვლელი დარჩეს. როგორც წესი დამხმარე დონეს (auxiliary level) წარმოადგენს იონის სპექტრში ზენაზი სტრუქტურის ერთ-ერთი ენერგეტიკული დონე [2.17]. ასეთი დონის აღგზნება შეიძლება განხორციელდეს ლაზერის იმპულსის პოლარიზაციის შეცვლით (ნახ.14.1). შესაბამის V და U ტიპის ოპერატორებს კი შემდეგი სახე ექნებათ:

$$\widehat{V}_m^{(\mathrm{aux})}(\Theta,\phi_V):\ \begin{matrix} |0\rangle_m \to \cos\Theta\,|0\rangle_m - i\sin\Theta\, e^{i\phi_V}|aux\rangle_m \\ |aux\rangle_m \to \cos\Theta\,|aux\rangle_m - i\sin\Theta\, e^{-i\phi_V}|0\rangle_m \end{matrix}\,, \qquad (2.14-49)$$



ნახ. 14.1

დამხმარე დონის (auxiliary level) აღგზნების სქემა ლაზერის გამოსხივების პოლარიზაციის შეცვლით.

$$\widehat{U}_m^{(\mathrm{aux})}(\Xi,\phi_U):\begin{matrix}|0\rangle|1p\rangle_m \to \cos\Xi\,|0\rangle|1p\rangle_m - i\sin\Xi\,e^{i\phi'_U}|aux\rangle|vac\rangle_m \\ |aux\rangle|vac\rangle_m \to \cos\Xi\,|aux\rangle|vac\rangle_m - i\sin\Xi\,e^{-i\phi'_U}|0\rangle|1p\rangle_m\end{matrix}. \quad (2.14-50)$$

ამრიგად, (14-32), (14-47), (14-49) და (14-50) ოპერატორები ასრულებენ ყველა იმ ოპერაციას რომელსაც კვანტური გამოთვლები ემყარება. თავად კონკრეტული ოპერაციები განხილულია მომდევნო პარაგრაფში.

15. ლოგიკური ოპერაციები m-ური ქუბიტისათვის V და U ტიპის ურთიერთქმედებებით განპირობებული ლოგიკური ოპერაციები

კვანტური გამოთვლების ჩასატარებლად აუცილებელია კვანტურ სისტემაში განვახორციელოთ ის საბაზისო ოპერაციები, რომლებიც შესაძლებლობას მოგვცემს ამ ბაზისისაგან ავაგოთ შესაბამისი "ლოგიკა". განსაზღვრის თანახმად (იხილე პარაგრაფი 14) U და V ტიპის ოპერაციები ფაზაში $\pi/2$-ით არიან წანაცვლებულნი, ანუ

$$\phi_V - \phi'_U = \pi/2.$$

კოჰერენტულობის მოსაზრებიდან ეს თანაფარდობა მთელი გამოთვლითი პროცესის განმავლობაში უნდა შევინარჩუნოთ, ხოლო აბსოლუტური

ფაზა არჩევა პირობითია. აქედან გამომდინარე U ტიპის ოპერატორის აბსოლუტური ფაზა ნულის ტოლად ჩავთვალოთ $(\phi'_U = 0)$, მაშინ $\phi_V = \pi/2$ და შესაბამისი ოპერაციებისათვის (14-32), (14-47), (14.19) და (14-50) გამოსახულებებიდან მივიღებთ

$$\widehat{V}_m(\Theta, \pi/2): \begin{matrix} |0\rangle_m \to \cos\Theta\,|0\rangle_m + \ \sin\Theta\ |1\rangle_m \\ |1\rangle_m \ \to \cos\Theta\,|1\rangle_m - \ \sin\Theta\,|0\rangle_m \end{matrix}, \qquad (2.15-01)$$

$$\widehat{U}_m(\Xi, 0): \begin{matrix} |0\rangle|1p\rangle_m \ \to \cos\Xi\,|0\rangle|1p\rangle_m - i\ \sin\Xi\,|1\rangle|vac\rangle_m \\ |1\rangle|vac\rangle_m \to \cos\Xi\,|1\rangle|vac\rangle_m - i\sin\Xi\,|0\rangle|1p\rangle_m \end{matrix}, \qquad (2.15-02)$$

$$\widehat{V}_m^{(\mathrm{aux})}(\Theta, \pi/2): \begin{matrix} |0\rangle_m \to \cos\Theta\,|0\rangle_m + \sin\Theta\,|aux\rangle_m \\ |aux\rangle_m \to \cos\Theta\,|aux\rangle_m - \sin\Theta\,|0\rangle_m \end{matrix}, \qquad (2.15-03)$$

$$\widehat{U}_m^{(\mathrm{aux})}(\Xi, 0): \begin{matrix} |0\rangle|1p\rangle_m \to \cos\Xi\,|0\rangle|1p\rangle_m - i\sin\Xi\,|aux\rangle|vac\rangle_m \\ |aux\rangle|vac\rangle_m \to \cos\Xi\,|aux\rangle|vac\rangle_m - i\sin\Xi\,|0\rangle|1p\rangle_m \end{matrix}. \qquad (2.15-04)$$

ინფორმაციის ჩაწერისთვის, ბუნებრივია უნდა განვახორციელოთ დამოუკიდებელი ოპერაციები თითოეულ ქუბიტზე, ისე რომ არ შევაშფოთოთ იონების მძივის დანარჩენი ქუბიტები. გამოთვლის პროცესში კი პირიქით, აუცილებელია ქუბიტებს შორის ინფორმაციის გაცვლა. განვიხილოთ ეს უკანასკნელი ორი, მაკონტროლებელი, c–ური, და სამიზნე, t–ური, იონების (ქუბიტების) მაგალითზე. c–ურ ქუბიტზე ვიმოქმედოთ U ტიპის, ხოლო t–ურ ქუბიტზე კი U და V ტიპის ოპერატორებით. თავდაპირველად სამიზნე ქუბიტზე V ტიპის ურთიერთქმედება განვახორციელოთ. ამ შემთხვევაში საქმე გვექნება ოთხ საბაზისო მდგომარეობასთან: $|0\rangle_c|0\rangle_t|vac\rangle$, $|0\rangle_c|1\rangle_t|vac\rangle$, $|1\rangle_c|0\rangle_t|vac\rangle$ და $|1\rangle_c|1\rangle_t|vac\rangle$. ამისათვის ლაზერის $\Theta = \pi/4$ იმპულსით ვიმოქმედოთ (იხ. (15-01)), რის შედეგადაც საბაზისო მდგომარეობები ასე შეიცვლება

$$\widehat{V}_t(\pi/4, \pi/2): \begin{matrix} |0\rangle_c|0\rangle_t|vac\rangle \Rightarrow 1/\sqrt{2}\ |0\rangle_c(|0\rangle_t + |1\rangle_t)|vac\rangle \\ |0\rangle_c|1\rangle_t|vac\rangle \Rightarrow 1/\sqrt{2}\,|0\rangle_c(|1\rangle_t - |0\rangle_t)|vac\rangle \\ |1\rangle_c|0\rangle_t|vac\rangle \Rightarrow 1/\sqrt{2}\ |1\rangle_c(|0\rangle_t + |1\rangle_t)|vac\rangle \\ |1\rangle_c|1\rangle_t|vac\rangle \Rightarrow 1/\sqrt{2}\,|1\rangle_c(|1\rangle_t - |0\rangle_t)|vac\rangle \end{matrix}. \qquad (2.15-05)$$

ამის შემდეგ და c-ქუბიტზე U ტიპის $\Xi = \pi/2$ იმპულსით ვიმოქმედოთ (იხ. (15-02)), რის შედეგადაც საბაზისო მდგომარეობები (15-05)-ის გათვალისწინებით უკვე ასეთ სახეს მიიღებენ:

$$\widehat{U}_c(\pi/2\,,0)\colon \begin{matrix} 1/\sqrt{2}\;|0\rangle_c(|0\rangle_t+|1\rangle_t)|vac\rangle \Rightarrow\; 1/\sqrt{2}\,|0\rangle_c(|0\rangle_t+|1\rangle_t)|vac\rangle \\ 1/\sqrt{2}\,|0\rangle_c(|1\rangle_t-|0\rangle_t)|vac\rangle \Rightarrow\; 1/\sqrt{2}\,|0\rangle_c(|1\rangle_t-|0\rangle_t)|vac\rangle \\ 1/\sqrt{2}\;|1\rangle_c(|0\rangle_t+|1\rangle_t)|vac\rangle \Rightarrow -1/\sqrt{2}\,|0\rangle_c(|0\rangle_t+|1\rangle_t)|1p\rangle \\ 1/\sqrt{2}\,|1\rangle_c(|1\rangle_t-|0\rangle_t)|vac\rangle \Rightarrow\; -1/\sqrt{2}\,|0\rangle_c(|1\rangle_t-|0\rangle_t)|1p\rangle \end{matrix}. \qquad (2.15-06)$$

ამ ოპერაციების შემდეგ t-ქუბიტზე U ტიპის π-იმპულსის ზემოქმედებით და დამხმარე დონის საშუალებით განვახორციელოთ ნიშნის შეცვლის ოპერაცია (იხ. (15-04))

$$\widehat{U}_t^{(\mathrm{aux})}(\pi,0)\colon \begin{matrix} 1/\sqrt{2}\,|0\rangle_c(|0\rangle_t+|1\rangle_t)|vac\rangle \;\Rightarrow\; 1/\sqrt{2}\,|0\rangle_c(-|0\rangle_t+|1\rangle_t)|vac\rangle \\ 1/\sqrt{2}\,|0\rangle_c(|1\rangle_t-|0\rangle_t)|vac\rangle \Rightarrow\; 1/\sqrt{2}\,|0\rangle_c(|1\rangle_t+|0\rangle_t)|vac\rangle \\ -1/\sqrt{2}\,|0\rangle_c(|0\rangle_t+|1\rangle_t)|1p\rangle \;\Rightarrow\; -1/\sqrt{2}\,|0\rangle_c(-|0\rangle_t+|1\rangle_t)|1p\rangle \\ -1/\sqrt{2}\,|0\rangle_c(|1\rangle_t-|0\rangle_t)|1p\rangle \Rightarrow\; -1/\sqrt{2}\,|0\rangle_c(|1\rangle_t+|0\rangle_t)|1p\rangle \end{matrix}. \qquad (2.15-07)$$

კვლავ ვიმოქმედოთ c-ქუბიტზე U ტიპის $\pi/2$-იმპულსით:

$$\widehat{U}_c(\pi/2\,,0)\colon \begin{matrix} 1/\sqrt{2}\,|0\rangle_c(-|0\rangle_t+|1\rangle_t)|vac\rangle \;\Rightarrow\; i/\sqrt{2}\,|0\rangle_c(|0\rangle_t-|1\rangle_t)|vac\rangle \\ 1/\sqrt{2}\,|0\rangle_c(|1\rangle_t+|0\rangle_t)|vac\rangle \Rightarrow\; -i/\sqrt{2}\,|0\rangle_c(|1\rangle_t+|0\rangle_t)|vac\rangle \\ -1/\sqrt{2}\,|0\rangle_c(-|0\rangle_t+|1\rangle_t)|1p\rangle \;\Rightarrow\; -i/\sqrt{2}\,|1\rangle_c(|0\rangle_t-|1\rangle_t)|vac\rangle \\ -1/\sqrt{2}\,|0\rangle_c(|1\rangle_t+|0\rangle_t)|1p\rangle \Rightarrow i/\sqrt{2}\,|1\rangle_c(|1\rangle_t+|0\rangle_t)|vac\rangle \end{matrix}. \qquad (2.15-08)$$

და ბოლოს ისევ t-ქუბიტზე V ტიპის $\pi/4$-იმპულსით ვიმოქმედოთ:

$$\widehat{V}_t(\pi/4\,,\pi/2)\colon \begin{matrix} i/\sqrt{2}\,|0\rangle_c(|0\rangle_t-|1\rangle_t)|vac\rangle \Rightarrow i|0\rangle_c|0\rangle_t|vac\rangle \\ -i/\sqrt{2}\,|0\rangle_c(|1\rangle_t+|0\rangle_t)|vac\rangle \Rightarrow -i|0\rangle_c|1\rangle_t|vac\rangle \\ -i/\sqrt{2}\,|1\rangle_c(|0\rangle_t-|1\rangle_t)|vac\rangle \Rightarrow -i|1\rangle_c|0\rangle_t|vac\rangle \\ i/\sqrt{2}\,|1\rangle_c(|1\rangle_t+|0\rangle_t)|vac\rangle \;\Rightarrow i|1\rangle_c|1\rangle_t|vac\rangle \end{matrix}. \qquad (2.15-09)$$

ამრიგად, თუ ჩატარებულ ოპერაციებს გავაერთიანებთ, მივიღებთ $C\,NOT$ ოპერატორს. განხილულ შემთხვევაში:

$$C\,NOT_{ct} = \widehat{V}_t(\pi/4\,,\pi/2)\;\widehat{U}_c(\pi/2\,,0)\;\widehat{U}_t^{(\mathrm{aux})}(\pi,0)\widehat{U}_c(\pi/2\,,0)\;\widehat{V}_t(\pi/4\,,\pi/2)\,. \qquad (2.15-10)$$

ხოლო ოპერაციის შედეგს კი შემდეგი სახე ექნება:

$$C\ NOT_{ct}: \begin{matrix} |0\rangle_c|0\rangle_t|vac\rangle \Rightarrow i|0\rangle_c|0\rangle_t|vac\rangle \\ |0\rangle_c|1\rangle_t|vac\rangle \Rightarrow -i|0\rangle_c|1\rangle_t|vac\rangle \\ |1\rangle_c|0\rangle_t|vac\rangle \Rightarrow -i|1\rangle_c|1\rangle_t|vac\rangle \\ |1\rangle_c|1\rangle_t|vac\rangle \Rightarrow i|1\rangle_c|0\rangle_t|vac\rangle \end{matrix}. \qquad (2.15-11)$$

ამრიგად, $C\ NOT_{ct}$ ოპერაციის რეალიზაცია იმაზე მიუთითებს, რომ ერთი ქუბიტის გარდაქმნის ოპერაციებთან ერთად ის წარმოქმნის კვანტური ლოგიკური ოპერაციების უნივერსალურ ბაზისს.

რიჩარდ ფეინმანი (1918-1988) ლეგენდარული ამერიკელი ფიზიკოსი, ნობელის პრემიის ლაურეატი (1965). კვანტური ელექტროდინამიკის ფუძემდებელი. ყველასათვის ცნობილი "ფეინმანის ლექციები ფიზიკაში" მრავალტომეულის გარდა ფეინმანს ეკუთვნის წიგნი "ფეინმანის ლექციები გამოთვლების თეორიაში", რომელიც მისი გარდაცვალების შემდეგ, 1996 წელს გამოიცა ენტონი ჰეისა და რობინ ალენის რედაქტორობით. ჩვენთვის მოყვანილი სტატია ამ წიგნის შენ ლექციაა. მისი ორიგინალი "*Quantum Mechanical Computers" 1982* წელს დაიბეჭდა ჟურნალში *Intr.journ. Theoretical Phys.Vol.21,N.6 /7.*

რ.ფეინმანი

კვანტურ-მექანიკური კომპიუტერები

ნაშრომში გაანალიზებულია კომპიუტერების ფუნქციონირებაზე კვანტური მექანიკის პრინციპებიდან გამომდინარე ფიზიკური შეზღუდვები.

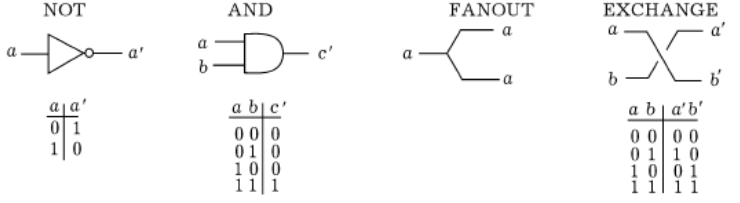
შესავალი

ეს ნაშრომი არის იმ შეზღუდვების გაანალიზების მცდელობა, რომლებიც ედება კომპიუტერებს ფიზიკის თვალსაზრისით. მაგალითად, ბენეტმა [1] ჩაატარა ძირეული გამოკვლევები თავისუფალი ენერგიის დისიპაციისა, რომელიც თან უნდა ახლდეს გამოთვლას და იპოვა, რომ ვირტუალურად იგი ნულის ტოლია. მან ჩემს წინაშე დასვა საკითხი იმ შეზღუდვების გამოკვლევის შესახებ, რომლებიც გამომდინარეობს კვანტური მექანიკიდან და განუზღვრელობის პრინციპიდან. ჩვენ დავადგინეთ, რომ გარდა თვალნათლივ არსებული შეზღუდვისა ზომაზე, თუ კომპიუტერის მუშა ნაწილები აგებულია ატომებით, ასევე არ არსებობს არავითარი ფუნდამენტური შეზღუდვები ამ თვალსაზრისით. აქ ჩვენ განვიხილავთ იდეალურ მანქანებს; მცირე არასრულყოფილობის ეფექტები განხილული იქნება მოგვიანებით. ეს კვლევა ატარებს პრინციპულ ხასიათს; ჩვენი მიზანია სისტემისათვის ვიპოვოთ ისეთი ჰამილტონიანი, რომელსაც შეეძლება გამომთვლელის როლი შეასრულოს. ჩვენ არ ვზრუნავთ

იმაზე, რომ მოცემული სისტემა იყოს ეფექტური, ან იმაზე, თუ როგორ განვახორციელოთ იგი საუკეთესო სახით.

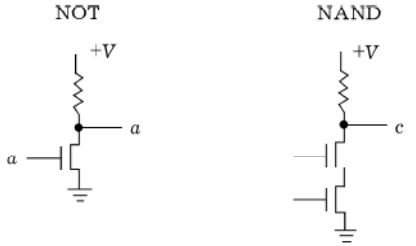
რამდენადაც კვანტური მექანიკის კანონები შექცევადია დროში, ჩვენ უნდა განვიხილოთ გამომთვლელი მანქანები, რომლებიც ემორჩილებიან ასეთ შექცევად კანონებს. აღნიშნული პრობლემა უკვე წარმოექმნა ბენეტს [1], ასევე ფრედკინს და ტოფოლის [2] და ამ თემაზე მრავალი მოსაზრება გამოითქვა. რამდენადაც შესაძლოა ეს ყველამ არ იცოდეს, ჩვენ მოგაწვდით გაკეთებულის შესაბამის მიმოხილვას და ამასთან ვისარგებლებთ შესაძლებლობით, მოვიყვანოთ ძალიან მოკლედ ბენეტის დასკვნები. ჩვენ მათ სრულად დავასაბუთებთ, როდესაც გავაანალიზებთ ჩვენს კვანტურ სისტემას.

როგორც ცნობილია, უნივერსალური კომპიუტერი შესაძლოა რეალიზებული იქნას როგორც ურთიერთდაკავშირებული ელემენტარული გეიტების შესაბამისი რთული ქსელი. თუ მივყვებით ჩვეულებრივ კლასიკურ ანალიზს, ჩვენ შეგვიძლია წარმოვიდგინოთ, რომ ურთიერთკავშირები ხორციელდება იდეალური გამტარებით, რომლებიც გადასცემენ ორიდან ერთ სტანდარტულ ძაბვას - ლოკალურად *0*-ს და *1*-ს. ჩვენ შეგვიძლია ავიღოთ მხოლოდ ორი ელემენტარული გეიტი – *NOT* და *AND* (სინამდვილეში საკმარისია მხოლოდ ერთი ელემენტი – *NAND = NOT AND,* რამდენადაც თუ ერთი შესასვლელი დაყენებულია *1*–ზე, გამოსასვლელს წარმოადგენს *NOT* მეორე შესასვლელიდან). ელემენტარული გეიტები სიმბოლურად გამოსახულია ნახ.1-ზე, სადაც ასევე მოყვანილია გამოსასვლელზე ლოგიკური მნიშვნელობები.



ნახ. 1. *ელემენტარული გეიტები*

გამტარები დეტალურად უნდა განვიხილოთ ლოგიკის თვალსაზრისით, რადგან სხვა სისტემებში და განსაკუთრებით ჩვენს კვანტურ სისტემებში შეიძლება არ გვქონდეს ასეთი გამტარები. აღვნიშნოთ, რომ სინამდვილეში გვაქვს კიდევ ორი ელემენტარული გეიტი – *FANAUT*, როდესაც ორი გამტარი ერთმანეთთან მიერთებულია და *EXCHANGE,* როდესაც გამტარები იკვეთება. ჩვეულებრივ კომპიუტერში *NOT* და *AND* გეიტები ხორციელდება ტრანზისტორებით, მაგალითად ისე, როგორც ნაჩვენებია ნახ.2–ზე.



ნახ. 2. *ტრანზისტორული წრედი NOT და AND –ისათვის*

როგორია მინიმალური თავისუფალი ენერგია, რომელიც უნდა დაიხარჯოს ასეთი ელემენტარული გეიტებით აგებული იდეალური კომპიუტერის ფუნქციონირებაზე? მაგალითად, როცა მოქმედებს *AND,* გამოსავალი ხაზი *c′* ღებულობს ორი მნიშვნელობიდან ერთ-ერთს და არა აქვს მნიშვნელობა რა იყო მანამდე, ენტროპია იცვლება ln2 ერთეულით. ეს ნიშნავს, რომ *T*– ტემპერატურაზე გამოიყოფა $KT\ln 2$ ერთეული სითბოს რაოდენობა. მრავალი წლის განმავლობაში ეს მნიშვნელობა ითვლებოდა სითბოს რაოდენობის აბსოლუტურ მინიმუმად, რომელიც უნდა გამოიყოს გამოთვლების პროცესის პირველ საფეხურზე.

ამჟამად, ეს საკითხი უფრო აკადემიურია. რეალურ მანქანებში საკმაოდ გვაწუხებს სითბოს დისიპაციის პრობლემა, რადგან გამოყენებული ტრანზისტორული სისტემა სინამდვილეში ახდენს დაახლოებით $10^{10}KT$ სითბოს რაოდენობის დისიპაციას! როგორც ბენეტმა აჩვენა, ეს ხდება იმის გამო, რომ გამტარში ძაბვის შესაცვლელად დასაწყისში მას ვამიწებთ წინაღობის გავლით, ხოლო შემდეგ, ისევ წინაღობის გავლით ვმუხტავთ მას. ენერგიის დანაკარგები შეგვეძლო მნიშვნელოვნად შეგვემცირებინა, თუ ენერგიას შევინახავდით ინდუქტიურ, ან რომელიმე სხვა რეაქტიულ ელემენტზე. თუმცა, ნათელია, რომ არსებული ტექნოლოგიებით ძნელი გასაკეთებელია ინდუქტიური ელემენტები სილიკონურ ფენებზე. ბუნებაც კი თავისი *დნმ*-კოპირების მანქანით ახდენს დაახლოებით $100KT$ სითბოს დისიპაციას ყოველ კოპირებულ ბიტზე. იმის გათვალისწინებით, რომ ამჟამად ასე შორს ვართ ამ $KT\ln 2$ რიცხვისგან, ჭკვიანური არ იქნება ვამტკიცოთ, რომ ეს მნიშვნელობაც კი ძალიან დიდია და არსებულ მინიმუმს სინამდვილეში წარმოადგენს ნული. მაგრამ, შემდგომში გამიზნული გვაქვს ვიყოთ უფრო თამამები და განვიხილოთ ამჟამად გამოყენებული 10^{11} ატომის ნაცვლად ერთ ატომზე ჩაწერილი ბიტები. ასეთი სითამამე მეტად სახალისოა ჩემნაირი მეცნიერისათვის. იმედი მაქვს, რომ თქვენც ჩათვლით მას საინტერესოდ და სახალისოდ.

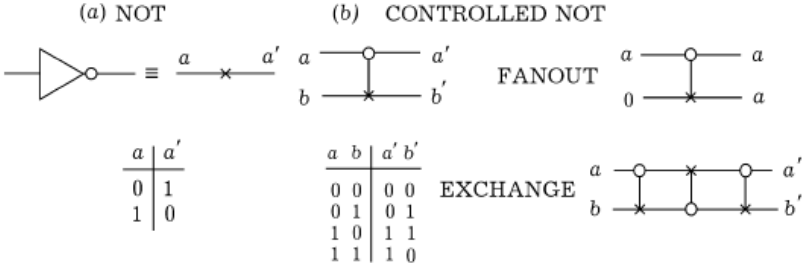
ბენეტმა აჩვენა, რომ უწინდელი ზღვარი იყო არასწორი იმიტომ, რომ შეუქცევადი ელემენტარული გეიტების გამოყენების აუცილებლობა არ იყო.

გამოთვლები შეიძლება ჩატარდეს შექცევადი გამომთვლელი მანქანებით, რომლებიც შეიცავენ შექცევად ელემენტარულ გეიტებს. ამ შემთხვევაში საჭირო თავისუფალი ენერგიის მინიმუმი არ არის დამოკიდებული გამოთვლებში ლოგიკური ბიჯების სირთულეებსა და რაოდენობაზე. იგი შეადგენს kT –ს პასუხის ბიტზე გამოსავალში. მაგრამ, ისიც კი, რაც აუცილებელია კომპიუტერის გასაწმენდად შემდგომი მოხმარებისათვის, შეიძლებოდა გაგვეხილა თავისუფალ ენერგიად, და ნაწილად იმისა, რის გაკეთებასაც ვუპირებთ პასუხს, ანუ ინფორმაციას, თუ მას გადავცემთ სხვა წერტილს. ესაა - ზღვარი, მიღწევადი მხოლოდ იდეალურ შემთხვევაში, თუ გამოთვლას ვაწარმოებთ უსასრულოდ მცირე სიჩქარის შექცევად კომპიუტერზე.

გამოთვლა შექცევად მანქანაზე

ახლა ჩვენ აღვწერთ სამ შექცევად ელემენტარულ გეიტს, რომლებიც შეიძლება გამოყენებულნი იქნან უნივერსალური მანქანის შესაქმნელად [4]. პირველი მათგანია *NOT,* რომელიც ცხადია, არ კარგავს ინფორმაციებს და ითვლება შექცევადად. შექცევა ხორციელდება *NOT*-ის განმეორებითი ქმედებით. რამდენადაც ეს სიმბოლო არასიმეტრიულია, მის მაგივრად სქემაში, გამტარზე, გამოვიყენებთ X სიმბოლოს (იხ. ნახ.3ა).

შემდეგი ელემენტია *CONTROLLED NOT* (კონტროლირებადი არა) (იხ. ნახ. 3b). აქ გვაქვს ორი შემავალი ხაზი a და b და ორი გამომავალი – a' და b'. ხაზი a' ყოველთვის იგივეა, რაც a, რომელიც ასრულებს საკონტროლო ხაზის მოვალეობას. თუ საკონტროლო ხაზი აქტივირებულია



ნახ. 3. შექცევადი ელემენტარული გეიტები

(a=1), მაშინ გამომავალი b' არის *NOT b*. წინააღმდეგ შემთხვევაში (როგორც ხედავთ, მე არ ვარ პროფესიონალი პროგრამისტი, ის "სხვაგვარად" იტყოდა - "else") *b* არ იცვლება: $b' = b$. შესავლის და გამოსავლის მნიშვნელობათა ცხრილი მოყვანილია ნახ.3-ზე. ამ მოქმედებების შებრუნება მათი განმეორებითი შესრულებით ხდება. b' სიდიდე სინამდვილეში წარმოადგენს *a*-სა და *b*-ს სიმეტრიულ ფუნქციას, რომელსაც ეწოდება *"გამომრიცხავი ან"* და *XOR* სიმბოლოთი აღინიშნება: *a* ან *b*, მაგრამ არა ორივე ერთად. ეს ოპერაცია შეესაბამება *a*-ს და *b*-ს შეჯამებას მოდულით 2. იგი შეიძლება გამოყენებულ იქნას *a*-სა და *b*-ს შესადარებლად, შედეგი იქნება 1-ის ტოლი იმის ნიშნად, რომ ისინი განსხვავებულია. გთხოვთ ყურადღება მიაქციოთ იმას, რომ ეს ფუნქცია – *XOR,* თავისთავად არ არის შექცევადი. მაგალითად, თუ მიიღება მნიშვნელობა 0, ჩვენ ვერ ვიტყვით იგი მიღებული იქნა *(a,b)*=(0,0)-დან თუ (1,1)-დან, მაგრამ ჩვენ ვინარჩუნებთ სხვა ხაზს, $a' = a,$ არაცალსახობის ასაცილებლად.

სქემატურად *CONTROLLED NOT*-ს ჩვენ წარმოვადგენთ საკონტროლო ხაზზე o-ს განთავსებით, რომელიც დაკავშირებულია კონტროლირებადი ვერტიკალური ხაზით X-თან.

მოცემულ ელემენტს ასევე შეუძლია ჩვენი უზრუნველყოფა *FANCOUT*-ოპერაციით, რადგან თუ $b=0,$ მოხდება *a*-ს კოპირდება b' ხაზზე, ეს ფუნქცია – *COPY,* მნიშვნელოვანი იქნება მოგვიანებით, რადგანაც სამი ასეთი ელემენტი გამოყენებული მიმდევრობითი ხაზების წყვილებზე, მაგრამ საკონტროლო ხაზის მორიგეობითი შერჩევით, ახდენენ ინფორმაციის გაცვლას ხაზზე (ნახ. 3ბ).

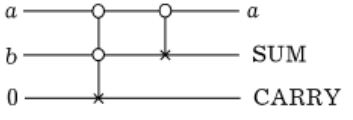
აღმოჩნდა, რომ მხოლოდ ამ ორი ელემენტის კომბინაცია არაა საკმარისი ნებისმიერი ლოგიკური ფუნქციის შესასრულებლად. აუცილებელია კიდევ რაიმე ელემენტი, რომელიც ჩართავს სამ ხაზს. ჩვენ შევარჩიეთ ერთ-ერთი ასეთი, რომელსაც ვუწოდებთ *"კონტროლირებად კონტროლირებად არა"*-ს და აღვიშნავთ *CONTROLLED CONTROLLED NOT*-თი. აქ (იხ. ნახ. 3c) გვაქვს ორი საკონტროლო ხაზი *a* და *b,* რომლებიც უცვლელად რჩებიან გამოსასვლელზე და ცვლიან მესამე *c* ხაზს *NOT c*-თი, მხოლოდ იმ შემთხვევაში თუ ორივე ხაზი აქტივირებულია *(a=1* და *b=1).* წინააღმდეგ შემთხვევაში $c' = c$. თუ მესამე ხაზის შესასვლელზე დაყენებულია *O*, ცხადია $c' = 1,$ მხოლოდ მაშინ, თუ *a=1* და *b=1.* ამით მივიღებთ *AND* ფუნქციას (იხ. ცხრილი 1).

ცხრილი 1

a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

(a, b)-ს სამ შესაძლო კომბინაციას, კერძოდ, *(0,0), (0,1)* და *(1,0)* მივყავართ *AND (a,b)* ფუნქციის ერთსა და იმავე *0* მნიშვნელობამდე, ამიტომ არაცალსახობის ასაცილებლად საჭიროა ორი ბიტი. ისინი ინახება *a,b* ხაზების გამოსავალზე, რის გამოც ამ ფუნქციის შებრუნება შესაძლებელია მისივე განმეორებითი ქმედებით. ფუნქცია *AND* წარმოადგენს *a* და *b* ბიტის ჯამის გადამტანს.

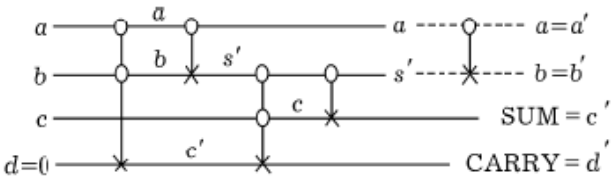
ცნობილია, რომ ამ ელემენტების კომბინაციით შესაძლებელია შეიქმნას ნებისმიერი ლოგიკური სქემა და მტკიცდება, რომ შეიძლება გაკეთდეს უნივერსალური კომპიუტერი. ვაჩვენოთ ეს მაგალითზე. ჯერ ერთი, როგორც ნახ.4-ზე ვხედავთ



ნახ. 4. *მაჯამებელი*

შეგვიძლია გავაკეთოთ მაჯამებელი, გამოვიყენებთ რა მიმდევრობით ჯერ *CONTROLLED CONTROLLED NOT*-ს და შემდეგ *CONTROLLED NOT*-ს. მაშინ *a,b* და 0-დან შემავალ ხაზებზე მიიღება თავდაპირველი *a* ერთ ხაზზე, ჯამი - მეორეზე და გადატანა - მესამეზე.

ბევრად რთული სქემა - სრული მაჯამებელი (იხ. ნახ.5), რომელიც იღებს რომელიღაც წინა შეჯამებიდან *c*-ს გადასაცემად, კრებს მას ორ *a* და *b* ხაზთან და გარდა ამისა შეიცავს დამატებით *d* ხაზს 0-ით შესავალზე. ეს სქემა მოითხოვს ოთხი გეიტის ერთად შედგენას. გარდა *a,b* და *c* სამი ხაზის სრული ჯამისა და გადატანისა, ვღებულობთ კიდევ ორ შეტყობინებას ორ სხვა ხაზზე. ერთ-ერთი მათგანია *a*, რომლითაც დავიწყეთ, ხოლო მეორე რაიმე შუალედური სიდიდეა, რომელიც გამოვთვალეთ.



ნახ. 5. *სრული მაჯამებელი*

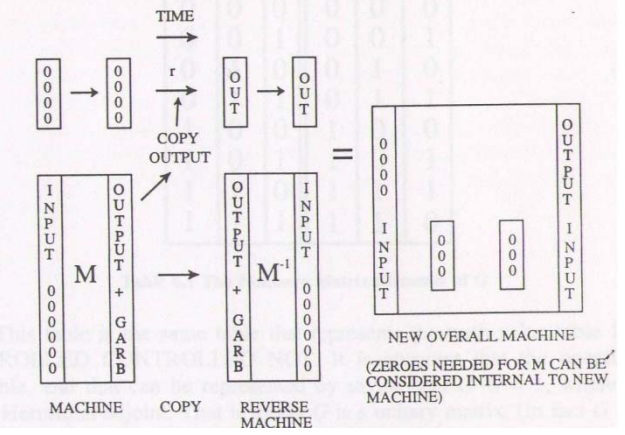
ეს ტიპიურია შექცევადი სისტემებისათვის. ისინი აწარმოებენ არა მხოლოდ იმას, რაც თქვენ გსურთ მიიღოთ გამოსავალზე, არამედ განსაზღვრული რაოდენობის ნაგავსაც. ამ კონკრეტულ შემთხვევაში და როგორც აღმოჩნდა, ყველა შემთხვევებში, ნაგავი სინამდვილეში შეიძლება მიყვანილ იქნას ზუსტად იმაზე, რაც გვქონდა შესავალზე. ამისათვის საკმარისია დავუმატოთ პირველ ორ ხაზზს *CONTROLLED NOT,* როგორც ეს ნაჩვენებია პუნქტირით ნახ.5-ზე. დავინახავთ, რომ ნაგავი გახდებოდა *a* და *b,* რაც სულ ცოტა ორი ხაზის შესავალს წარმოადგენს (ეს სქემა შეიძლება გამარტივებულიყო, მაგრამ ამას ვაკეთებთ თვალსაჩინოებისათვის).

ამგვარად, სხვადასხვა კომბინაციებით შეგვიძლია შევქმნათ საერთო ლოგიკური ბლოკი, რომელიც შექცევადი ოპერაციით გარდაქმნის *n* ბიტს *n* ბიტად. თუ ამოცანა, რომლის გადაჭრასაც ვცდილობთ თავისთავად შექცევადია, მაშინ შესაძლოა აღარ გაჩნდეს დამატებით ნაგავი, მაგრამ საზოგადოდ იგი აუცილებელია რომელიღაც დამატებითი ხაზზე ინფორმაციის შესანახად. ეს უკანასკნელი კი დაგვჭირდება იმისათვის, რომ გვქონდეს ოპერაციის შექცევის შესაძლებლობა. სხვა სიტყვებით რომ ვთქვათ, შეგვიძლია მივიღოთ ნებისმიერი ფუნქციის მნიშვნელობები, რაც შეუძლია ჩვეულებრივ სისტემას, პლუს ნაგავი. ნაგავი მოიცავს ინფორმაციას, რომელიც აუცილებელია პროცესის შექცევისათვის.

რა რაოდენობისაა ნაგავი? ზოგადად აღმოჩნდა, რომ თუ საძიებელი გამოსავალი მონაცემები შეიცავს *k* ბიტს, მაშინ, დაწყებული რომელიმე შესავალი მონაცემებითა და *k* რაოდენობის ბიტებით, რომლებიც მოიცავენ *O*-ს, შეგვიძლია მივიღოთ მხოლოდ შემავალი და გამომავალი ინფორმაცია და არავითარი ნაგავი. ეს პროცესი შექცევადია იმიტომ, რომ შემავალი და გამომავალი ინფორმაციის ცოდნა ყველა ჩატარებული ქმედებების ანულირების საშუალებას იძლევა. ასეთი პროცესი ყოველთვის შექცევადია. ამის სასარგებლოდ არგუმენტი მოყვანილია ნახ.6-ზე.

დავუშვათ ვიწყებთ ნებისმიერი *M*-მანქანით, რომელიც მუშაობას იწყებს რაიმე შესავალი ინფორმაციით და დიდი რაოდენობის ნულებით და გვაძლევს სასურველ გამოსავალს პლუს დამატებითი ინფორმაციის გარკვეულ რაოდენობას, რასაც ჩვენ ნაგავი ვუწოდეთ. შესაძლებელია კოპირების

ოპერაციის შესრულება *CONTROLLED NOT* გეიტების მიმდევრობით, ამიტომ, თუ თავდაპირველად გვაქვს თავისუფალი რეგისტრი *k* ბიტებით გამოსავალი ინფორმაციისათვის, შეგვიძლია *M*-ის პროცესორის მოქმედების შემდეგ მოვახდინოთ გამოსავალი ინფორმაციის კოპირება *M*-დან ამ ახალ რეგისტრში. ამის შემდეგ, ჩვენ შეგვიძლია ავაგოთ შექცევადი *M*-მანქანა, რომელიც პირიქით აიღებს *M*-დან გამომავალ ინფორმაციას და ნაგავთან ერთად გაუშვებს შესაბამისად შემავალ ინფორმაციაში და ნულებში. ამგვარად, ყოველივე ეს განხილული, როგორც ზოგადი მანქანა, იწყებს გამომავალი ინფორმაციის და შემავალი მონაცემების რეგისტრის *k* ნულებიდან და ბოლოში შედეგის სახით ღებულობს ამ *k* ნულებს, დაკავებულებს გამომავალი ინფორმაციით და შემავალი მონაცემების განმეორებით. ეს არის ნულების რაოდენობა, რომელიც თავდაპირველად აუცილებელია *M*-მანქანაში ნაგავის შესანახად, აღდგება ისევ ნულებად და შესაძლოა განხილულ იქნას, როგორც შიგა შეერთებები ახალი სრული მანქანის შიგნით (*M, $\bar{M}$* და კოპირება). ასე რომ, ჩვენ დავასრულეთ ის რის გაკეთებასაც ვაპირებდით და ამრიგად, ნაგავი არასოდეს იმაზე მეტი არ უნდა იყოს, ვიდრე შემავალი მონაცემების განმეორებისთვისაა საჭირო.



ნახ. 6. *ნაგვის განუფთავება*

კვანტურ მექანიკური კომპიუტერი

ახლა განვიხილოთ ასეთი კომპიუტერის აგების შესაძლებლობა კვანტური მექანიკის კანონების გამოყენებით. ჩვენ ვაპირებთ ჩავწეროთ ურთიერთქმედი ნაწილებისაგან შედგენილი სისტემის ჰამილტონიანი, რომელიც რაღაც აზრით მოიქცევა როგორც დიდი სისტემა და გამოდგება უნივერსალური კომპიუტერის პროტოტიპად. რა თქმა უნდა, დიდი სისტემა ასევე ექვემდებარება კვანტურ მექანიკას, მაგრამ იგი ურთიერთქმედებს თერმოსტატთან და სხვა საგნებთან, რამაც იგი შეიძლება გახადოს არაშექცევადი. ჩვენ გვინდა

გავაკეთოთ კომპიუტერი იმდენად პატარა და იმდენად მარტივი, რამდენადაც ეს შესაძლებელია. ჩვენი ჰამილტონიანი დეტალურად აღწერს ყოველ შინაგან გამოთვლით ქმედებებს, მაგრამ გარე სამყაროსთან ურთიერთქმედების გარეშე, რაც მოიცავს შემავალი მონაცემების შეყვანას (საწყისი მონაცემების მომზადებას) და გამომავალი ინფორმაციის წაკითხვას.

რამდენად მცირე შეიძლება იყოს ასეთი კომპიუტერი? რამდენად მცირე შეიძლება იყოს რიცხვი? როგორც ცნობილია, რიცხვი შეიძლება წარმოდგენილი იქნას ერთიანებითა და ნულებით შედგენილი ბიტებით. წარმოვიდგინოთ, რომ გვაქვს ორდონიანი სისტემები (ანუ ისეთები, რომელთაც შეუძლიათ ორიდან ერთ-ერთ დონეზე ყოფნა), რომლებსაც დავარქმევთ "ატომებს". ასეთ შემთხვევაში n ბიტიანი რიცხვი წარმოდგენილია "რეგისტრის" n რაოდენობის ორდონიანი სისტემების ერთობლიობით. ცხადია, შეგვიძლია ჩავწეროთ ნებისმიერი რიცხვი, თუ მოვათავსებთ თითოეულ ატომს ერთში ან მეორეში მისი ორი მდგომარეობიდან, რომლებსაც აღვნიშნავთ |1> და |0> სიმბოლოებით. რიცხვი შეიძლება იყოს წაკითხული ასეთი რეგისტრიდან იმის განსაზღვრით ან გაზომვით, თუ რა მდგომარეობაში იმყოფება თითოეული ატომი მოცემულ მომენტში. ამრიგად, ერთი ბიტი წარმოდგენილი იქნება ერთი ატომით, რომელიც იმყოფებოდა ორი მდგომარეობიდან ერთ-ერთში.

იმისათვის, რომ გავიგოთ რა უნდა გავაკეთოთ შემდგომ, განვიხილოთ ელემენტ *CONTROLLED CONTROLLED NOT*-ის მაგალითი. დავუშვათ G რაღაც ოპერაციაა სამ a,b და c ატომზე, რომელსაც გადაყავს a, b და c-ს საწყისი მდგომარეობა რომელიღაც a', b' და c' მდგომარეობაში ისე, რომ კავშირი a', b', c'-სა და a,b,c-ს შორის ისეთია, როგორსაც ველოდით. აქ a, b, c და a', b', c' წარმოადგენენ *CONTROLLED CONTROLLED NOT* გეიტის შესაბამისად შესავალ და გამოსავალ ხაზებს. ყურადღება მივაქციოთ იმას, რომ მოცემულ მომენტში ჩვენ არ ვცდილობთ გადავიტანოთ ინფორმაცია ერთი ადგილიდან მეორეში, ჩვენ უბრალოდ ვაპირებთ იგი შევცვალოთ. ეს განსხვავდება იმისაგან, რასაც აქვს ადგილი არსებულ კომპიუტერში, სადაც ძაბვა გადაეცემა ერთი გამტარიდან მეორეზე. ის რასაც აქ ვაკეთებთ ბევრად მარტივია და კერძოდ, თუ გვაქვს სამი ატომი რაღაც განსაზღვრულ მდგომარეობაში, ვატარებთ ოპერაციას, რომელიც ცვლის მათ მდგომარეობას ახალი a', b', c' მდგომარეობით.

ამ შემთხვევაში $|a', b', c' >$ მდგომარეობა მიიღება $|a, b, c >$ მდგომარეობაზე რაღაც G-ქმედებით. კვანტურ მექანიკაში ოპერატორები, რომლებიც ცვლიან მდგომარეობებს ითვლებიან წრფივად. ამრიგად, G არის მატრიცი, რომლის $G_{a',b',c'a,b,c}$ ელემენტები ყველა ნულის ტოლია, გარდა იმ ელემენტებისა, რომლებიც ეთანადებიან ცხრილი 1-ით მოცემულ მდგომარეობებს. ისინი კი ცხადია 1-ის ტოლია.

ეს იგივეა, რაც *CONTROLLED CONTROLLED NOT* -ის ჭეშმარიტობის ცხრილი. ცხადია, რომ ეს ოპერატორი შექცევადია, რაც შეიძლება ჩაიწეროს ფორმულით $G^*G = 1$, სადაც * ნიშნავს ერმიტულ შეუღლებას. ანუ G არის უნიტარული მატრიცი (სინამდვილეში G არის ნამდვილი მატრიცი და $G^* = G$, მაგრამ ეს მხოლოდ ამ შემთხვევაში). სიცხადისათვის G-ოპერაციის შესაბამისი მატრიცი აღვნიშნოთ $A_{a,b,c}$–თი. ჩვენ გამოვიყენებთ იგივე A სიმბოლოს ინდექსებით იმ მატრიცების აღსანიშნავად, რომლებიც შეესაბამებიან სხვა ელემენტარულ გეიტებს.

მაგალითად, *NOT*-ს წარმოვადგენთ A_a ოპერატორის შესაბამისი *2x2*-მატრიცი

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

რომელიც შეიძლება ჩაიწეროს მრავალი გზით სხვადასხვა აღნიშვნებში, მაგრამ ჩვენ ავირჩევთ იმ ხერხს, რომელიც ეთანადება წარმოქმნისა და გაქრობის ოპერატორების მეთოდს. განვიხილოთ ამ შემთხვევაში ერთ a ხაზზე მოქმედება. ეს მოქმედება $\underline{a}$– სიმბოლოთი აღვნიშნოთ.

$$\underline{a} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

მატრიცი აქრობს 1-ს a ატომზე, და გარდაქმნის მას 0-ად; სხვა სიტყვებით, $\underline{a}$ არის ოპერატორი, რომელსაც $|1\rangle$ მდგომარეობა გადაყავს $|0\rangle$ მდგომარეობაში. მაგრამ, თუკი ატომი საწყის $|0\rangle$ მდგომარეობაში იყო, მაშინ $\underline{a}$ ოპერატორი მოგვცემს რიცხვს 0-ს, ანუ ის არ ცვლის მდგომარეობას, ის უბრალოდ იძლევა ნულოვან რიცხვით მნიშვნელობას მასზე ზემოქმედებისას. $\underline{a}$-ს შეუღლებული

$$\underline{a}^* = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

მატრიცი, რომელიც წარმოქმნის ოპერატორია იმ აზრით, რომ $|0\rangle$ მდგომარეობა მას გადაყავს $|1\rangle$ მდგომარეობაში. $|1\rangle$ მდგომარეობაზე მოქმედებისას ის იძლევა 0-ს, რადგანაც არ არსებობს შემდეგი მდგომარეობა, რომელიც შეიძლება შეიქმნას. ნებისმიერი სხვა 2×2 მატრიცული ოპერატორი შეიძლება წარმოვადგინოთ ამ $\underline{a}$ და $\underline{a}^*$ ოპერატორების ტერმინებში. მაგალითად, ნამრავლი $\underline{a}^*\underline{a}$, ტოლია

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

მატრიცის, რომელიც N_a-თი აღვნიშნოთ. ის იძლევა 1-ს, თუ იმოქმედებს $|1\rangle$-ზე, და 0-ს, თუ იმოქმედებს $|0\rangle$ მდგომარეობაზე, ანუ, სხვა სიტყვებით, იძლევა ატომის მდგომარეობის ნომერს. ანალოგიურად ნამრავლი

$$\underline{a}^*\underline{a} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

არის $1-N_a$, რომელიც იძლევა 0-ს ზედა მდგომარეობისათვის და 1-ს, ქვედასათვის. 1-იანი გამოიყენება

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

დიაგონალური მატრიცის აღსანიშნავად. ზემოთ ნათქვამიდან გამომდინარეობს, რომ $\underline{a}\,\underline{a}^* + \underline{a}^*\underline{a} = 1$.

ახლა ნათელია, რომ მატრიცი, რომელიც წარმოქმნის *NOT* ოპერატორს არის $A_a = \underline{a} + \underline{a}^*$, ნათელია აგრეთვე, რომ იგი შებრუნებადია და $A_a^* A_a = 1$.

მსგავსი მოსაზრებით *CONTROLLED NOT*-თვისაც შეიძლება $A_{a,b}$ მატრიცის მიღება. თუ დავაკვირდებით *CONTROLLED NOT* ჭეშმარიტობის ცხრილს, შევნიშნავთ, რომ ის შეიძლება დაიწეროს შემდეგი

$$\underline{a}^*\underline{a}\left(\underline{b} + \underline{b}^*\right) + \underline{a}\underline{a}^*$$

სახით. პირველი $\underline{a}^*\underline{a}$ შესაკრები გამოყოფს პირობას $a = 1$. ამ შემთხვევაში ჩვენ გვინდა, რომ $\underline{b} + \underline{b}^*$-მ, ე.ი. *NOT*-მა იმოქმედოს b-ზე. მეორე შესაკრები გამოყოფს იმის პირობას, რომ ხაზი a ტოლია *0*-ის; ამ შემთხვევაში ჩვენ არ გვინდა, რომ b-ზე რაიმემ იმოქმედოს, ანუ იგულისხმება, რომ b-ზე მოქმედებს ერთეულოვანი მატრიცი. ეს შეიძლება ასეც დაიწეროს

$$1+\underline{a}^*\underline{a}\left(\underline{b} + \underline{b}^* - 1\right).$$

აქ 1 შეესაბამება იმას, რომ ყველა ხაზი უცვლელია, მაგრამ $a = 1$ შემთხვევაში ჩვენ გვსურდა ეს გაგვესწორებინა, *NOT*-ის ჩასმით, იმის ნაცვლად, რომ b ხაზი დარჩენილიყო შეუცვლელი.

როგორი სახე აქვს *CONTROLLED CONTROLLED NOT* მატრიცს, თქვენ ალბათ უკვე მოხვდით:

$$A_{ab,c} = 1 + \underline{a}^* a\, \underline{b}^*\underline{b}(\underline{c} + \underline{c}^* - 1).$$

შემდეგი საკითხი–როგორ გამოიყურება მატრიცი მიმდევრობითი შეერთებული ელემენტარული გეიტებისაგან შედგენილი ლოგიკური ბლოკისათვის? განვიხილოთ სრული მაჯამებლის მაგალითი. ზემოთ იგი უკვე აღვწერეთ (იხ.ნახ.5). ახლა, საზოგადოდ, ოთხი გამტარი გვექნება, აღვნიშნოთ ისინი a, b, c და d-თი. აუცილებელი არ არის, რომ d ყოველთვის 0-ად ჩავთვალოთ. გვინდა ზოგად შემთხვევაში აღვწეროთ ასეთი ობიექტის ქმედება (თუ d გახდება 1-ის ტოლი, მაშინ d' მასზე *NOT*-ს მოქმედებით მიიღება). შედეგად ახალი a', b', c' და d' რიცხვები მიიღება. შეგვიძლია ჩვენი სისტემა წარმოვადგინოთ როგორც ოთხი a, b, c და d ატომების ერთობლიობა, რომელიც $|a, b, c, d\rangle$ მდგომარეობაში იმყოფება. M მატრიცი მოქმედებს ამ ოთხ ატომზე ისე, რომ ცვლის მდგომარეობას $|a', b', c', d'\rangle$ მდგომარეობით. ამრიგად, $|\psi_{in}\rangle$ არის ოთხი ბიტის შემავალი მდგომარეობა, ხოლო M მატრიცი კი გამოსავალი მდგომარეობების გენერირებას ახდენს: $|\psi_{out}\rangle = M|\psi_{in}\rangle$.

მაგალითად, თუ შემავალი მდგომარეობა იქნებოდა $|1,0,1,0\rangle$, მაშინ როგორც ვიცით გამოსავალი მდგომარეობა უნდა ყოფილიყო $|1,0,0,1\rangle$; პირველი ორი a', b' უნდა იყოს 1,0, რადგან ეს ორი ხაზი არ იცვლება, ბოლო ორი c', d' უნდა იყოს 0,1, რადგან ისინი არიან ჯამი და პირველი სამი a, b, c ბიტის გადატანა, როდესაც $d = 0$. ამჯერად, მავჯამებლისთვის M მატრიცი შეიძლება განხილული იქნას როგორც ხუთი ელემენტარული ოპერაციის თანმიდევრულად შესრულების შედეგი და ამრიგად, იმ ხუთი მატრიცის ნამრავლი, რომლებიც ელემენტარულ ოპერაციებს შეესაბამებიან:

$$M = A_{a,b}A_{b,c}A_{bc,d}A_{a,b}A_{ab,d}.$$

პირველი მატრიცი, უკიდურესი მარჯვენა, არის $A_{ab,d}$, რადგან იგი *CONTROLLED CONTROLLED NOT*–ია, რომელშიდაც a და b მაკონტროლებელი ხაზებია, ხოლო *NOT* ძევს d-ზე. შევხედავთ რა დიაგრამას ნახ.5-ზე დავინახავთ, თუ რას შეესაბამება სხვა მამრავლები. მაგალითად, ბოლო $A_{a,b}$ მამრავლი არის *CONTROLLED NOT* a მაკონტროლებელი ხაზით და *NOT* ძევს b ხაზზე. ეს მატრიცი უნიტარულია -- $M^*M = 1$, რადგან არის უნიტარული A მატრიცების ნამრავლი. ე.ი. M შებრუნებადი მატრიცია და M^* არის მისი შებრუნებული.

ამრიგად, ჩვენი მთავარი ამოცანა შემდეგში მდგომარეობს: ვთქვათ $A_1, \dots, A_k$ რომელიმე ბლოკში საჭირო ოპერაციებია, რომლებიც n ხაზზე მოქმედებენ. $2^n \times 2^n$-ზომის M მატრიცი, რომელიც აუცილებელია ამ მიზნის მისაღწევად, არის $A_k \dots A_1$ ნამრავლი, სადაც ყოველი A რაიმე მარტივი მატრიცია. თუ ცნობილია როგორ შევქმნათ უფრო მარტივი ელემენტები, როგორაა შესაძლებელი ამ M მატრიცის ფიზიკური რეალიზაცია?

საზოგადოდ, კვანტურ მექანიკაში, სისტემისათვის H ჰამილტონიანით, დროის t მომენტში მდგომარეობები გამოსავალზე არის $e^{iHt}\psi_{in}$, სადაც ψ_{in} მდგომარეობაა შესავალზე. ვიპოვოთ ჰამილტონიანი, რომელიც t მომენტისათვის მოგვცემს $M = e^{iHt}$-ს, სადაც M გარკვეული სიმარტივის მატარებელი არაკომუტაციური მატრიცების ნამრავლია, რთული ამოცანაა.

შევნიშნოთ, რომ თუ e^{iHt}-ს დავშლით, როგორც $1 + iht - \frac{H^2t^2}{2} - \cdots$, მაშინ გავარკვევთ, რომ H ოპერატორი მოქმედებს "გაურკვეველჯერ" (ერთჯერ, ორჯერ, სამჯერ, და ა.შ.) და სრული მდგომარეობა მიიღება როგორც ყველა შესაძლო სუპერპოზიცია. ეს გვკარნახობს, რომ ამ A მატრიცების აგების ამოცანა შემდეგნაირად გადავჭრათ. რეგისტრში მყოფ n ატომს დავუმატოთ სრულიად ახალი $k+1$ რაოდენობის ახალი ატომები, რომლებსაც ვუწოდოთ "პროგრამულად წაკითხვადი უჯრედები". აღვნიშნოთ შესაბამისად i უჯრედისათვის წარმოქმნისა და გაქრობის ოპერატორები q_i და q_i^* სიმბოლოებით. მაგალითისათვის შეგვიძლია წარმოვიდგინოთ ელექტრონი. რომელიც ერთი თავისუფალი უჯრედიდან მეორეში გადადის. თუ i უჯრედში

ელექტრონია, მაშინ მისი მდგომარეობა იქნება $|1\rangle$, თუ უჯრედი თავისუფალია, მაშინ $|0\rangle$.მივიღებთ ჰამილტონიანს

$$H = \sum_{i=0}^{k} q_{i+1}^{*} q_i A_{i+1} + \text{კომპლექსურად შეუღლებულები} =$$
$$q_1^{*} q_0 A_1 + q_2^{*} q_1 A_2 + q_3^{*} q_2 A_3 + \cdots + q_0^{*} q_1 A_1^{*} + q_1^{*} q_2 A_3^{*} + \cdots$$

უპირველეს ყოვლისა შევნიშნოთ, რომ თუ ყველა პროგრამული უჯრედი დაკავებული არ არის, ე.ი. თუ ყველა პროგრამული ატომი თავიდან $|0\rangle$ მდგომარეობაში იმყოფებოდა, მაშინ არაფერი არ მოხდება, რადგან ჰამილტონიანის ყოველი წევრის ქმედება დაიწყება გაქრობის ოპერატორით, რომელიც 0-ს მოგვცემს.

მეორეც, თუ მხოლოდ ერთია (ერთი ან მეორე) დაკავებული პროგრამული უჯრედიდან, ხოლო დანარჩენები კი თავისუფალია (იმყოფებიან მდგომარეობაში $|0\rangle$), მაშინ ეს დებულება ყოველთვის სამართლიანია. მართლაც, პროგრამულ უჯრედთა რაოდენობა, რომლებიც $|0\rangle$ მდგომარეობაში იმყოფებიან, შენახვადი სიდიდეა. ვუშვებთ, რომ ჩვენი კომპიუტერის მუშაობის დროს ან ყველა უჯრა თავისუფალია (ამ შემთხვევაში არაფერი არ ხდება), ან მხოლოდ ერთი უჯრაა დაკავებული. კომპიუტერის ნორმალური ფუნქციონირებისას არასოდეს არ ხდება, რომ ორ ან ორზე მეტი პროგრამული უჯრედი იყოს დაკავებული.

დავიწყოთ ისეთი საწყისი მდგომარეობით, რომლის დროსაც უჯრედი ნულითაა დაკავებული (იმყოფება მდგომარეობაში $|0\rangle$), თუ კი მოგვიანებით, დროის გარკვეულ მომენტში რაიმე ბოლო უჯრედი k აღმოჩნდა q_0 მდგომარეობაში, ოპერატორი გააკეთებს იმას, რომ უჯრედი ნომრით 0 გახდება თავისუფალი, ხოლო q_1^{*} ოპერატორი დაკავებულს გახდის უჯრედს, რომლის ნომერია 1. ამრიგად, $q_1^{*} q_0$ წევრი დაკავებულ უჯრედს 0 პოზიციიდან 1 პოზიციაში გადაადგილებს. მაგრამ, ეს ყველაფერი მრავლდება A_1 მატრიცზე, რომელიც მხოლოდ n ატომების რეგისტრზე მოქმედებს. ამრიგად, n ატომების საწყისი მდგომარეობა მრავლდება A_1-ზე.

ახლა, თუ ჰამილტონიანს ვაიძულებთ მეორედ იმოქმედოს სისტემაზე, პირველი წევრი არაფერს მოგვცემს, რადგან q_0-ის ქმედება თავისუფალ არანულოვან უჯრედზე 0-ია. ოპერატორი, რომელიც ამჯერად "შედეგიანად მუშაობს", არის $q_1^{*} q_0 A_2$ შესაკრები, რადგან მხოლოდ მას შეუძლია დაკავებული უჯრედის გადაადგილება. ჩვენ მას "კურსორს" ვუწოდებთ. კურსორს შეუძლია უჯრედი 1-დან უჯრედ 2-ში გადაადგილოს, ხოლო A მატრიცი ამჯერად მოქმედებს რეგისტრზე. ამრიგად, რეგისტრზე მოქმედებს $A_2 A_1$ მატრიცი. ჰამილტონიანის თანმიმდევრობით მოქმედებით კურსორი გადაადგილელდება 0-დან k-მდე და მივიღებთ ერთმანეთზე მიყოლებით A მატრიცებს, რომლებიც n ატომების რეგისტრებზე ისეთი თანმიმდევრობით

მოქმედებენ, როგორც M მატრიცის ასაგებადაა საჭირო. ამასთან ჰამილტონიანი ერმიტული უნდა იყოს, ამიტომ ყოველ ოპერატორს თავისი შეუღლებული თან უნდა სდევდეს. დავუშვათ გარკვეულ ეტაპზე გვაქვს კურსორი უჯრედზე ნომრით 2 და რეგისტრზე მოქმედი A_2A_1 მატრიცი. q_2 ოპერატორი, რომელიც საჭიროა კურსორის ერთი მდგომარეობიდან ახალ მდგომარეობაში გადასაყვანად, შესაძლოა შედიოდეს სხვა შესაკრებშიც. მართლაც, ის შედის $q_1^*q_2A_2^*$ შესაკრებში, რომელიც კურსორს 2 პოზიციიდან 1 პოზიციაში გადაიყვანს, ამასთან, როდესაც ასეთი რამ ხდება, რეგისტრზე მოქმედი სრული ოპერატორი იქნება $A_2^*A_2A_1$. მაგრამ, $A_2^*A_2 = 1$, დარჩა მხოლოდ A_1. ამრიგად, ვხედავთ, რომ როდესაც კურსორი ბრუნდება პოზიციაში 1, მაშინ რეგისტრზე რეალურად მხოლოდ A_1 ოპერატორი მოქმედებს.

საერთო ჯამში, მას შემდეგ, რაც ჰამილტონიანის სხვადასხვა წევრები ამოძრავებენ კურსორს წინ და უკან, A მატრიცები ან გროვდებიან ნამრავლში, ან თანამამრავლთა რიცხვი თანდათან იკლებს. ფუნქციონირების ნებისმიერ ეტაპზე, მაგალითად, თუკი კურსორი იქნებოდა j მდგომარეობაში, მატრიცები A_1-დან A_j-მდე იმოქმედებდნენ n რეგისტრზე თანმიმდევრობით, არ აქვს მნიშვნელობა როგორ მოხვდებოდა იგი j მდგომარეობაში, პირდაპირ იმოძრავებდა 0-დან j-მდე თუ ივლიდა წინ და დაბრუნდებოდა უკან, თუ იმოძრაებდა უკან და წინ ნებისმიერად, მთავარია ის, რომ კურსორი საბოლოოდ აღმოჩნდა j მდგომარეობაში. ამრიგად, თუ კურსორი იმყოფებოდა k უჯრედზე, მაშინ M მატრიცი n ატომების რეგისტრის საწყის მდგომარეობაზე მოქმედებს. რაც მოითხოვებოდა.

როგორ შევძლებთ ოპერაციები ვაწარმოოთ ამ კომპიუტერზე? ვიწყებთ იმით, რომ ჩავტვირთავთ შესავალ ბიტებს რეგისტრებში და მოვათავსებთ კურსორს 0-ოვან უჯრედზე. შემდეგ ვამოწმებთ k უჯრედს, ვთქვათ, ელექტრონების გაფანტვით, არის თუ არა იგი დაკავებული, ან იმყოფება თუ არა მასზე კურსორი. ამ დროს, ვხედავთ რა კურსორს k უჯრედზე, ჩვენ უკუვაგდებთ მას ისე, რომ კურსორს არ შეეძლოს პროგრამულ ხაზზე დაბრუნება. ამის შემდეგ ვიცით, რომ რეგისტრი გამოსავალ მონაცემებს შეიცავს. როდესაც ჩვენთვის ხელსაყრელი იქნება, მაშინ შეგვეძლება მისი გაზომვა. რა თქმა უნდა, გაზომვის პროცესში ჩართულია გარე ფაქტორები, ისინი არ არიან ჩვენი კომპიუტერის ნაწილი. ცხადია, ისიც, რომ ბოლოს და ბოლოს კომპიუტერმა უნდა იმოქმედოს გარე სამყაროსთან როგორც მონაცემთა ჩატვირთვის, ასევე მათი ამოკითხვის დროს.

მათემატიკურად აღმოჩნდა, რომ კურსორის მოძრაობა პროგრამული ხაზის გასწვრივ ზევით და ქვევით ექვივალენტურია იმისა, თითქოს ჰამილტონიანში არ იყოს A ოპერატორები. სხვა სიტყვებით, ესენი არიან ერთგანზომილებიანი სპინური ტალღები ან ის ტალღები, რომლებიც ძლიერ

შეკავშირებული ელექტრონების გავრცელების ამოცანიდანაა ცნობილი. ესენი ის ტალღებია, რომლებიც მოძრაობენ ზევით და ქვევით წრფეზე, შესაძლოა გვქონდეს აგრეთვე ტალღური პაკეტები და ა.შ. შეგვიძლია სრულვყოთ კომპიუტერის მუშაობა გადავიყვანოთ იგი ბალისტიკურ ქმედებაში, დამატებითი უჯრედების მწკრივის შექმნით იმ უჯრედების შიგნით, რომლებსაც რეალურად ვიყენებთ გამოთვლებისას ან მრავალ უჯრედთა მწკრივი დამატებით მანამდე და მის შემდეგ. ეს იქნება იგივე, თითქოს გვქონდა i ინდექსის მნიშვნელობა q_i-სათვის, რომელიც 0-ზე მეტი და k-ზე ნაკლებია და ყოველთვის A მატრიცზე გამრავლების ნაცვლად ყოფილიყო 1-ზე გამრავლება. ასეთ პირობებში გვექნებოდა გრძელი სპინური ჯაჭვი და დავიწყებდით კურსორის მიყვანით სხვადასხვა უჯრედებზე შესაბამისი ამპლიტუდის მეშვეობით (შესავალ სპინურ ტალღას წარმოვადგენთ მიახლოებით იმპულსების ფართო პაკეტით), იმის ნაცვლად, რომ კურსორი დაგვეყენებინა საწყის 0-ოვან უჯრედზე. ეს სპინური ტალღა ბალისტიკურად გაივლიდა მთელ კომპიუტერს და გავიდოდა გამოსავალ მოწყობილობაში, რომელსაც დავუმატებთ ჩვენი პროგრამული უჯრედების ჯაჭვს. სად არის პასუხი, შესაძლებელია ადვილად განისაზღვროს ან გადატანილი იქნას სხვა ადგილზე მისი კურსორით ჩაწერის შემდეგ. ამრიგად, ლოგიკური ელემენტი შესაძლოა ბალისტიკურად მოქმედებდეს.

მნიშვნელოვანი მომენტი ისაა, რომ გამოთვლითი თეორიის სპეციალისტებს მაინც შეუძლიათ აჩვენონ, რომ უნივერსალური კომპიუტერი აიგება, თუ ნებისმიერი ლოგიკური ელემენტის გაკეთებაა შესაძლებელი. ჯერ-ჯერობით უცნობია, როგორ წარმოვადგინოთ უნივერსალური კომპიუტერი ლოგიკურ ელემენტთა ნებისმიერი ერთობლიობისაგან. ამისათვის საჭიროა დამატებითი ინფორმაცია, რომელსაც შემდგომში შევეხებით.

ნაკლოვანებები და თავისუფალი ენერგიის დაკარგვის შეუქცევადობა

ბევრი კითხვა ჩნდება და მათი უფრო დაწვრილებით განხილვაა საჭირო. კერძოდ, ყურადღება გვინდა გავამახვილოთ იმ სიძნელეებზე, რომლებიც ასეთი სისტემის აგების დროს წარმოიშვება.

არსებობს სიძნელეების ბევრი წყარო ამგვარ მანქანებში და პირველ რიგში ჩვენ ყურადღებას გავამახვილებთ იმაზე, რომ სავარაუდოდ კავშირში, პროგრამული ხაზების ურთიერთკავშირის კოეფიციენტები შეიძლება განსხვავებულები აღმოჩნდნენ. თუ ეს ხაზები იქნებიან საკმარისად გრძელები, როგორც რეალურ გამოთვლებშია, მცირე არარეგულარულობა გამოიწვევს ტალღის გაფანტვას და ის გადაიხრება ბალისტიკურიდან. მაგალითად, თუ ის უჯრედები, რომლებისგანაც შედგება სისტემა, წარმოადგენენ ჩვეულებრივ ფიზიკურ ატომებს, მაშინ მათი სითბური ვიბრაციები გამოიწვევს მცირე რაოდენობის ბიტებს შორის კავშირის ცვლილებებს და შექმნის სიძნელეებს

(ჩვენთვის აუცილებელიც კი არის ასეთი ხმაური, რადგან მცირე ფიქსირებული დეფექტების პირობებში არსებობს ზედაპირული შემაჩერებელი ზონები, რომლებშიც შეიძლება ჩავიჭიროთ კურსორი). დავუშვათ p არის ნებისმიერ მდგომარეობამდე კურსორის იმპულსის გაფანტვის ალბათობა გამოთვლის ყოველ ბიჯზე (სხვა სიტყვებით რომ ვთქვათ, კურსორის გადაადგილების ყოველ $i \to i+1$ ბიჯზე. $\frac{1}{p}$ თავისუფალი განარბენის საშუალო სიგრძეა). ვთქვათ p ალბათობა საკმაოდ მცირეა. მაშინ ძალიან გრძელი გამოთვლებისათვის ტალღას დაჭირდება დიდი დრო მთელი გზის გასავლელად, რადგან გაფანტვის გამო მას ბევრჯერ მოუწევს უკან დაბრუნება. ეს კი მიგვიყვანს იქამდე, რომ კურსორი პროგრამული ხაზის გასწვრივ უნდა ვატაროთ რაიმე გარე ძალის მეშვეობით. თუ კურსორი მაგალითად, წარმოადგენს ელექტრონის გადადგილებას, რომელიც გადაადგილდება ერთი თავისუფალი უჯრედიდან მეორესკენ, მაშინ მივიღებთ, რომ თითქოს ელექტრული ველი ცდილობს გადაადგილოს ელექტრონი მავთულის გასწვრივ, რომლის წინაღობა წარმოდგენილია დეფექტებით ან გაფანტვის ალბათობით. ასეთ გარემოებაში შეიძლება გამოითვალოს ამ გარე ძალის მიერ მოხმარებული ენერგია.

ასეთი ანალიზის ჩატარება მარტივად შეიძლება, ეს არის ელექტრონის თავისუფალი განარბენის თითქმის კლასიკური ანალიზი. ყოველთვის, როდესაც კურსორის გაფანტვა ხდება, ჩვენ ვგულისხმობთ, რომ იგი შემთხვევით გაიფანტება წინ ან უკან. რა თქმა უნდა, იმისათვის, რომ მანქანამ რაიმე მოქმედება შეასრულოს, მან უნდა იმოძრაოს წინ უფრო დიდი ალბათობით, ვიდრე უკან. როდესაც გაფანტვა ასე გამჟღავნდება, მაშინ ენტროპიის დანაკარგი არის იმ ალბათობის ლოგარითმი, რომ კურსორი მოძრაობს წინ, გაყოფილი იმის ალბათობაზე, რომ კურსორი მოძრაობს უკან. ეს სიდიდე შესაძლებელია აპროქსიმირებული იქნას შემდეგნაირად:

$$\frac{\textit{წინ გაფანტვის ალბათობა} - \textit{უკან გაფანტვის ალბათობა}}{\textit{წინ გაფანტვის ალბათობა} + \textit{უკან გაფანტვის ალბათობა}}$$

ეს იყო ენტროპიის დანაკარგი გაფანტვის ერთი აქტის დროს. ჩვენთვის კი უფრო საინტერესოა ენტროპიის დანაკარგები გამოთვლების მთელ ჯაჭვზე, რომელიც ტოლია p სიდიდის ნამრავლისა ნაბიჯების რაოდენობაზე. შეგვიძლია გამოვთვალოთ ენტროპიის დანაკარგი გამოთვლის ერთ ნაბიჯზე, როგორც

$$\frac{pv_D}{v_R}$$

სიდიდე, სადაც v_D კურსორის დრეიფის სიჩქარეა, ხოლო v_R კი შემთხვევითი სიჩქარე.

სხვა სიტყვებით რომ ვთქვათ, $\frac{1}{p}$ საზოგადოდ არის დრო, გამრავლებული იმ მინიმალურ დროზე, რომელიც საჭიროა გამოთვლების ჩასატარებლად

(ე.ი. თუ ყველა ნაბიჯი შესრულებულია პირდაპირი მიმართულებით) და გაყოფილი რეალურად საჭირო დროზე. ასეთ პირობებში თავისუფალი ენერგიის დანაკარგი ერთი ნაბიჯის შემდეგ ტოლი იქნება $kT \times p \times$ *(მინიმალური დრო)*, რომელშიც ეს გამოთვლა შეიძლება განხორციელდეს, გაყოფილი იმ რეალურ დროზე, რომელიც საჭირო იქნება ამ ოპერაციის ჩასატარებლად. ეს ფორმულა მიიღო ბენეტმა. მამრავლი p წარმოადგენს გამაგლუვებელ ფაქტორს იმ შემთხვევაში, რომელშიც ყოველი უჯრედი წარმოადგენს კურსორის შემთხვევით გაფანტვას, მცირე ალბათობით. მხედველობაში უნდა მივიღოთ ის, რომ ენერგეტიკული დანაკარგი ყოველ ნაბიჯზე არ არის kT-ს ტოლი, არამედ წარმოადგენს ორი სიდიდის ნამრავლს. პირველი, $\frac{1}{p}$, შეესაბამება იმას, თუ რამდენად სრულყოფილად შეგვიძლია ავაგოთ მანქანა, ხოლო მეორე პროპორციულია იმ დროის მონაკვეთისა, რომელიც საჭიროა გამოთვლების ჩასატარებლად. ყოველივე ეს ძალიან გავს კარნოს მანქანას, რომელშიც იმისათვის, რომ პროცესები წარიმართოს შექცევადად, საჭიროა მოქმედებები წარმოებდეს ძალიან ნელა. იდეალურია მანქანა, რომლისთვისაც $p=0$, ან მაშინ, როდესაც მანქანა გამოთვლებზე დახარჯავს უსასრულო დროს; ასეთ შემთხვევაში ენერგიის საშუალო დანაკარგი ნულის ტოლია.

საჭიროა აღინიშნოს, რომ განუზღვრელობის პრინციპს, რომელიც თავის მხრივ ადებს გარკვეულ განუზღვრელობას ენერგიასა და დროს, პირდაპირ არ მივყავართ რაიმე შეზღუდვებამდე. თუმცა ჩვენი კომპიუტერი წარმოადგენს მანქანას, რომელიც გამოთვლებს აწარმოებს, მაგრამ კურსორის საწინააღმდეგო მხარეს მისვლის დრო და გამომავალი რეგისტრის მნიშვნელობის გაზომვის პროცედურა (სხვა სიტყვებით–დრო, რომელიც საჭიროა გამოთვლების ჩასატარებლად) არ არიან განსაზღვრულები. ესენი ალბათური სიდიდეებია და ამიტომ ადგილი აქვს გარკვეულ განუზღვრელობას იმ დროში, რომელშიც გამოთვლები ხდება. არ არსებობს კურსორის ენერგიის განუზღვრელობასთან დაკავშირებული დანაკარგები. ყოველ შემთხვევაში, ეს დანაკარგები არ არიან კავშირში გამოთვლის ბიჯების რიცხვთან. რა თქმა უნდა, თუ თქვენ აწარმოებთ ბალისტიკურ გამოთვლებს სრულყოფილ მანქანაზე, ენერგიის რაღაც ნაწილი ჩადებული იქნება გამომავალ ტალღაში, მაგრამ ამ ენერგიას მიიღებთ უკვე გამომავალი ტალღიდან პროგრამული ხაზის დასრულებისას. ყველა საკითხი, რომელიც დაკავშირებულია ოპერატორის განუზღვრელობასთან და გაზომვის შეუქცევადობასთან, ასოცირდება შემავალ და გამომავალ ფუნქციებთან. ამგვარად, არ არსებობს სხვა შეზღუდვები, რომლებიც გამომდინარეობენ კომპიუტერის კვანტური ბუნებიდან და რომლებიც იქნებოდნენ გამოთვლის ბიჯების ჯამის პროპორციული.

ამ ტიპის მანქანაში ადგილი აქვს დიდი რაოდენობით სხვა პრობლემებს, რომლებიც უკავშირდება მის არასრულყოფილებას. მაგალითად, იმ რეგისტრებში, რომლებიც შეიცავენ მონაცემებს, შეიძლება წარმოიშვას წაკითხვასთან დაკავშირებული პრობლემები, რომელიც გამოწვეულია გარკვეული ატომებისა და მოცემული რეგისტრის სხვა ატომის ურთიერთზემოქმედებით ან რეგისტრების ატომებისა და იმ პროცესების ურთიერთზემოქმედებით, რომლებიც მიმდინარეობენ პროგრამული ხაზის გასწვრივ და რომელთა ასახვაც ზუსტად არ შეგვიძლია. სხვა სიტყვებით – ჰამილტონიანში შეიძლება არსებობდნენ მცირე წევრებიც უკვე აღწერილს გარდა. მანამ, სანამ ეს ფაქტორები არ იქნება მთლიანად გათვალისწინებული, ანალიზის ჩატარება ძნელი იქნება. ყოველ შემთხვევაში, რამდენიმე ამ პრობლემათაგანი შეიძლება გადაიჭრას იმ მარტივი მეთოდების მეშვეობით, როგორიცაა, მაგალითად, შეცდომების კორექტირების ტექნიკა. ეს საკითხი კარგადაა შესწავლილი ჩვეულებრივი კომპიუტერების თეორიაში. მაგრამ მანამ, სანამ არ გვიპოვნია ასეთი კომპიუტერის კონკრეტული რეალიზაცია, ჩვენ არ შემიძლია ვთქვათ, როგორ უნდა გაგრძელდეს ამ ეფექტების ანალიზი. თუმცა, საკმაოდ ნათელია, რომ ეს საკითხები ძალიან მნიშვნელოვანია პრაქტიკული თვალსაზრისით. ასეთი კომპიუტერი შესაძლებელია იყოს ძალიან მგრძნობიარე სისტემა და ასეთ წინააღმდეგობებს შეუძლიათ მიგვიყვანოს მისი მუშაობის მნიშვნელოვან გართულებამდე.

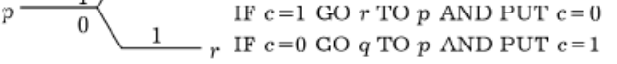
დრო, რომელიც საჭიროა გამოთვლების ჩატარების ერთი საფეხურისათვის, დამოკიდებულია დაძაბულობაზე ან ჰამილტონიანის წევრებს შორის ურთიერთზემოქმედების ენერგიაზე. თუ ჰამილტონიანის ყოველი ასეთი წევრი სავარაუდოდ იქნება 0,1 ელექტრონ-ვოლტის რიგის, მაშინ დრო, რომელშიც კურსორი ასრულებს ყოველ ნაბიჯს, თუ პროცესი ბალისტიკურია, იქნება 6×10^{-15} წამის რიგის. ეს სიჩქარის არც თუ ძლიერი გაზრდაა, იგი მხოლოდ ოთხი რიგით სწრაფია, ვიდრე არსებულ ტრანზისტორების შემთხვევაში, და ცოტათი ნელი, ვიდრე ოპტიკურ სისტემებში მიიღწევა.

უმარტივესი რეალიზაცია

ჩვენ ამოვხსენით დასმული ამოცანა–ვიპოვეთ გარკვეული კვანტურ-მექანიკური ჰამილტონიანი სისტემისათვის, რომელიც გამოთვლებისათვის შეიძლება იქნას გამოყენებული. მაგრამ კარგი იქნებოდა რაღაც გაგვეკეთებინა ასეთი სისტემის რეალიზაციისათვის. ჰამილტონიანი, რომელსაც ჩვენ ამოვწერთ, შეიცავს წევრებს, რომლებიც ასახავენ ხუთი ატომის განსაკუთრებულ ქმედებას. მაგალითად, სამი ასეთი ატომი გამოიყენება რეგისტრში *CONTROLLED CONTROLLED NOT* ოპერაციისათვის, ხოლო ორი დანარჩენი პროგრამული მრიცხველისათვის.

ამის გაკეთება შესაძლებელია, მაგრამ ძალზე ძნელია. შეგვიძლია გავაკეთოთ ისე, რომ ურთიერთქმედებაში მონაწილეობდეს მხოლოდ სამი ატომი. დავიწყებთ ახალი ელემენტარული გეიტებით. მივიღებთ იგივე *NOT* ოპერაციას, მაგრამ მისი დამატება იქნება მარტივი გადამრთველი.

ვთქვათ ჰამილტონიანში გვაქვს ასეთი წევრი *q*cp + r*c*p* და მისადმი კომპლექსურად შეუღლებული წევრი (ალფავიტის საწყისი ასოები გამოვიყენოთ რეგისტრის ატომებისათვის, ხოლო ბოლო ასოები – პროგრამული ადგილისათვის). ნახ. 7-ზე გამოსახულია გადამრთველის მოქმედება: თუ საწყის მომენტში *c* იმყოფება |1⟩-ში, მაშინ კურსორი *p*-დან გადაადგილდება *q*-ში. წინააღმდეგ შემთხვევაში, თუ *c* იმყოფება |0⟩-ში, მაშინ კურსორი გადაადგილდება *p*-დან *r*-ში. ამ ოპერაციის დროს კონტროლირებადი ატომი *c* იცვლის მდგომარეობას (შესაძლებელია ჩავწეროთ ისეთი გამოსახულება, სადაც *c* არ იცვლის მდგომარეობას. კერძოდ: *q*c*cp + r*cc*p* და მისი კომპლექსურად შეუღლებული. ეს არ იძლევა არც უპირატესობას და არც რაიმე ნაკლია (რაც განვიხილეთ, არის უმარტივესი შემთხვევა).

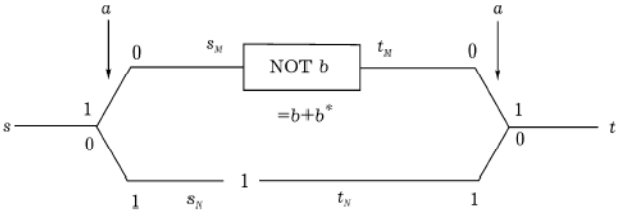


$$H = q^*cp + r^*c^*p + p^*c^*q + p^*cr$$

ნახ.7. *გადამრთველი*

კომპლექსური შეუღლება იწვევს საპირისპირო შედეგს. მაგრამ, თუ კურსორი იმყოფება *q*-ში და *c* იმყოფებოდა |1⟩ მდგომარეობაში (ან კურსორი არის *r*-ში, *c* კი |0⟩-ში), მაშინ *H = 0* და კურსორი უკან ბრუნდება. ჩვენ გავაკეთებთ ყველა სქემას და ვირჩევთ საწყის მდგომარეობას ისე, რომ ასეთი პირობები არ წარმოიქმნას ნორმალური ფუნქციონირების დროს და კომპიუტერმა იმუშავებს იდეალურ ბალისტიკურ რეჟიმში.

ასეთი გადამრთველით შეგვიძლია სხვადასხვა ოპერაციების მიღება, მაგალითად, შეგვიძლია მივიღოთ *CONTROLLED NOT* ოპერაცია, როგორც ეს ნაჩვენებია ნახ. 8-ზე: *a* გადამრთველი აკონტროლებს 0 ოპერაციას. დავუშვათ კურსორი იმყოფება *s* მდგომარეობაში. თუ *a = 1*, პროგრამული კურსორი მოძრაობს ზედა ხაზზე, ხოლო თუ *a = 0* კურსორი მოძრაობს ქვედა ხაზზე. ორივე შემთხვევაში ჩვენ მივიღებთ პროგრამულ *t* მდგომარეობას.



ნახ.8

გადამრთველის მეშვეობით CONTROLLED NOT-ის რეალიზაცია

ამ დიაგრამებზე ჰორიზინტალური და ვერტიკალური ხაზები პროგრამულ ატომებს აღნიშნავს. გადამრთველები გამოისახება როგორც დიაგონალური ხაზები, ხოლო მართკუთხედი წარმოადგენს რეგისტრებზე მოქმედ მატრიცებს, მაგალითად, როგორიცაა *NOTb*. ასე რომ ჰამილტონიანი *CONTROLLED NOT* ოპერაციისათვის, რომელიც იწყება s მდგომარეობით და მთავრდება t-თი, გამოისახება შემდეგი ჰამილტონიანით:

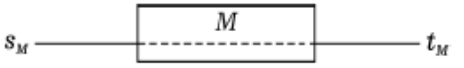
$$H_c(s,t) = s_M^* as + t^* a^* t_M + t_M^*(b+b^*)s_M + s_N^* a^* s + t^* a t_N +$$
$$t_N^* s_N + \text{წინა წევრების კომპლექსური შეულღება.}$$

ზემოთ თქმულიდან ჩანს, თითქოს არსებობს კვანტური მექანიკის ყველა სახის სრული მახასიათებლების მიღების ორი შესაძლებლობა, მაგრამ ეს ასე არ არის. თუ გამოთვლითი სისტემა გამოთვლას იწყებს a ატომის რაიმე განსაზღვრული მდგომარეობიდან და შემდეგ კურსორი აღწევს s მდგომარეობას, მაშინ a რჩება რაიმე განსაზღვრულ მდგომარეობაში (თუმცა შესაძლოა საწყისისგან განსხვავებულში, რაც განპირობებული იქნება მასზე ადრე ჩატარებული ოპერაციებით). ამიტომ ორიდან მხოლოდ ერთ გზას ვირჩევთ. თუ გამოსახულების გასამარტივებლად ჩავთვლით, რომ $t_N = s_N$, მაშინ წევრი $s_N^* t_N$ შეგვიძლია უგულებელვყოთ.

ასეთ შემთხვევაში არ უნდა შეგვაშფოთოს იმან, რომ ერთ-ერთი გზა (ორ-კურსორული პოზიცია) მეორეზე (ერთ-კურსორული პოზიცია) გრძელია, რადგან ინტერფერენციას არ აქვს ადგილი. არც ერთ ჩვენს მიერ განხილულ შემთხვევაში ადგილი არ ექნება არც გაბნევას.

განვიხილოთ ერთ ჯაჭვში გაერთიანებული ერთმანეთთან შეერთებული მონაკვეთები (იხ. ნახ. 9). ჯაჭვის M მონაკვეთი შეიძლება განვიხილოთ, როგორც ურთიერთმოქმედი ნაწილების ლოგიკური ელემენტი, რომელშიც ვგულისხმობთ კურსორის საწყის s_M და საბოლოო t_M მდგომარეობებს. დანარჩენი პროგრამული მდგომარეობები, რომლებიც s_M-სა და t_M–ს შორის გვექნება, წარმოდგენილები არიან M-ის შიგა ნაწილებად, M აგრეთვე შეიცავს საკუთარ რეგისტრებს, ხოლო s_M და t_M მდგომარეობები შესაძლოა იყოს დაკავშირებული გარე კავშირებით.

ასეთი ქვესისტემის ჰამილტონიანი აღვნიშნოთ $H_M(t_M, s_M)$-ით. s_M-სა და t_M-ის ქვეშ გვესმის საწყისი და საბოლოო პროგრამული მდგომარეობები. მაშასადამე, H_M იმ ჰამილტონიანის ნაწილია, რომელიც აღწერს ბოქსში შემავალი ყველა ატომის საწყის და საბოლოო მდგომარეობებს. განსაკუთრებით საინტერესო და მნიშვნელოვანია შემთხვევა, როდესაც გარე მონაცემები (რეგისტრის ატომები) მოდიან განსაზღვრული ლოგიკური ელემენტებიდან და ჩვენთვის აუცილებელია ამ მონაცემების სხვაგან გადატანა (იხ.ნახ.10).



ნახ. 9. *წრფის მონაკვეთის ნაწილი*

s_M – მონაკვეთის საწყისი პროგრამული მდგომარეობა.
t_M – მონაკვეთის საბოლოო პროგრამული მდგომარეობა.
$H_M(s_M, t_M)$-ჰამილტონიანის ნაწილი, რომელიც შეესაბამება ყველა "ატომს" და პროგრამულ მდგომარეობას შემავალს M ბოქსში, ავრეთვე მათ ურთიერთქმედებას s_M-თან და t_M-თან.

დავუშვათ *M* ბოქსი იწყებს მუშაობას თავისი შემავალი რეგისტრის იმ მდგომარეობიდან, რომელიც შეიცავს 0-ს და გამავალი რეგისტრის იმ მდგომარეობიდან (შესაძლებებლია იგივე), რომელიც ასევე 0-ის ტოლია. ამით შეგვიძლია შემდეგნაირად ვისარგებლოთ. პროგრამული ხაზი ასეთი წესით ავაგოთ: ვთქვათ ის იწყება s'_M მდგომარეობიდან და პირველი ოპერაციაა შემავალი მონაცემების გარე რეგისტრიდან ინფორმაციის გადადგილება იმ *M*-ურ შემავალ რეგისტრში, რომელიც მოცემულ მომენტში 0-ებს შეიცავს. მაშინ ჩვენი გამოთვლების პირველი ნაბიჯი იქნება, ვთქვათ s'_M-დან დაწყებული, *M*-ის რეგისტრსა და შიგა რეგისტრს შორის ინფორმაციის გაცვლა. ამასთან 0-ები შედის თავდაპირველ შემავალ რეგისტრში, ხოლო შემავალი მონაცემები იწერება *M* ბოქსის შიგნით. ამ დროს კურსორი იმყოფება s_M პოზიციაში (უკვე ავხსენით თუ როგორ ხდება ინფორმაციის გაცვლა *CONTROLLED NOT* ოპერაციის მაგალითზე). პროგრამული მოქმედებების ჩატარების შემდეგ s_M-დან t_M-მდე ჩვენ *M* ბოქსში ვპოულობთ გამოსავალ მონაცემებს. ამის შემდეგ *M* ბოქსის გამოსავალი რეგისტრი იწმინდება, ხოლო ინფორმაცია, რომელსაც იგი შეიცავს შეგვაქვს წინასწარ მომზადებულ გარე რეგისტრში, რომელიც თავდაპირველად შეიცავდა 0-ებს. ასე, რომ t_M-დან t'_M-მდე იცვლება ინფორმაცია ცარიელ გარე რეგისტრსა და *M* ბოქსის გამოსავალ რეგისტრს შორის.

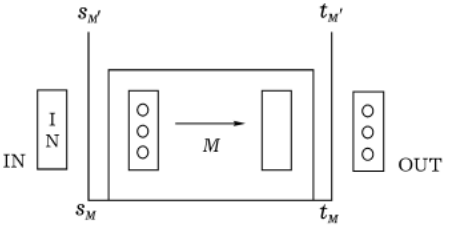
ჩვენ უკვე შეგვიძლია ასეთ ლოგიკურ ელემენტებს შორის მრავალმხრივად განვიხილოთ კავშირები. მაგალითად, თუ გვინდა ჯერ ვაწარმოოთ *M* ბოქსის მოქმედება, შემდეგ კი–*N*-ის, მაშინ შეგვიძლია

შევაკავშიროთ პირველის ბოლო და მეორის საწყისი პოზიციები (იხ. ნახ. 11). ამრიგად, ვღებულობთ ახალ *K* ოპერაციას, რომლის H_K ჰამილტონიანია

$$H_K(s_K, t_K) = H_M(s_K, t) + H_N(t, t_K)$$

გამოისახება. მოქმედებები სრულდება შემდეგი თანმიმდევრობით: თუ *a=1,* მაშინ სრულდება *M,* ხოლო თუ *a=0,* სრულდება *N* (იხილე ნახ.12). ამ ოპერაციისათვის ჰამილტონიანი ასე გამოისახება:

$$H_{cond}(s_c, t_c) = (s_M^* a s_c + t_c^* a^* t_M + s_N^* a^* s_c + t_c^* a t_N + \textit{კომპლექსური შეუღლებული}) +$$
$$+ H_M(s_M, t_M) + H_N(s_N, t_N).$$



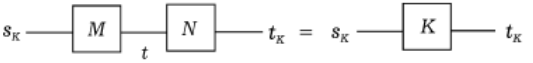
ნახ. 10

მონაკვეთი გარე შესასვლელითა და გასასვლელით

CONTROLLED NOT ოპერაცია არის ზემოთ მოყვანილი *M = NOTb*–ს კერძო შემთხვევა, რომლისთვისაც ჰამილტონიანს აქვს სახე:

$$H_{NOT\ b}(s, t) = s^*(b + b^*)t + \textit{კომპლექსურად შეუღლებული}$$

და *N* ოპერაცია შეესაბამება *s*t*-ს.

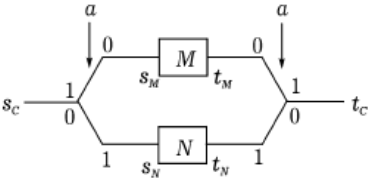


$$H_K(s_K, t_K) = H_M(s_K, t) + H_N(t, t_K)$$

ნახ.11.

ოპერაციების თანმიმდევრობა

სხვა მაგალითად შეგვიძლია განვიხილოთ "ნაგვის გამანადგურებელი" (იხ.ნახ.6), რომელიც შედგება არა ორი, პირდაპირი და საპირისპირო მოწყობილობებისაგან, არამედ საპირისპირო იყენებს იგივე მანქანას, რასაც პირდაპირი, ოღონდ აგზავნის მონაცემებს უკან, დანადგარში, საპირისპირო მიმართულებით მე-13 ნახაზზე გამოსახული გადამრთველის გამოყენებით. დავუშვათ, რომ ასეთი

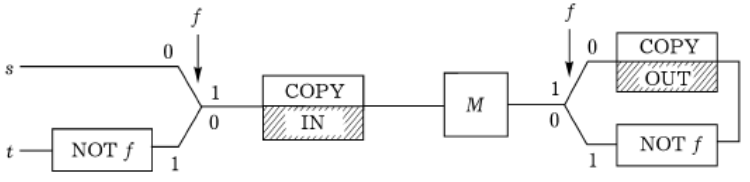


ნახ. 12

*კონტროლირებადი ოპერაცია: თუ **a**=1 სრულდება M, ხოლო თუ a=0 სრულდება N*

სისტემა შეიცავს სპეციალურ ალამს, რომელიც თავიდან ყოველთვის იმყოფება 0-ში. ასევე დავუშვათ, რომ საწყის მონაცემებს შეიცავს გარე რეგისტრი და ცარიელი გარე რეგისტრი გამოიყენება გამოსავალი მონაცემებისათვის. ასევე მანქანის ყველა რეგისტრი ცარიელია (შეიცავს 0-ებს). ასე, რომ ჩვენ მივიღებთ სისტემის საწყის *s* მდგომარეობას. უპირველესად გარე რეგისტრის შემადგენლობას გავუკეთებთ კოპირებას (*CONTROL NOT* ოპერაციის გამოყენებით) *M*-ში, შემდეგ მოქმედებს *M* და კურსორი გადადის ზედა პოზიციაზე. შემდეგ *M* ოპერატორის მოქმედების შედეგად მიღებულ მონაცემებს ვუკეთებთ კოპირებას გარე გამოსავალ რეგისტრში. ახლა *M* შეიცავს ნაგავს. *f* შევცვალოთ *NOT f*-ით და დავბრუნდეთ უკან გადამრთველის სხვა ხაზით, გადავდივართ *M*-ის მეორე მხარეს, ვათავისუფლებთ მას ნაგვისაგან, და გარე შემავალ რეგისტრში თავიდან ვუკეთებთ კოპირებას ყველაფერს. როდესაც მონაცემებს ვუკეთებთ კოპირებას, შემდეგ კი ამას ვიმეორებთ, ერთ-ერთი რეგისტრი ნულდება, კერძოდ კი ის, რომელსაც ჩვენ თავიდან გავუკეთეთ კოპირება. ასეთი კოპირების შემდეგ მონაცემები (რადგან *f* უკვე შეცვლილია) მიდის სხვა ხაზით, სადაც ჩვენ *f*-ში აღვადგინეთ *0*-ოვანი მნიშვნელობა *t* მომენტში. ასე რომ, *s*-დან *t*-მდე მონაკვეთზე ახლა გვაქვს ახალი მოწყობილობა, რომელსაც ქვემოთ მოყვანილი თვისებები აქვს.

მუშაობის დასაწყისში IN რეგისტრი შეიცავს საწყის მონაცემებს, გარე რეგისტრი OUT – კი 0-ებს. შიგა ალამი არის 0-ოვან მდგომარეობაში, *M* ბოქსი კი არ შეიცავს არავითარ მონაცემებს.



ნახ. 13

ნაგვის გამანადგურებელი

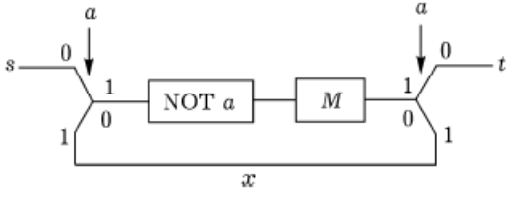
ჩატარებული მოქმედებების შედეგად შემავალ რეგისტრში t-მომენტში იქნება შემავალი მონაცემები, ხოლო გამომავალი რეგისტრი შეიცავს M ოპერატორის ქმედების შედეგს, M ცარიელი რჩება და f ალამი კი 0-ში მდებარეობს.

კომპიუტერული პროგრამისათვის ძალიან მნიშვნელოვანია ერთიდაიმავე ქვეპროგრამის მრავალჯერ გამოყენება. ლოგიკის თვალსაზრისით, რა თქმა უნდა, ამის მიღწევა შესაძლებელია ამ მონაკვეთის იმდენჯერ ჩაწერით, რამდენიც საჭიროა, მაგრამ პრაქტიკულად, გამოთვლების დროს, უკეთესი იქნებოდა თუ შეგვეძლებოდა კომპიუტერის ისეთი ნაწილის აგება, რომელსაც შეეძლებოდა ნაწილობრივ ქმედება, შემდეგ კი იგივეს მრავალჯერ გამოყენების საშუალება იქნებოდა. იმისათვის, რომ ამის შესაძლებლობა ვაჩვენოთ დავუშვათ, რომ გვჭირდება განსაზღვრული ოპერაციის ორჯერ მიმდევრობითი განმეორება (იხ. ნახ. 14). დავიწყოთ s მომენტიდან: a ალამი 0-ოვან მდგომარეობაშია. შემდეგ ვიმოძრავებთ რა ხაზის გასწვრივ შევამჩნევთ, რომ უპირველეს ყოვლისა შეიცვლება a-ს მნიშვნელობა. შემდეგ ჩავატაროთ ოპერაცია M. რადგან a-ს მნიშვნელობა შეცვლილია, იმის მაგივრად, რომ გავყვეთ ზედა ხაზს, საიდანაც დავიწყეთ, ვბრუნდებით ქვედა ხაზით, რომელიც აბრუნებს პროგრამას უკან a ალამის მნიშვნელობის მორიგი ცვლილების მომენტზე. ამგვარად, ყველაფერი თავიდან იწყება. ამჯერად M-ის გავლით გავალთ ქვეპროგრამიდან ზედა ხაზით და ასე მივაღწევთ საბოლოო მომენტ t-ს.

ამ სისტემის ჰამილტონიანი გამოისახება შემდეგნაირად

$$H_{MM}(s_c, t_c) = (s_M^* a^* s + s_M^*(a^* + a)s_N + x^* a^* t_M + s_N^* a x + t^* a t_M + \text{კომპლექსური შეუღლებული}) + H_M(s_M, t_M).$$

ასეთი სქემების გამოყენებით შესაძლებელია ოპერაციების ბევრჯერ განმეორება. მაგალითად, თუ იგივე იდეას სამჯერ გამოვიყენებთ ჩადგმული ციკლის ასაგებად, შევძლებთ ოპერაციის რვაჯერ განმეორებას მე-15 ნახაზზე მოყვანილი მოწყობილობის საშუალებით. ამისათვის დაგვჭირდება სამი a, b, c ალამი. ისინი საჭიროა იმის გასარკვევად, თუ პროგრამის რომელი ადგილიდან იწყება ოპერაცია და რამდენჯერ მეორდება. სხვა შემთხვევაში შექცევადობის მიღწევა შეუძლებელი იქნება.



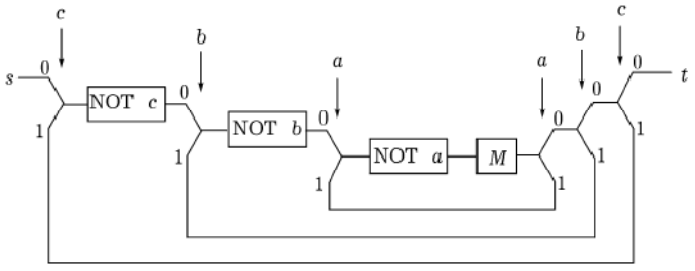
ნახ.14

M ოპერაციის 2-ჯერ გამმეორებელი მოწყობილობა

ჩვეულებრივ კომპიუტერში ქვეპროგრამა შეიძლება გამოვიყენოთ, შემდეგ გავანულოთ იგი და თავიდან გამოვიყენოთ ყოველგვარი ჩანაწერების გარეშე იმის შესახებ, თუ რა მოხდა. თუმცა მოცემულ შემთხვევაში ჩვენ უნდა შევინახოთ და ვაკეთოთ იგივე ალმებით, რათა ზუსტად ვიცოდეთ ქვეპროგრამის ციკლის გამოყენების რა მონაკვეთში ვიმყოფებით.

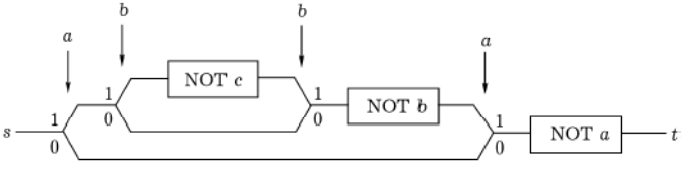
თუ ქვეპროგრამა გამოძახებულია პროგრამის განსაზღვრული ადგილიდან და უნდა დაბრუნდეს რაიმე სხვა ადგილზე, მაშინ მისი შემდგომი გამოძახების დროს მისი საწყისი და საბოლოო მდგომარეობები განსხვავებულია წინა შემთხვევისაგან. ჩვენ აუცილებლად უნდა ვიცოდეთ და დავიმახსოვროთ თუ საიდან მოვიდა იგი და სავარაუდოდ სად უნდა მივაკითხოთ ინდივიდუალურად ყოველი ასეთი შემთხვევისათვის, ასე, რომ აუცილებელია დიდი რაოდენობით მონაცემების შენახვა. პროგრამის მრავალჯერ გამოყენება შექცევად მანქანებში უფრო რთულია, ვიდრე ჩვეულებრივ მანქანებში. ყველაფერი ეს განხილული იყო ფრედკინის, ბენეტის და ტოფოლის ნაშრომებში.

აქედან ჩანს, რომ ალმებისა და ხისებური სტრუქტურის მქონე გადამრთველების გამოყენებით ჩვენ შეგვიძლია მონაცემების ჩაწერა მეხსიერების ნებისმიერ ადგილზე. მეხსიერებაში იგულისხმება ადგილი, სადაც მდებარეობს მონაცემების შემცველი რეგისტრები და რეგისტრები, რომლებსაც პროგრამა მიმართავს.



ნახ. 15

M ოპერაციის 8-ჯერ გამამეორებელი მოწყობილობა



ნახ. 16

ზრდადი, 3 ბიტიანი მრიცხველი

კურსორი იმოძრავებს ამ მონაცემების შესაბამისად. ალბათ უნდა არსებობდეს სხვა გადამრთველების სისტემები, რომლებიც საშუალებას მოგვცემს მონაცემების ჩაწერის შემდეგ დავაბრუნოთ კურსორი უკან და ამავე დროს სისტემა დარჩეს შექცევადი.

მე-16 ნახაზზე ნაჩვენებია ბინარული მრიცხველი (შეიცავს სამ *a, b, c* ბიტს, რომელთაგან *c* გამორჩეული ბიტია თავისი მნიშნელობით), რომელიც ინახავს ინფორმაციას იმის შესახებ, თუ რამდენჯერ გაიარა კურსორმა *s*-დან *t*-მდე. მოყვანილი მაგალითებიდან ჩანს, რომ შესაძლებელია ნებისმიერი ფუნქციის აგება გადამრთველებისა და *NOT* ოპერაციის გამოყენებით.

დასკვნა

შემოთავაზებული მაგალითებიდან ჩანს, რომ განხილულ კვანტურ მანქანაში სინამდვილეში არ არის გამოყენებული კვანტური მექანიკის დიფერენციალური განტოლების ყველა სპეციფიური თვისება.

ჩვენ ვცდილობდით, რამდენადაც ეს შესაძლებელი იყო, ციფრული მანქანის მუშაობის იმიტირებას. ცნობილია, რომ ჩვეულებრივ კომპიუტერებში ტრანზისტორების გამოყენებისას არ ვიყენებთ მათი თვისებების მთელ ანალოგურ კონტინუუმს, არამედ ვიყენებთ მათ როგორც ციფრულ მოწყობილობას ჩართულ-გამორთული მდგომარეობით. ამ შემთხვევაში სისტემის ქცევის ლოგიკური ანალიზია გამარტივებული. უფრო მეტიც, ასეთი სისტემა აბსოლუტურად თანმიმდევრულია. მაგ.: *ორი k* ბიტიანი რიცხვის შედარებისას თანმიმდევრულად უნდა შევადაროთ ყოველი მათი ბიტი ერთმანეთს. საკითხი იმის შესახებ, თუ როგორ მოვიქცეთ, რომ გავზარდოთ კვანტურ სისტემაში ერთდროულად მოქმედი ოპერაციების სიჩქარე, ამ შრომაში არ განხილულა.

თეორიული და აკადემიური მიზეზებით ჩვენ შევისწავლეთ მხოლოდ ჩაკეტილი და შექცევადი სისტემები, თუმცა, თუ ასეთი მცირე მანქანების პრაქტიკულად შექმნა მოხერხდება, არ არის ცხადი, რატომ არ შეიძლება ისეთი ურთიერთქმედების წარმოქმნა ოპერაციის შესრულების დროს, რომელსაც შეუბრუნებამობამდე და ენტროპიის ზრდამდე მივყავართ. მაგალითად, რთული და გრძელი გამოთვლებით ჩვენ შეგვიძლია დავამტკიცოთ, რომ სინამდვილეში კურსორს აქვს რაღაც ზღვარი, რომლის მიღწევისას მას აღარ შეუძლია უკან დაბრუნება. შეიძლება პრაქტიკული აღმოჩნდეს შეუქცევადი მეხსიერების შენახვის შეერთება შექცევად - ლოგიკურ და მოკლედ მოქმედ, შექცევად, დამმახსოვრებელ რეგისტრებთან. და მაინც, შესაძლებელია არ იყოს აუცილებელი ავაგოთ ერთმანეთთან დაკავშირებული უჯრედები იმისათვის, რომ განვახორციელოთ კავშირი დიდ მანძილებზე, მაშინ როდესაც ასეთ მანძილებზე კავშირი სინათლის სხივის ან მავთულის საშუალებით უფრო სწრაფი და მარტივია.

ყოველ შემთხვევაში, როგორც ჩანს, ფიზიკის კანონები არ გვიკრძალავს კომპიუტერის ზომების შემცირებას მანამ, სანამ ბიტის ზომები არ მიაღწევს ატომისას და კვანტური ქცევა არ გახდება დომინანტური.

ლიტერატურა

[1] C.H.Bennett, *Logical Reversibility of Computation*, IBM J.Res. Dev. **6**, 525-532, 1979.

[2] E.Fredkin and T.Toffoli, *Conservetive Logic,* Int. J. Theor. Phys. **21**, 219-259,1982.

[3] C.H.Bennett, *Thermodynamics of Computation - A Review*, Int. J. Theor. Phys. Syst. Theory **21**,905-940,1982.

[4] T.Toffoli, *Bicontinuous of invertible Combinatorical Functions*, Math. Syst. Theory **14**, 13-23, 1981.

[5] L.Priese, *On a Single Combinatorial Structure Sufficient for Sublying Non Trivial Self Reproduction*, J.Cybern. **6**, 102-137, 1976.

დეჯად დოიჩი (დაიბ. 1953 წელს ისრაელში), ოქსფორდის უნივერსიტეტის პროფესორი, კვანტური გამოთვლების ცენტრის თანაშემოქმედი კლარენდონის ლაბორატორიაში. დაჯილდოებულია დირაკის პრიზითა და მედლით (1998), მიღებულია აქვს პრიზი კომპიუტერული მეცნიერების დარგში (*Edge of Computation Science Prize 2005).* დეჯად დოიჩი კვანტური გამოთვლების ერთ-ერთი პიონერია. იგი ითვლება კვანტური მექანიკის ერერეტის ეულო მრავალსამყაროიანი ინტერპრეტაციის პროპაგანდისტად. ჰროფესორი დოიჩი დასაჯლეთის სამეცნიერო-პოპულარული საგნელეზიო არხების ხშირი სტუმარია. წინამდებარე სტატია არის *"Quantum theory, the Church-Turing principle and the universal quantum computer"*-ის თარგმანი. აღნიშნული შრომა გამოქვეყნდა 1985 წელს ჟურნალში *Proceedings of the Royal Society of London, A 400, pp.97-117.*

დ. დოიჩი

კვანტური თეორია, ჩიორჩ-ტიურინგის პრინციპი და უნივერსალური კვანტური კომპიუტერი

მოყვანილია არგუმენტები იმ აზრის სასარგებლოდ, რომლის თანახმად ჩიორჩ-ტიურინგის პრინციპი ფიზიკური დებულებაა. სტატიაში ეს დებულება ჩამოყალიბებულია ცხადი სახით: "ყოველი სასრული რეალიზებადი ფიზიკური სისტემა შესაძლოა სრულად იქნას მოდელირებული სასრული საშუალებების მქონე უნივერსალური მამოდელირებელი გამომთვლელი მანქანის მიერ". კლასიკური ფიზიკა და უნივერსალური ტიურინგის მანქანა არ აკმაყოფილებენ ამ პრინციპს: პირველი უწყვეტობის, მეორე – კი დისკრეტულობის გამო. აღწერილია გამოთვლითი მანქანების ერთი მოდელი, ტიურინგის მანქანის კვანტური განზოგადება და ნაჩვენებია, რომ კვანტური თეორია და "უნივერსალური კვანტური კომპიუტერი" ეთანხმებიან ამ პრინციპს.

გამომთვლელი მანქანები, რომლებიც უნივერსალური კვანტური მანქანების თვისებებს ატარებენ, პრინციპში შესაძლებელია აგებადია და მათ იქნებათ მრავალი ისეთი კარგი თვისება, რომლებიც არ გააჩნია ტიურინგის მანქანას. ამ თვისებათა შორის არ იქნება რეკურსიული ფუნქციის გამოთვლა, მაგრამ იქნება "კვანტური პარალელიზმის" თვისება – რომლის საშუალებითაც ალბათური ამოცანები ამოიხსნება გაცილებით სწრაფად, ვიდრე ეს კეთდებოდა კლასიკურ ანალოგზე. აღნიშნული თვისებების ინტუიციური ახსნა ზომაზე მეტად დამაბნეველია კვანტური თეორიის ყველა ინტერპრეტაციაში, გარდა ევერეტის ინტერპრეტაციისა. გამოკვლეულია გამოთვლების კვანტური თეორიის და დანარჩენი ფიზიკის ურთიერთთანახების ზოგიერთი ამოცანა. სირთულის კვანტური თეორია საშუალებას იძლევა გამოკვლეული იქნას "სირთულე" (complexity) და "ცოდნა" (knowledge) ფიზიკის თვალსაზრისით, რაც არ ხერხდება კლასიკური გამოთვლების შემთხვევაში.

1. გამომთვლელი მანქანები და ჩიორჩ-ტიურინგის პრინციპი

ბოლო რამდენიმე ათეული წლის განმავლობაში ინტენსიურად ვითარდებოდა გამომთვლელი მანქანების თეორია. ინტუიციურად გამომთვლელი მანქანა - ესაა ნებისმიერი ფიზიკური სისტემა, რომლის დინამიურ ევოლუციას იგი „შესავალ" მდგომარეობათა ერთი სიმრავლიდან გადაყავს „გამოსავალ" მდგომარეობათა მეორე სიმრავლეში. ეს მდგომარეობები მონიშნულია კანონიკური საზით. გარკვეული საზით მონიშნული შესავალი მდგომარეობებით ხდება მანქანის მომზადება და რაღაც მოძრაობის შემდეგ იზომება გამოსავალი მდგომარეობა. კლასიკური დეტერმინირებული სისტემისათვის გამოსავლის გაზომილი ნიშნული ესაა შესავლის ნიშნულით მოცემული გარკვეული f ფუნქციაა. უფრო მეტიც, პრინციპში შესაძლებელია ამ ნიშნულის მნიშვნელობა გაზომილი იქნას გარეშე დამკვირვებლის („მომხმარებლის") მიერ და ამ შემთხვევაში ამბობენ, რომ მანქანა „ითვლის" f ფუნქციას.

ორი კლასიკური დეტერმინირებული მანქანა „გამოთვლის თვალსაზრისით ექვივალენტურია" შესავალ და გამოსავალ მდგომარეობათა მოცემული ნიშნულების მიმართ, თუ ისინი ერთი და იგივე ფუნქციას ითვლიან ამ ნიშნულების მიმართ, მაგრამ კვანტური გამომთვლელი მანქანები და კლასიკური ალბათური გამომთვლელი მანქანები „არ ითვლიან" ფუნქციებს ზემოთხსენებული აზრით: ალბათური მანქანების გამოსავალი მდგომარეობა შემთხვევითია, ცნობილია მხოლოდ შესაძლო გამოსავლების განაწილების ფუნქცია, რომელიც შესავალ მდგომარეობებზეა დამოკიდებული. თუმცაღა კვანტური მანქანის გამოსავალი მდგომარეობა სრულად განისაზღვრება შესავალი მდგომარეობით, იგი დაკვირვებადი არაა და ე.ი. მომხმარებელს არ შეუძლია მისი ნიშნულის განსაზღვრა. ამის მიუხედავად, გამოთვლის

თვალსაზრისით ექვივალენტობის ცნება შეიძლება ისეთნაირად განზოგადდეს, რომ ასეთი მანქანებისათვის გამოდგეს.

ჩვენ კვლავ განვსაზღვრავთ მოცემული ნიშნულების მიმართ გამოთვლების ექვივალენტობას, მხოლოდ ამჯერად აუცილებელია უფრო ზუსტად აღვწეროთ - რა უნდა იქნას მონიშნული. რამდენადაც საუბარია შესავალზე, ნიშნულები მოცემული უნდა იქნან მანქანის საწყისი მომზადების ყველა შესაძლო ხერხით, რომლებიც განმარტების თანახმად შეესაბამებიან ყველა შესაძლო შესავალ მდგომარეობებს. ეს კლასიკური დეტერმინირებული შემთხვევის იდენტურია, რადგანაც არის ერთგვარი ასიმეტრია შესავალსა და გამოსავალს შორის: იმ დროს, როცა კვანტური სისტემა ნებისმიერ სასურველ შესავალ მდგომარეობაში შეიძლება იქნას მომზადებული, ზოგად შემთხვევაში გაზომვას არ შეუძლია განსაზღვროს მისი გამოსავალი მდგომარეობა: ამის ნაცვლად, უნდა გაიზომოს ზოგიერთ გაზომვად სიდიდეთა მნიშვნელობები (ამ სტატიაში ჩვენ გამოვიყენებთ შრედინგერის სურათს, რომელშიც კვანტური მდგომარეობა დროის ფუნქციაა, მაგრამ დაკვირვებადი სიდიდეები–მუდმივი ოპერატორებია). ამრიგად, ის რაც შეიძლება მონიშნული იქნას–ესაა დალაგებული წყვილების სიმრავლე, რომელიც შედგება გამოსავალი დაკვირვებადი სიდიდეებისაგან (კვანტურ თეორიაში - ერმიტული ოპერატორი თავისი ერთ-ერთ საკუთრივი მნიშვნელობით). ასეთი მოწესრიგებული წყვილი ფაქტიურად შეიცავს შესაძლო ექსპერიმენტის სპეციფიკაციას, რომელიც შეიძლება ჩატარდეს გამოსავალზე ექსპერიმენტის შესაძლო რეზულტატთან ერთად.

ორი გამომთვლელი მანქანა ექვივალენტურია გამოთვლის თვალსაზრისით, თუ ნებისმიერ ექსპერიმენტში ან შესაძლო ექსპერიმენტთა მიმდევრობაში, რომელშიც ამ მანქანების შესასვლელები ექვივალენტურადაა მომზადებული შესასვლელების ნიშნულთა მიმართ და დაკვირვებადი შესაბამისი სიდიდეები გაზომილია გამოსავლის ნიშნულთა მიმართ, ამ დაკვირვებადი სიდიდეების გაზომვადი მნიშვნელობები ორი მანქანისათვის სტატისტიკურად განუსხვავებელია. ე.ი. ორი მანქანის გამოსავალი ალბათობის განაწილების ფუნქცია იდენტურია.

ზემოთ აღწერილი M მანქანა ითვლის არა უმეტეს ერთ ფუნქციას. მიუხედავად ამისა, არ უნდა იყოს არსებითი განსხვავება M მოწყობილობის სისტემატიურ ცვლილებასა და იმ შესავალი მდგომარეობის ცვლილებას შორის, რომელშიც ხდება M-ის მომზადება. იგი იქცევა სხვა M' მანქანად, რომელიც ითვლის სხვა ფუნქციას. იმისათვის, რომ მოხდეს ასეთი ოპერაციების ფორმალიზება, ხშირად სასარგებლოა განვიხილოთ მანქანები ორი შესასვლელით, რომელთაგან ერთ-ერთის მომზადება შეადგენს ,,პროგრამას'', რომელიც იმას განსაზღვრავს, თუ მეორე შესავალის რა ფუნქცია უნდა იქნას

გამოთვლილი. ყოველ ასეთ $\mathcal{M}$-მანქანას შეესაბამება „გამოთვლადი ფუნქციების“ $C(\mathcal{M})$ სიმრავლე. f ფუნქცია $\mathcal{M}$ გამოთვლადია, თუ $\mathcal{M}$-ს შეუძლია f-ის გამოთვლა, როდესაც მომზადებულია რაიმე პროგრამა.

$C(\mathcal{M})$ სიმრავლის გაფართოება შესაძლებელია $\mathcal{M}$ მოწყობილობაში გაზომვადი სიმრავლის გაზრდით. იგულისხმება ის სიმრავლე, რომელიც მონიშნულია როგორც შესაძლო $\mathcal{M}$-პროგრამები. მოცემული ორი $\mathcal{M}$ და $\mathcal{M}'$ მანქანით შეიძლება აიგოს შედგენილი მანქანა, რომლის გამოთვლადი ფუნქციების სიმრავლე შეიცავს $C(\mathcal{M})$ და $C(\mathcal{M}')$-ის გაერთიანებას.

არ არსებობს წმინდა ლოგიკური მიზეზი, რომელიც თავიდან აგვაცილებდა სულ უფრო და უფრო მძლავრი გამომთვლელი მანქანის აგებას. მიუხედავად ამისა, იარსებებს ფუნქცია, რომელიც მდებარეობს ნებისმიერი შესაძლო ფიზიკური მანქანის გამოთვლადი სიმრავლის ზღვარს გარეთ. თუმცა ლოგიკა არ კრძალავს ნებისმიერი ფუნქციის ფიზიკურ გამოთვლას, მაგრამ როგორც ჩანს ასეთ აკრძალვას ადებს ფიზიკა. როგორც კარგად ცნობილია, გამომთვლელი მანქანის შემქმნელი სწრაფად აღწევს იმ წერტილს, როდესაც ახალი აღჭურვილობის დამატება არ ცვლის მანქანის მიერ გამოთვლილ ფუნქციათა სიმრავლეს (მეხსიერების შეზღუდვის იდეალიზაციის შემთხვევაში); უფრო მეტიც, მთელი რიცხვების $\mathbb{Z}$ სიმრავლის თავისთავში ასახვების $C(\mathcal{M})$ სიმრავლე ყოველთვის შედის $C(\mathcal{T})$-ში, სადაც $\mathcal{T}$-ტიურინგის უნივერსალური გამომთვლელი მანქანაა (ტიურინგი 1936), თვითონ $C(\mathcal{T})$ ცნობილია როგორც ნაწილობრივ რეკურსიული ფუნქციების სიმრავლე, ე.ი. - თვლადია და ამდენად გაცილებით მცირეა, ვიდრე ყველა ფუნქციათა სიმრავლე $\mathbb{Z}$-დან $\mathbb{Z}$-ში.

ჩიორჩმა (1936)[11] და ტიურინგმა (1936)[21] ივარაუდეს, რომ შეზღუდვა იმაზე, რაც შეიძლება გამოითვალოს, არაა დამოკიდებული არც გამომთვლელი მანქანების კონსტრუირების საქმეში არსებულ ვითარებაზე და არც ჩვენს უნარზე გამოთვლითი მოდელების შექმნაში - არამედ უნივერსალურია. ამას ეწოდება ჩიორჩ-ტიურინგის ჰიპოთეზა ტიურინგის მიხედვით:

”ბუნებრივად” გამოთვლადი ნებისმიერი ფუნქცია შეიძლება გამოთვლილი იქნას უნივერსალური მანქანის მიერ. (1.1)

(1.1)-სადმი ჩვეულებრივი არაფიზიკური მიდგომა ამას განიხილავს როგორც კვაზიმათემატიკურ ვარაუდს იმაზე, რომ ინტუიციური მათემატიკური ცნებების „ალგორითმისა“ და „გამოთვლების“ ყველა შესაძლო ინტუიციური ფორმალიზაცია ერთმანეთის ექვივილენტურია, მაგრამ ვნახავთ, რომ ეს შეიძლება აგრეთვე განხილული იქნას როგორც ახალი ფიზიკური პრინციპი,

რომელსაც ვუწოდებთ ჩიორჩ-ტიურინგის პრინციპს, იმისათვის, რომ გავარჩიოთ იგი (1.1)-ს სხვა ფორმულირებიდან ან მისგან გამომდინარე შედეგებიდან.

(1.1) ჰიპოთეზა ან სხვა ფორმულირებები, რომელიც არსებობს ლიტერატურაში [16] ძალზე ბუნდოვანია ისეთ ფიზიკურ პრინციპებთან შედარებით, როგორიცაა, მაგალითად, თერმოდინამიკის კანონი ან გრავიტაციული ექვივალენტურობის პრინციპი. მაგრამ ქვემოთ დავინახავთ, რომ ჩიორჩ-ტიურინგის (1.2) პრინციპის ჩვენს მიერ შემოთავაზებული მტკიცება არსებითად ფიზიკურია და ცალსახა. ვაჩვენებთ, რომ მას ისეთივე ეპისტომოლოგიური სტატუსი აქვს, როგორც სხვა ფიზიკურ პრინციპებს.

გთავაზობთ ახლებურ ინტერპრეტაციას ტიურინგის ცნებისა –„ბუნებრივად გამოთვლადი ფუნქციები“–როგორც ფუნქციებისა, რომლებიც პრინციპში შესაძლოა გამოთვლილი იქნან რეალური ფიზიკური სისტემის მიერ. მართლაც, ძნელია განიხილო ფუნქცია ბუნებრივად გამოთვლადად, თუ იგი გამოთვლადი არაა ბუნების მიერ და პირიქით. ჩვენ აქ განვსაზღვრავთ სრული მოდელირების ცნებას:

გამომთვლელ M მანქანას შეუძლია S ფიზიკური სისტემის სრული მოდელირება მისი შესავლისა და გამოსავალის მოცემული ნიშნულების მიმართ, თუ M-თვის არსებობს პროგრამა $\pi(S)$, რომელიც M-ს აქცევს გამოთვლის თვალსაზრისით S-ის ექვივალენტურად ამ ნიშნულების მიმართ. სხვა სიტყვებით, $\pi(S)$ პროგრამა M-ს გადააქცევს „შავ ყუთად“, რომელიც ფუნქციონალურად არ განირჩევა S სისტემისაგან.

ახლა ჩვენ შეგვიძლია ჩიორჩ-ტიურინგის პრინციპის ფიზიკური ვერსიის ფორმულირება:

ყოველი სასრული რეალიზებადი ფიზიკური სისტემა შესაძლოა სრულად იქნას მოდელირებული სასრული საშუალებების მქონე უნივერსალური მამოდელირებელი გამომთვლელი მანქანის მიერ. (1.2)

ეს უკეთესი ფორმულირებაა და უფრო მეტი ფიზიკური აზრიც აქვს, ვიდრე საკუთვრივ ტიურინგის მიერ ფორმულირებულ (1.1) პრინციპს, რადგანაც იგი ემყარება მხოლოდ ფიზიკურ ცნებებს, ისეთებს როგორიცაა „გაზომვა“ და „ფიზიკური სისტემა“, რომლებიც არსებობენ გაზომვების თეორიაში. ის არ შეიცავს ისეთ ტერმინს, როგორიცაა, „ბუნებრივია“, რომელიც არ დევს ფიზიკის არსებულ სტრუქტურაში.

ცნება „სასრულრეალიზებადი ფიზიკური სისტემები“– რომელზეც ლაპარაკია (1.2)-ში უნდა მოიცავდეს ნებისმიერ ფიზიკურ ობიექტს, რომელზეც შეიძლება ჩატარდეს ექსპერიმენტი. მეორეს მხრივ, „უნივერსალური გამომთვლელი მანქანა“ უნდა იყოს მხოლოდ იდეალიზირებული (მხოლოდ

თეორიულად ამოხსნილი) სასრული განსაზღვრადი მოდელით. ნიშნულები, რომლებზეც არაცხადი მითითებაა (1.2)-ში, აგრეთვე სასრული სიდიდეები უნდა იყვნენ.

(1.1)-ში განსაკუთრებულ უნივერსალურ მანქანაზე (ტიურინგის) მითითება აუცილებლობის გამო (1.2)-ში შეცვლილია უფრო ზოგადი მოთხოვნით, რომლის თანახმადაც ეს მანქანა მოქმედებს „სასრული საშუალებებით“. „სასრული საშუალებების“ ცნება შესაძლოა აქსიომატურად ჩამოყალიბდეს ფიზიკური კანონების შესახებ შემზღუდავი დაშვების გარეშე (შეადარეთ განდი (1980), [15]). რამდენადაც ჩვენ შეგვიძლია წარმოვიდგინოთ, რომ გამომთვლელი მანქანა მოქმედებს მიმდევრობითი ბიჯებით, რომელთა ხანგრძლივობას არანულოვანი ქვედა ზღვარი გააჩნია, ამდენად ის მოქმედებს "სასრული საშუალებებით", თუ *(i)* მხოლოდ სასრული ქვესისტემა (თუმცა არა ყოველთვის ერთ და იგივე) იმყოფება მოძრაობაში ერთი ბიჯის განმავლობაში, *(ii)* მოძრაობა დამოკიდებულია სასრული ქვესისტემის მდგომარეობაზე და *(iii)* წესი, რომელიც განსაზღვრავს ამ მოძრაობას, შეიძლება მოცემული იქნას სასრული რიცხვით (მაგ. მთელი რიცხვით). ტიურინგის მანქანები აკმაყოფილებენ ამ პირობებს. მათ გარდა ამ პირობას აკმაყოფილებენ უნივერსალური კვანტური კომპიუტერებიც (იხ. პარაგრაფი 2).

ჩიორჩ-ტიურინგის (1.2) პრინციპი უფრო ძლიერია, ვიდრე ის რაც გამომდინარეობს (1.1)-დან. სინამდვილეში ის იმდენად ძლიერია, რომ კლასიკურ ფიზიკაში ტიურინგის მანქანა ვერ აკმაყოფილებს მას. კლასიკური დინამიკის უწყვეტობის გამო კლასიკური სისტემის შესაძლო მდგომარეობები აუცილებლად შეადგენენ კონტინუუმს, მაშინ, როდესაც არსებობს შესავლის მომზადების მხოლოდ სასრული გზები, ე.ი. არ არსებობს T-ს შესავლის მომზადების ხერხების თვლადი სიმრავლე. აქედან გამომდინარე T-ს არ შეუძლია ნებისმიერი კლასიკური დინამიური სისტემის სრულად მოდელირება (ჩვენი აზრით, კარგად შესწავლილი უწყვეტი სისტემების „მოდელირების“ თეორია T-ს მეშვეობით განიხილავს არა სრულ მოდელირებას, არამედ მიმდევრობით დისკრეტულ აპროქსიმაციას). მე-3 პარაგრაფში ვაჩვენებთ, რომ ბუნებაში არსებულ ურთიერთქმედებებზე ჩვენს თანამედროვე ცოდნას ეთანხმება ის, რომ თითოეული რეალური (დისიპაციური) სასრული სისტემა შესაძლოა სრულად მოდელირებული იქნას უნივერსალური Q კვანტური კომპიუტერით. ამრიგად, კვანტური თეორია თავსებადია ჩიორჩ-ტიურინგის პრინციპის (1.2) ძლიერ ფორმასთან.

ახლა გადავდივართ არგუმენტების მოყვანაზე იმის სასარგებლოდ, რომ (1.2) ემპირიული დებულებაა. თეორიის ემპირიული სტატუსის ჩვეულებრივი კრიტერიუმი – ეს არის მისი ექსპერიმენტული ფალსიფიკაციის კრიტერიუმი (პოპერი 1959, [19]). ე.ი. შესაძლოა არსებობდნენ პოტენციური დაკვირვებები,

რომლებიც შეიძლება მას ეწინააღმდეგებოდნენ. მაგრამ რამდენადაც უფრო ღრმა თეორიებს „პრინციპებს“ ვუწოდებთ, ამდენად ვლაპარაკობთ მხოლოდ ცდებზე სხვა თეორიების გავლით. ფალსიფიკაციის კრიტერიუმები თითოეულ შემთხვევაში გამოყენებული უნდა იქნას ირიბად. მაგალითად, ენერგიის შენახვის პრინციპი თავისთავად არ შეიძლება ეწინააღმდეგებოდეს რაიმე შესაბამის დაკვირვებას, რამდენადაც ის არ შეიცავს იმის განსაზღვრას, თუ როგორ გაიზომოს ენერგია.

თერმოდინამიკის მე-3 კანონს, რომელიც ასეა ფორმულირებული:

არავითარ სასრულ პროცესს არ შეუძლია 0-მდე შეამციროს სისტემის ენტროპია ან სასრულრეალიზებადი ფიზიკური სისტემის ტემპერატურა, (1.3)

რაღაც საერთო აქვს ჩიორჩ-ტიურინგის პრინციპის ძლიერ ფორმასთან, პირდაპირი სახით ისიც ასევე არ არის უარყოფილი: ტემპერატურის არანაირ გაზომვას სასრული სიზუსტით არ შეუძლია განასხვაოს აბსოლუტური ნული ნებისმიერად მცირე დადებითი ტემპერატურისაგან. ანალოგიურად, რამდენადაც უნივერსალური კომპიუტერისათვის განკუთვნილი შესაძლო პროგრამების რიცხვი უსასრულოა, ზოგადად რომ ვთქვათ, არავითარ ექსპერიმენტს არ ძალუძს დაადგინოს, რომ არც ერთ მათგანს არ შეუძლია მოახდინოს სისტემის მოდელირება ისე, რომ პრეტენზია ჰქონდეს იყოს (1.2)-ის კონტრმაგალითი.

მაგრამ ყოველივე ამას „პრინციპები“ არ გააქვს ემპირიულ მეცნიერებათა მოქმედების სფეროს ფარგლებს გარეთ, პირიქით, ისინი არსებით საფუძველს ქმნიან იმისათვის, რომ მათზე უშუალო დაყრდნობით შემოწმებული იქნას სხვა თეორიები. ეწინააღმდეგება თუ არა მოცემული ფიზიკური თეორია პრინციპებს, დგინდება წმინდა ლოგიკით. ამრიგად, თუ უშუალოდ შემოწმებული თეორია ეძებს გადამწყვეტ ტესტებს, მაგრამ ეწინააღმდეგება პრინციპს, მაშინ ეს პრინციპი უკუგდებული უნდა იქნას ირიბად მაინც. თუ ექსპერიმენტალურად შემოწმებული თეორიები აკმაყოფილებენ შემზღუდავ პრინციპებს, მაშინ ეს პრინციპები ითვლება შემოწმებულად და იქცევა ერთის მხრივ, ახალი თეორიების კონსტრუირებაში სახელმძღვანელოდ, ხოლო მეორეს მხრივ, არსებული თეორიების შინაარსის უფრო ღრმა გაგების საშუალებად.

ხშირად მტკიცდება, რომ ნებისმიერი „გონიერი“ ფიზიკური (მათემატიკურის საწინააღმდეგოდ) გამოთვლის მოდელი, უკიდურეს შემთხვევაში $\mathbb{Z}$-დან $\mathbb{Z}$-ში ფუნქციების დეტერმინისტული გამოთვლა, ტიურინგისეულის ექვივალენტურია, მაგრამ ეს ასე არაა: არ არსებობს არავითარი აპრიორული მიზეზი, რის გამოც ფიზიკურმა კანონებმა უნდა დაიცვან მათემატიკური პროცესების შეზღუდვები, რომელთაც ჩვენ „ალგორითმებს“ (ე.ი. ფუნქციები

$C(\mathcal{T})$-დან) ვუწოდებთ, თუმცა საჭიროდ არ ჩავთვალეთ წინამდებარე სტატიაში ეს გაგვეკეთებინა, მაგრამ არაფერია პარადოქსული ან წინააღმდეგობრივი ისეთი ფიზიკური სისტემების პოსტულირებაში, რომლებიც ფუნქციებს ითვლიან არა $C(\mathcal{T})$-დან. შეიძლება არსებობდეს ექსპერიმენტულად შემოწმებული თეორიები ასეთი ეფექტით: განვიხილოთ ნებისმიერი რეკურსიულად გადათვლადი არარეკურსიული სიმრავლე (ისეთი, როგორიცაა მოცემულ ტიურინგის მანქანაზე დასრულებადი ალგორითმების შემცველი პროგრამების რიცხვთა სიმრავლე). პრინციპში, ფიზიკურ თეორიას თავის შედეგთა შორის შეიძლება ჰქონდეს ის, რომ რაღაც ფიზიკურ მოწყობილობას, $\mathcal{F}$-ს, განსაზღვრულ დროში შეუძლია გამოთვალოს ეკუთვნის თუ არა ნებისმიერი მთელი რიცხვი ამ სიმრავლეს. ეს თეორია ექსპერიმენტალურად უარყოფილი იქნებოდა თუ ტიურინგისეული ტიპის უფრო მარტივი კომპიუტერი, იმისათვის დაპროგრამებული, რომ ჩამოთვალოს სიმრავლე, როდისმე არ შეუთანხმდებოდა $\mathcal{F}$-ს (რასაკვირველია თეორია სხვა რაიმესაც იწინასწარმეტყველებდა, სხვანაირად იგი არ იქნებოდა არატრივიალურად შემოწმებადი და მისი სტრუქტურა იქნებოდა ისეთი, რომ ეგზოტიკური წინასწარმეტყველებები $\mathcal{F}$-ზე შეუძლებელი იქნებოდა მიგვეღო სხვა ფიზიკური შინაარსიდან. ეს ყოველივე ლოგიკურად შესაძლებელია).

მეორეს მხრივ, *a priori* არ არის ცხადი, რომ ნებისმიერი ცნობილი რეკურსიული ფუნქციათაგანი ფიზიკურ სინამდვილეში გამოთვლადია. მიზეზი იმისა, თუ რატომ მიგვაჩნია შესაძლებლად, მაგალითად, კალკულატორის კონსტრუირება და ამასთანავე რატომ შეგვიძლია არითმეტიკული მოქმედებების შესრულება გონებაში, არ შეიძლება მოიძებნოს მათემატიკასა და ლოგიკაში. მიზეზი იმაში მდგომარეობს, რომ ფიზიკის კანონები აღმოჩდნენ ისეთები, რომ უშვებენ ფიზიკური მოდელების არსებობას ისეთი არითმეტიკული ოპერაციებისათვის, როგორიცაა შეკრება, გამოკლება და დამრგვალება. ეს რომ ასე არ იყოს, ეს ცნობილი ოპერაციები არაგამოთვლადი ფუნქციები იქნებოდნენ, ჩვენ შეგვეძლო გვცოდნოდა ამ ფუნქციების შესახებ და გამოგვეყენებინა ისინი მათემატიკურ მტკიცებებში (რომლებიც თავიდანვე წოდებულნი იქნებოდნენ "არაკონსტრუქციულად"), მაგრამ ვერ შევძლებდით მათ შესრულებას.

რაიმე ფიზიკური სისტემის დინამიკა დამოკიდებული რომ ყოფილიყო რაღაც ფუნქციაზე არა $C(\mathcal{T})$-დან, მაშინ ასეთი სისტემები, პრინციპში შესაძლოა გამოყენებული ყოფილიყო ამ ფუნქციის გამოსათვლელად. ჩეიტინმა (1977) [10] აჩვენა, რომ ტიურინგის აზრით არაგამოთვლადი ყველა „საინტერესო" ფუნქციის ჭეშმარიტი მნიშვნელობები, მოცემული ფორმალური სისტემის მიერ, შესაძლებელია ძალზე ეფექტურად იქნას ჩაწერილი ცხრილის სახით, როგორც ერთი ფიზიკური მუდმივის პირველი რამდენიმე ციფრი.

მაგრამ ეს რომ ასე ყოფილიყო, შეგვეძლო გაგვეპროტესტებინა, რამდენადაც ჩვენ ამის შესახებ ვერასოდეს გავიგებდით, რადგან ვერ

შევამოწმებდით იმ ცხრილის სიზუსტეს, რომელიც ბუნების მიერაა შემოთავაზებული. ესა შეცდომაა. იმის მიზეზი, რომ გვჯერა მანქანები, რომელსაც კალკურატორებს ვუწოდებთ, სინამდვილეში ითვლიან არითმეტიკულ ფუნქციებს, რომელთა გამოთვლაც მათ ევალებათ, იმაში კი არ მდგომარეობს, რომ მათი პასუხების შემოწმება შეგვიძლია (ორი მანქანის შედარება უკიდურესად უსარგებლო პროცესია), არამედ ნამდვილი მიზეზი იმაშია, რომ გვჯერა დეტალური ფიზიკური თეორიისა, რომელიც გამოყენებული იქნა მათი კონსტრუირებისას. Quis custodient custodias ipsos? (ვინ უდარაჯებს დარაჯებს?) ეს თეორია ემპირიულია იმ მტკიცების ჩათვლით, რომ არითმეტიკის აბსტრაქტული ფუნქციები რეალიზებულია ბუნებაში.

2.კვანტური კომპიუტერები

გამოთვლის ნებისმიერი არსებული ზოგადი მოდელი - ეფექტურად კლასიკურია. ე.ი. ყოველ მომენტში მისი მდგომარეობის სრული აღწერა გარკვეული რიცხვთა სიმრავლის განსაზღვრის ექვივალენტურია. ყველა ეს რიცხვები პრინციპში გაზომვადია. ამასთან, კვანტური თეორიის შესაბამისად, სისტემები ასეთი თვისებებით არ არსებობენ. ის ფაქტი, რომ კლასიკური ფიზიკა და ტიურინგის უნივერსალური კლასიკური მანქანა მკაცრ ფიზიკურ ფორმაში ვერ უზრუნველყოფენ ჩიორჩ-ტიურინგის (1.2) პრინციპს–არის ჭეშმარიტად კვანტური მოდელის ძიების ერთ-ერთი მოტივაცია. უფრო დაბეჯითებული მოტივაცია კი არის ის, რომ კლასიკური ფიზიკა მცდარია!

ბენოფმა (1982, [5]) კვანტური კინემატიკისა და დინამიკის ჩარჩოებში ააგო გამოთვლების მოდელი, მაგრამ კვლავ ეფექტურად კლასიკური ზემოთ ხსენებული აზრით. იგი ისეა აგებული, რომ არც ერთი კვანტური მახასიათებელი თვისებათაგანი–ინტერფერენცია, განუყოფლობა, განუზღვრელობა –არ ვლინდება გამოთვლების არც ერთ ნაბიჯზე. მისი გამოთვლა შეიძლება სრულად იქნას მოდელირებული ტიურინგის მანქანაზე.

ფეინმანი (1982,[14]) კიდევ ერთი ნაბიჯით მიუახლოვდა კვანტურ კომპიუტერს თავისი „უნივერსალური კვანტური სიმულატორით“. იგი შედგება სპინური სისტემის მესერისაგან, რომლებიც ურთიერთქმედებენ ახლო მეზობლებთან, თუმცაღა მას ნამდვილად შეუძლია მდგომარეობათა სასრული სივრცის მქონე ნებისმიერი სისტემის მოდელირება (ჩვენ არ გვესმის რატომ ეპარება ფეინმანს ეჭვი, რომ მას ფერმიონების სისტემის მოდელირება შეუძლია), იგი არ წარმოადგენს, ჩვენი აზრით, გამომთვლელ მანქანას. გამომთვლელი მანქანის იმიტატარორის „პროგრამირება“ ესაა მისი აწყობა სასურველი დინამიური კანონების შესაბამისად და შემდეგ მისი მიყვანა იმ საწყის მდგომარეობამდე, რომელიც მოითხოვება. მაგრამ მექანიზმი, რომელიც ნებისმიერი დინამიური კანონების ამორჩევის საშუალებას იძლევა, არ

მოდელირდება. ჩვენი აზრით ნამდვილი „კომპიუტერის“ დინამიკა ერთხელ და სამუდამოდ უნდა დაფიქსირდეს, ხოლო დაპროგრამება მთლიანად უნდა შედგებოდეს მისი სათანადო მდგომარეობის მომზადებაში (ან შერეული შემთხვევა).

ალბერტმა (1983, [1]) აღწერა კვანტურ-მექანიკური გამზომი „აპარატი“ და შენიშნა, რომ მის თვისებას, გაზომოს საკუთარი თავი, არ გააჩნია ანალოგი კლასიკურ ავტომატებს შორის. თუმცაღა ალბერტის ავტომატები არ არიან ზოგადი დანიშნულების გამომთვლელი მანქანები. ისინი კვანტური კომპიუტერებია, იმ ზოგადი კლასის წევრები, რომელთაც შევისწავლით ამ თავში.

ახლა ჩვენ აღვწერთ ზოგადად გამოთვლის სრულ კვანტურ მოდელს. შემდეგ კი—უნივერსალურ Q კვანტურ კომპიუტერს, რომელსაც შეუძლია ნებისმიერი სასრულრეალიზებადი სისტემის მოდელირება. მას შეუძლია (ნულოვანი ტემპერატურის მქონე) იდეალური ჩაკეტილი სისტემის მოდელირება, ასევე სხვადასხვა კვანტური კომპიუტერების და კვანტური იმიტატორების მოდელირება საკმაოდ დიდი სიზუსტით. $\mathbb{Z}$-დან $\mathbb{Z}$-ში კონკრეტული ფუნქციების გამოთვლისას ის ზუსტად ახდენს $C(T)$ კლასიკური რეკურსიული ფუნქციების გენერირებას (ექვივალენტურობის პრინციპის გამოვლინება). T-საგან განსხვავებით, მას შეუძლია დისკრეტული შემთხვევითი პროცესის ნებისმიერი სასრული კლასიკური თვისების მოდელირება. უფრო მეტიც, როგორც ჩვენ მესამე პარაგრაფში ვნახავთ, მას აქვს შესაძლებლობები, რომელთაც კლასიკური ანალოგი არ გააჩნიათ.

ისევე როგორც ტიურინგის მანქანა, კვანტური Q კომპიუტერის მოდელი ორი კომპონენტისაგან შედგება: სასრული პროცესორისა და უსასრულო მეხსიერებისაგან, რომლის სასრული ნაწილია გამოყენებული ყოველ მომენტში. გამოთვლა T ფიქსირებული ხანგრძლივობის ნაბიჯების შესრულებაში მდგომარეობს და თითოეული ნაბიჯზე ურთიერთქმედებენ მხოლოდ პროცესორი და მეხსიერების სასრული ნაწილი, დარჩენილი მეხსიერება სტატიკური რჩება.

პროცესორი შედგება 2-მდგომარეობიანი M რაოდენობის დაკვირვებადი სიდიდისაგან

$$\{\hat{n}_i\} \quad (i\epsilon\mathbb{Z}_M), \tag{2.1}$$

სადაც $\mathbb{Z}_M$ არის მთელი რიცხვი 0-დან M-1-მდე. მეხსიერება შედგება დაკვირვებადი 2-მდგომარეობიანი სიდიდეების უსასრულო მიმდევრობისაგან

$$\{\hat{m}_i\} \quad (i\epsilon\mathbb{Z}). \tag{2.2}$$

ტიურინგის მანქანაში ეს შეესაბამება უსასრულოდ გრძელ „ლენტას“. ჩვენ ვიხმართ მთლიანად $\{\hat{n}_i\}$-ის აღსანიშნავად $\hat{\boldsymbol{n}}$-ს, ხოლო $\{\hat{m}_i\}$-ის აღსანიშნავად კი - $\hat{\boldsymbol{m}}$-ს. ტიურინგის მანქანის ლენტის მდგომარეობას შეესაბამება $\hat{x}$ სიდიდე, რომელიც როგორც მდგომარეობათა სიმრავლე შეიცავს $\mathbb{Z}$-ის ყველა

ქვესიმრავლეს. დაკვირვებადი სიდიდე $\hat{x}$ „ამისამართებს“ ლენტის იმ ადგილის ნომერს, რომლის სკანირებაც ხდება მოცემულ მომენტში. რადგან „ლენტა“ უსასრულოდ გრძელია, მაგრამ გამოთვლების დროს მოძრაობაში იმყოფება, იგი არ უნდა იყოს მაგარი ანდა წინააღმდეგ შემთხვევაში არ შეიძლება იგი აიძულო იმოძრაოს „სასრული ხერხებით“. მოითხოვება, რომ მექანიზმი რომელიც ამოძრავებს ლენტას იმ სიგნალების შესაბამისად, რომლებიც გადაიცემიან სასრული სიჩქარით მხოლოდ მომიჯნავე სეგმენტებს შორის, უნდა აკმაყოფილებს „სასრული ხერხი“-ს მოთხოვნას და საკმარისია იმისათვის, რომ შეასრულოს ის, რაც შემდგომაა აღწერილი. დაკმაყოფილებული იმით, რომ ასეთი მექანიზმის არსებობა შესაძლებელია, ჩვენ არ გვჭირდება მისი ცხადი სახით მოდელირება. ამრიგად, Q-ს მდგომარეობა $\mathcal{H}$ სივრცის ერთეულოვანი ვექტორია, რომელიც მოჭიმულია $\hat{x}, \hat{\boldsymbol{n}}$ და $\hat{\boldsymbol{m}}$ ოპერატორების საკუთრივ ვექტორებზე, რომლებიც აღნიშნულია შესაბამისად $x, \boldsymbol{n}, \boldsymbol{m}$-ით:

$$|x; \boldsymbol{n}; \boldsymbol{m}> \equiv |x; n_0, n_1 \dots n_{M-1}; m_{-1}, m_0, m_1 \dots >. \qquad (2.3)$$

(2.3)-ს ჩვენ ვუწოდებთ „გამოთვლითი ბაზისის მდგომარეობებს“. მოხერხებულია, რომ ჩვენს მიერ დაკვირვებადი ორმდგომარეობიანი სიდიდეების სპექტრად ჩავთვალოთ $\mathbb{Z}_2$, ე.ი. *{0,1}* და არა *{-/2,+1/2}* როგორც ჩვეულებრივ იხმარება ფიზიკაში. *{0,1)* სპექტრის მქონე დაკვირვებადი სიდიდეების ბუნებრივი ინტერპრეტაციაა მეხსიერების ერთ ბიტიანი ელემენტი.

Q-ს დინამიკა ზოგადად აღიწერება $\mathcal{H}$-ზე მოქმედი მუდმივი U უნიტარული ოპერატორით. U ოპერატორი აღწერს ნებისმიერი $|\Psi(t)> \in \mathcal{H}$ მდგომარეობის ევოლუციას (შრიოდინგერის სურათში დროის t მომენტში) გამოთვლების პროცესში

$$|\Psi(t)> = U^n|\Psi(0)> \quad (n \in \mathbb{Z}^+), \qquad (2.4)$$

$$U^*U = UU^* = \hat{1}. \qquad (2.5)$$

ჩვენ არ გვჭირდება მდგომარეობათა განსაზღვრა დროის იმ მომენტებში, რომლებიც განსხვავდებიან T-ს არაუარყოფითი მთელი ჯერადებისაგან. გამოთვლები იწყება $t=0$-დან. ამ მომენტში $\hat{\boldsymbol{x}}$ და $\hat{\boldsymbol{n}}$ მომზადდებიან ნულოვანი მნიშვნელობით. $\hat{\boldsymbol{m}}$-ის ელემენტთა სასრული რიცხვის მდგომარეობა მომზადდება როგორც „პროგრამა“ და „შესასვლელი“ პარაგრაფი 1-ის აზრით, ხოლო დანარჩენ ელემენტებში მყარდება ნულოვანი მდგომარეობები. ამრიგად,

$$\left.\begin{aligned} |\Psi(0)> = \sum_m \lambda_m |0; \mathbf{0}; \boldsymbol{m}>, \\ \sum_m |\lambda_m|^2 = 1, \end{aligned}\right\} \qquad (2.6)$$

სადაც მხოლოდ სასრული რაოდენობის λ_m-ია არანულოვანი და λ_m-ები ხდებიან ნულოვანი როგორც კი $\boldsymbol{m}$ -ში უსასრულო რაოდენობა ელემენტებია არანულოვანი.

იმისათვის, რომ დაკმაყოფილდეს მოთხოვნა, Q მოქმედებს “სასრული სახით”, U მატრიცის ელემენტებს უნდა ჰქონდეთ შემდეგი სახე:

$$< x'; \boldsymbol{n}'; \boldsymbol{m}'|U|x; \boldsymbol{n}, \boldsymbol{m} >=$$
$$[\delta_{x'}^{x+1} U^{+}(\boldsymbol{n}', m'_x|\boldsymbol{n}, m_x) + \delta_{x'}^{x-1} U^{-}(\boldsymbol{n}', m'_x|\boldsymbol{n}, m_x)] \prod_{x \neq y} \delta_{m_y}^{m_y}, \quad (2.7)$$

მარჯვენა მხარეში უსასრულო ნამრავლი უზრუნველყოფს იმას, რომ მეხსიერების მხოლოდ ერთი x-ური ბიტი მონაწილეობს გამოთვლებში. $\delta_{x'}^{x\pm1}$ წევრები უზრუნველყოფენ იმას, რომ თითოეული ნაბიჯის განმავლობაში ლენტის x პოზიცია არ შეიძლება შეიცვალოს ერთ ერთეულზე მეტად: ერთი ერთეულით წინ, ან ერთი ერთეულით უკან, ან ორივე მხარეს თითო ერთეულით. ფუნქციები $U^{\pm}(\boldsymbol{n}', m'|\boldsymbol{n}, m)$, რომლებიც დინამიკას აღწერენ, დამოკიდებულნი არიან მხოლოდ ლოკალურ დაკვირვებად $\hat{\boldsymbol{n}}$ და $\hat{m}_x$ სიდიდეებზე და აკმაყოფილებენ მხოლოდ (2.5) ტოლობას. თითოეული მათგანი განსაზღვრავს ახალ კვანტურ *Q[U+, U-]* კომპიუტერს.

ამბობენ, რომ ტიურინგის მანქანა "ჩერდება" და იტყობინება გამოთვლების დამთავრებას, როდესაც ორი ერთმანეთის მომდევნო მდგომარეობა იდენტურია. "სწორი" ეწოდება პროგრამას, რომელიც იწვევს მანქანის გაჩერებას სასრული ბიჯების შემდეგ. ამის მიუხედავად (2.4) გვიჩვენებს, რომ Q კვანტური კომპიუტერის ორი მომდევნო მდგომარეობა არასოდეს არ შეიძლება ერთმანეთს ემთხვეოდეს არატრივიალური გამოთვლების შემდეგ (ეს სამართლიანია ნებისმიერი შებრუნებადი კომპიუტერისათვის).

უფრო მეტიც, Q არ შეიძლება დაიმზიროს მანამ, სანამ გამოთვლა არ დამთავრდება, რამდენადაც ეს, საზოგადოდ, შეცვლიდა მის მდგომარეობას. ამიტომ მოითხოვება, რომ კვანტური კომპიუტერები აქტიურად იძლეოდნენ შეტყობინებას იმის თაობაზე, რომ ჩერდებიან. ამ მიზნით არჩეული უნდა იქნას პროცესორის ერთი შიგა ბიტი, მაგალითად $\hat{n}_0$. თითოეული სწორი Q პროგრამა n_0-ს გადაიყვანს 1-ში, როდესაც პროგრამა ჩერდება და არ ურთიერთქმედებს $\hat{n}_0$-თან სხვა შემთხვევებში. მაშინ $\hat{n}_0$ პერიოდულად შეიძლება დაიმზიროს გარედან Q-ზე ზემოქმედების გარეშე. პროგრამის სისწორის კლასიკური პირობის ანალოგი შეიძლება იმაში მდგომარეობდეს, რომ $\hat{n}_0$ სიდიდის მათემატიკური ლოდინი უნდა გადავიდეს 1-ში სასრულ დროში. ამის მიუხედავად შეგვიძლია განვიხილოთ ფიზიკის თვალსაზრისით Q-პროგრამების უფრო ფართო კლასი. Q- პროგრამა სწორია, თუ მისი მუშაობის დროის მათემატიკური ლოდინი სასრულია.

უნიტარულობის გამო Q-ს დინამიკა, ისევე როგორც ნებისმიერი კვანტური სისტემის დინამიკა, აუცილებლად შექცევადია. მეორეს მხრივ, ტიურინგის მანქანები გამოთვლების დროს ახდენენ შეუბრუნებად ცვლილებებს და არცთუ ისე დიდი ხნის წინ გავრცელებული იყო აზრი, რომლის თანახმადაც შეუბრუნებლობა – გამოთვლების არსებითი თვისებაა. ამის მიუხედავად, ბენეტმა (1973,[6]) დაამტკიცა, რომ ეს ასე არაა, ცხადი სახით ააგო რა გამომთვლელი

მანქანის შექცევადი კლასიკური მოდელი, ექვივალენტური (ე.ი. იგივე გამოთვლადი ფუნქციების გამომთვლელი, რისაც არის T) T-სი (იხ. აგრეთვე ტოფოლი (1979,[20]) (ბენიოფის მანქანები ბენეტის მანქანების ექვივალენტურია, მაგრამ იყენებენ კვანტურ დინამიკას).

კვანტური კომპიუტერები $Q[U^+, U]$, რომლებიც ექვივალენტურნი არიან ნებისმიერი შექცევადი ტიურინგის მანქანისა, შეიძლება მივიღოთ შემდეგი ტოლობით:

$$U^{\pm}(\boldsymbol{n}', m'|\boldsymbol{n}, m) = \delta_{n'}^{A(n,m)}\delta_{m'}^{B(n,m)}[1 \pm C(\boldsymbol{n}, m)], \qquad (2.8)$$

სადაც A, B, C – ფუნქციებია მნიშვნელობებით $(\mathbb{Z}_2)^M$, $\mathbb{Z}_2$ და {-1,1}-ში შესაბამისად. სხვა სიტყვებით, ტიურინგის მანქანები ისეთი კვანტური კომპიუტერებია, რომელთა დინამიკა უზრუნველყოფს იმას, რომ თუ მათ დაიწყეს ქმედება ძირითადი მდგომარეობიდან, ისინი რჩებიან ძირითად მდგომარეობაში ყოველი ბიჯის შემდეგ. უნიტარულობის უზრუნველსაყოფად აუცილებელი და საკმარისია, რომ ასახვა

$$\{(\boldsymbol{n}, m)\} \leftrightarrow \{(A(\boldsymbol{n}, m), B(\boldsymbol{n}, m), C(\boldsymbol{n}, m))\} \qquad (2.9)$$

იყოს ბიექციური. რამდენადაც A, B, C ფუნქციები ნებისმიერია, კერძო შემთხვევაში უნდა არსებობდეს ვარიანტები, რომლებიც Q-ს გახდიან ტიურინგის T უნივერსალური მანქანის ექვივალენტურს.

უნივერსალური Q კვანტური კომპიუტერის აღწერა უშუალოდ მისი შემადგენელი $U^{\pm}$ გარდაქმნების ტერმინებში შესაძლებელია, მაგრამ გაუმართლებლად დამძანცავია. Q-ს თვისებები უმჯობესია განისაზღვროს უფრო მაღალ დონეზე აღწერით, ცხადი სახით $U^{\pm}$-ს აგებას სავარჯიშოდ ვუტოვებთ მკითხველს. შემდგომში ჩვენ რამდენჯერმე ვიხმარ T-ს "უნივერსალურობის" თვისებას.

ნებისმიერი f რეკურსიული ფუნქციისათვის არსებობს T -ს ისეთი $\pi(f)$ პროგრამა, რომ თუ $\pi(f)$ ანასახს მოსდევს ნებისმიერი მთელი i რიცხვების ანასახი T-ს შესავალზე, ამასთან i არის გამოსავალზე, რომელსაც მოსდევს $f(i)$ ანასახი, ხოლო ყველა დანარჩენი ბიტი 0-ებია, მაშინ T ჩერდება სწორედ $\pi(f)$-ზე. ე.ი. რომელიმე n დადებითი მთელი რიცხვისათვის გვაქვს:

$$U^n|0; \mathbf{0}, \pi(f), i, \mathbf{0} >= |0; 1; \mathbf{0}; \pi(f), i, f(i), \mathbf{0} >. \qquad (2.10)$$

აქ $\mathbf{0}$ აღნიშნავს ნულების მიმდევრობას, ხოლო $\widehat{m}_i(i<0)$-ს ნულოვანი საკუთრივი მნიშვნელობები ცხადი სახით არაა ნაჩვენები. T-ს ზოგადობა არ იზღუდება, თუ პროგრამას მოვთხოვთ, რომ მან გაანაწილოს მეხსიერება, როგორც ნებისმიერი მთელი რიცხვის შემცველი უსასრულო უჯრედების მიმდევრობა. (მაგალითად, a-ური უჯრედი შეიძლება შედგებოდეს ბიტებისაგან, რომელთა ნიშნულებია a მარტივი რიცხვის ხარისხები). თითოეული რეკურსიული f ფუნქციისა და a და b მთელი რიცხვებისათვის არსებობს პროგრამა $\pi(f,a,b)$, რომელიც ითვლის f

ფუნქციისა და a უჯრედის შემცველ რიცხვებს და რეზულტატს განათავსებს b უჯრედში, ისე, რომ a-ს ტოვებს უცვლელად. თუ b უჯრედი თავდაპირველად არ შეიცავდა 0-ს, მაშინ შეუქცევადობა მოითხოვს, რომ მისი ძველი მნიშვნელობის დავიწყება კი არ მოხდეს, არამედ კომბინირებული იქნას რაიმე შექცევადი ხერხით, ფუნქციის მნიშვნელობასთან. ამრიგად, ვტოვებთ რა ზედმეტი წვრილმანების მოხსენიებას, π პროგრამის მოქმედება შეიძლება გამოვსახოთ დიაგრამის

$$|\overbrace{\pi(f,2,3)}^{slot\ 1},\ \overbrace{i}^{slot\ 2},\ \overbrace{j}^{slot\ 3}> \rightarrow |\pi(f,2,3),i,j\oplus f(i)> \tag{2.11}$$

სახით, სადაც $\oplus$ ნებისმიერი ასოციაციური, კომუტაციური ოპერაციაა თვისებებით:

$$\left.\begin{aligned} i\oplus i &= 0,\\ i\oplus 0 &= i,\end{aligned}\right\} \tag{2.12}$$

(გამოდგება, მაგალითად, "გამომრიცხავი ან"). $\pi_1\pi_2$-ით ჩვენ აღვნიშნავთ ორი პროგრამის π_1-ის და π_2-ის გადაბმას; რომელიც ყოველთვის არსებობს, თუ π_1 და π_2 სწორი (გამართული) პროგრამებია; $\pi_1\ \pi_2$ არის პროგრამა, რომელიც იწყება π_1-ს მოქმედებათ, მას კი მოსდევს π_2-ის მოქმედება.

ნებისმიერი ბიექციური g ფუნქციისათვის არსებობს პროგრამა $\Phi(g,a)$, რომლის ერთადერთი მოქმედება a უჯრედზე ესაა ნებისმიერი i მთელი რიცხვის შეცვლა $g(i)$-თი. ამის დამტკიცება ძნელი არაა, რადგან თუ რაიმე უჯრედი თავიდან შეიცავს ნულს, მაშინ

$$\Phi(g,a) = \pi(g,b,a)\ \pi(g^{-1},b,a)\ \pi(I,b,a)\ \pi(I,a,b); \tag{2.13}$$

აქ I სრული გაზომვის ფუნქციაა (დოიჩი 1985, [12]):

$$|\pi(I,2,3),i,j> \rightarrow |\pi(I,2,3),i,j\oplus i>. \tag{2.14}$$

Q უნივერსალურ კომპიუტერს გააჩნია T-ს ყველა ახლახან აღწერილი თვისება, როგორც ნაჩვენებია (2.10) და (2.14) გამოსახულებებით, მაგრამ Q-სათვის დასაშვებია აგრეთვე პროგრამების კლასი, რომლებიც საბაზისო მდგომარობებს გარდაქმნიან მათ წრფივ სუპერპოზიციაში.

ყველა პროგრამები Q-თვის შეიძლება გამოისახოს ჩვეულებრივი ტიურინგისეული ოპერაციების ტერმინებში და ზუსტად 8 დამატებითი ოპერაციით. ესაა უნიტარული გარდაქმნები, რომლებიც მოქმედებენ ორგანზომილებიან ჰილბერტის H სივრცეზე, როგორც ერთი ბიტის მდგომარეობათა სივრცეზე. ეს გარდაქმნები ქმნიან ოჯახს ოთხი (ნამდვილი) პარამეტრით. დავუშვათ α არის π-ს ნებისმიერი ირაციონალური ჯერადი, მაშინ ოთხი გარდაქმნა

$$V_0 = \begin{pmatrix} cos\alpha & sin\alpha \\ -sin\alpha & cos\alpha \end{pmatrix}, \quad V_1 = \begin{pmatrix} cos\alpha & isin\alpha \\ isin\alpha & cos\alpha \end{pmatrix}, \\ V_2 = \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & 1 \end{pmatrix}, \qquad V_3 = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}, \Bigg\} \tag{2.15}$$

და მათი შებრუნებულები V_4, V_5, V_6, V_7 წარმოქმნიან კომპოზიციის მიმართ ჯგუფს, რომელიც არის მკვრივი $\mathcal{H}$-ის ყველა უნიტარულ გარდაქმნათა ჯგუფში. მოხერხებულია, მაგრამ არა არსებითი, დავუმატოთ კიდევ ორი წარმომქნელი:

$$V_8 = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \text{ და } V_9 = \frac{1}{2}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}, \tag{2.16}$$

რომლებიც შეესაბამებიან "სპინის მობრუნებას" 90^0-ით. თითოეულ V_i-ურ წარმომქმნელს შეესაბამება გამოთვლითი ბაზისის ელემენტი, რომელიც თავის მხრივ $\Phi(V_i,a)$ პროგრამას წარმოადგენს, იგი ასრულებს V_i ოპერატორს a უჯრედის უმცირეს ნიშნად ბიტზე. ამრიგად, თუ j არის 0 ან 1, ეს საბაზისო ელემენტები მოქმედებენ შემდეგი ფორმულის შესაბამისად:

$$|\phi(V_i,2), j> \rightarrow \sum_{k=0}^{1} < k|V_i|j > \phi(V_i,2), k>. \tag{2.17}$$

V_i კომპოზიცია შეიძლება განხორციელებული იქნას $\Phi(V_i,a)$ გადაბმის საშუალებით. ამრიგად, არსებობს პროგრამები, რომლებიც მოქმედებენ ნებისმიერი ერთი ბიტის მდგომარეობაზე სასურველთან რაგინდ ახლო უნიტარული გარდაქმნით.

ანალოგიური დასკვნა სამართლიანია მოცემული სასრული L რაოდენობის ბიტების ერთობლივი მდგომარეობისათვის. ეს არაა ტრივიალური დაკვირვება, რადგან არაა აუცილებელი, რომ ასეთი მდგომარეობა იყოს ცალკეული ბიტების მდგომარეობების პირდაპირი ნამრავლი, არამედ, ზოგადად, ასეთი ნამრავლების წრფივი სუპერპოზიციაა. ამის მიუხედავად ახლა მოვიყვანთ ისეთი პროგრამის არსებობის მონახაზს, რომელიც იწვევს L ბიტის უნიტარულ გარდაქმნას, რაგინდ ახლოს მდგომს სასურველ უნიტარულ გარდაქმნასთან. შემდგომში "ზუსტი" აღნიშნავს "რაგინდ ახლოს შიგა ნამრავლის ნორმის მიმართ". შემთხვევა, როდესაც $L=1$, ტრივიალურია. დავამტკიცოთ დებულება L ბიტისათვის ინდუქციის მეთოდით.

გამოთვლითი ბაზისის 2^L მდგომარეობის ყველა შესაძლო $(2^L)!$ გადანაცვლება შებრუნებადი რეკურსიული ფუნქციაა და განსაზღვრავს $\mathcal{T}$-ს და აქედან გამომდინარე Q-პროგრამას.

ახლა ვაჩვენოთ, რომ Q-ს შეუძლია წარმოქმნას 2^L განზომილებიანი უნიტარული გარდაქმნები, რომლებიც დიაგონალურებია გამოთვლით ბაზისში და რაგინდ ახლოს მდებარეობენ ნებისმიერ დიაგონალურ გარდაქმნასთან ამ ბაზისში. ინდუქციის დაშვების თანახმად, $(L-1)$ ბიტიანი დიაგონალური გარდაქმნები ზუსტად Q-გამოთვლადია და წარმოიქმნებიან გარკვეული 2^L ზომის დიაგონალური უნიტარული მატრიცებით, რომელთა საკუთრივი მნიშვნელობები

ლუწი რიგით გადაგვარებულებია. საბაზისო მდგომარეობის გადანაცვლებები Q-ს საშუალებას აძლევს ზუსტად გამოიძახოს ნებისმიერი დიაგონალური უნიტარული გარდაქმნა. გადაგვარებული გარდაქმნების სიმრავლის ჩაკეტვა გამრავლების მიმართ–დიაგონალური გარდაქმნების ჯგუფია, რომელიც ყველგან მკვრივია 2^L ზომის დიაგონალური უნიტარული გარდაქმნების ჯგუფში.

შემდგომში ჩვენ ვაჩვენებთ, რომ თითოეული $|\psi>$ L ბიტიანი მდგომარეობისთვის არსებობს Q-პროგრამა $\rho(|\psi>)$, რომელსაც $|\psi>$ ზუსტად გადაყავს $|0_L>$ საბაზისო მდგომარეობაში. ამრიგად,

$$|\psi>= c_0|0>|\psi_0> +c_1|1>|\psi_1>, \qquad (2.18)$$

სადაც $|\psi_0>$ და $|\psi_1>$ არიან *L-1*-ბიტიანი მდგომარეობები. ინდუქციის დაშვებით არსებობს Q პროგრამები ρ_0 და ρ_i, რომლებსაც გადაჰყავთ $|\psi_0>$ და $|\psi_1>$ მდგომარეობები $|0_{L-1}>$-ში. ამიტომ არსებობს შემდეგი Q-პროგრამა: თუ ბიტი ნომერით 1 არის ნული, შესრულდეს ρ_0, წინააღმდეგ შემთხვევაში ρ_1. ის (2.18)-ს გარდაქმნის შემდეგნაირად:

$$(c_0|0>+c_1|1>)|0_{L-1}>. \qquad (2.19)$$

შემდეგ (2.19) შესაძლებელია გადაყვანილი იქნას $|0_L>$-ში ნომერი 1 ბიტის გარდაქმნით.

საბოლოოდ, ნებისმიერი 2^L ზომის U გარდაქმნა ზუსტად მიიღება U მატრიცის თითოეული $|\psi>$ საკუთრივი ვექტორის მიმდევრობითი გადაყვანით $|0_L>$-ში ($\rho^{-1}(|\psi>)$ პროგრამის შესრულებით), შემდეგ ხორციელდება დიაგონალური უნიტარული გარდაქმნები, რომლებიც $|0_L>$-ს ამრავლებენ $|\psi>$-ს შესაბამის საკუთრივ მნიშვნელობაზე (ფაზური მამრავლი), მაგრამ, ადგილი აქვს რაგინდ მცირე მოქმედებას გამოთვლითი ბაზისის ნებისმიერ სხვა მდგომარეობაზე და შემდგომ სრულდება $\rho(|\psi>)$ პროგრამა.

ამით მტკიცდება, რომ Q უნივერსალური კვანტური კომპიუტერია. მას შეუძლია ნებისმიერი სიზუსტით მოახდინოს ნებისმიერი სხვა $Q[U^+,U]$ კვანტური კომპიუტერის მოდელირება. ეს ასეა, რამდენადაც, მიუხედავად იმისა, რომ კვანტურ კომპიუტერს გააჩნია მდგომარეობათა უსასრულო სიმრავლე, მისი ევოლუციის მოდელირებისათვის, თითოეულ ნაბიჯზე საჭიროა მხოლოდ სასრულგანზომილებიანი უნიტარული გარდაქმნები.

3. უნივერსალური კვანტური კომპიუტერის თვისება

ჩვენ უკვე ვნახეთ, რომ უნივერსალურ Q კვანტურ კომპიუტერს შეუძლია მოახდინოს ტიურინგის ნებისმიერი მანქანის მოდელირება და ნებისმიერი სიზუსტით შეუძლია ნებისმიერი კვანტური კომპიუტერისა და იმიტატორის მოდელირება. ახლა ვაჩვენებთ, თუ როგორ შეუძლია Q-ს მოახდინოს იმ სხვადასხვა ფიზიკური სისტემების მოდელირება, როგორც

რეალურის, ასევე თეორიულის, რომლებიც იმყოფებიან $\mathcal{T}$ ტიურინგის უნივერსალური მანქანისათვის დასაშვები ფარგლების გარეთ.

შემთხვევით რიცხვები და დისკრეტული სტოქასტური სისტემები

როგორც მოსალოდნელი იყო, არსებობს Q-თვის პროგრამა, რომლებიც წარმოქმნიან შემთხვევით რიცხვებს, მაგალითად, როდესაც ჩერდება პროგრამა

$$\phi(V_8, 2) \cdot \pi(I, 2, a) \tag{3.1}$$

a უჯრედი ½-ის ტოლი ალბათობით შეიცავს ნულს ან ერთს. იტერაციულ პროგრამებს, რომლებიც შეიცავენ (3.1), შეუძლიათ წარმოქმნან სხვა ალბათობები, ნებისმიერი რეკურსიული ალბათობის ჩათვლით. ამის მიუხედავად ეს არ ამოწურავს Q-ს შესაძლებლობებს. მარტო ეს რომ იყოს, ჩვენი პროგრამები ფაქტიურად კლასიკურები იქნებოდნენ, მიუხედავად იმისა, რომ მათ შეეძლებოდათ გამოეწვიათ გადასვლა მეხსიერების „გამოსავალი“ ნაწილის არაგამოთვლადი ბაზისის მდგომარეობაში. ახლა ჩვენ განვიხილავთ პირველ კვანტურ პროგრამას:

$$\frac{1}{\sqrt{2}}|\pi(I, 2, a) > (cos\theta|0 > + sin\theta|1 >). \tag{3.2}$$

მისი შესრულება იძლევა a ბიტს, რომელიც $cos^2\theta$ ალბათობით არის ნულის ტოლი. ყველა (3.2) სახის N_1 მდგომარეობები არიან სწორი პროგრამები Q-თვის. კერძოდ, არსებობენ სწორი პროგრამები ნებისმიერი ირაციონალური $cos^2\theta$ და $sin^2\theta$ ალბათობით. აქედან გამომდინარე, ნებისმიერი დისკრეტული სასრული სტოქასტური სისტემა იმისაგან დამოუკიდებლად, არის თუ არა მისი ალბათობის განაწილების ფუნქცია $\mathcal{T}$ გამოთვლადი, შესაძლოა სრულად იქნას მოდელირებული Q-თი. თუ $\mathcal{T}$-მანქანას გააჩნია წვდომა „შემთხვევით რიცხვთა აპარატურულ გენერატორზე“ (რომელიც “კლასიკური” სინამდვილეში არ შეიძლება არსებობდეს) ანდა „შემთხვევით ორაკულზე“ (ბენეტი, 1981 [7]) მას მაშინაც კი არ გააჩნია ეს თვისება.

მეორეს მხრივ, ჩვენ შეგვიძლია ვაიძულოთ იგი მოახდინოს მოდელირება ნებისმიერისი ზუსტით, მაგრამ არც $\mathcal{T}$-ს, არც ნებისმიერ სხვა კლასიკურ სისტემას, თვით სტოქასტურის ჩათვლით, არ შეუძლიათ მიახლოებით მაინც მოახდინონ Q-ს შემდეგი თვისების მოდელირება.

კვანტური კორელაციები

შემთხვევითი რიცხვების (3.1) და (3.2) გენერატორები სხვა პროგრამებისაგან, რომლებიც აქამდე განვიხილეთ, ცოტათი განსხვავდებიან იმით, რომ აუცილებლად წარმოქმნიან „ნაგავს“ გამოსასვლელზე. ბიტი a უჯრედში, მკაცრად რომ ვთქვათ, სავსებით შემთხვევითია მხოლოდ მაშინ, თუ უჯრედი 2-ის შიგთავსი დაფარულია მომხმარებლისაგან და შემდგომში არ ღებულობს მონაწილეობას გამოთვლებში. (3.2) კვანტური პროგრამა შესაძლებელია გამოყენებულ იქნას მხოლოდ ერთხელ, იმისათვის, რომ

წარმოქმნას ერთი შემთხვევითი ბიტი. თუ იგი ხელმეორედ იქნება გამოყენებული, გამოსავალზე გვექნება არაშემთხვევითი კორელაციები.

უფრო მეტიც, ზოგჯერ გამოყენებებში ასეთი კორელაციები ზუსტად ისაა, რაც მოითხოვება. 2 და a უჯრედების მდგომარეობები (3.1)-ის შესრულების შემდეგ „არასეპარაბელური“ (განუყოფელი) მდგომარეობებია (დ'ესპანი, 1976 [13])

$$\frac{1}{\sqrt{2}}(|0>|0>+|1>|1>). \tag{3.3}$$

განვიხილოთ პროგრამათა წყვილი, რომლებიც ერთჯერ ადგილებს უცვლიან ამ უჯრედებს. გამოსავალი თავდაპირველად ცარიელია, ე.ი.:

$$\frac{1}{\sqrt{2}}(|0>|0>+|1>|1>)|0>|0>. \tag{3.4}$$

პირველი პროგრამის მუშაობა გაჩერდება მდგომარეობაზე

$$\frac{1}{\sqrt{2}}|0>(|0>|0>+|1>|1>)|0>, \tag{3.5}$$

ხოლო მეორე პროგრამის შესრულება ჩერდება

$$\frac{1}{\sqrt{2}}|0>|0>(|0>|0>+|1>|1>)| \tag{3.6}$$

მდგომარეობაზე. ექვივალენტური პროგრამა ცხადადაა ნაჩვენები მეოთხე პარაგრაფის ბოლოს. ბელის თეორემა (1964 [4]) ამბობს, რომ არავითარ კლასიკურ სისტემას არ შეუძლია წარმოქმნას სტატისტიკური რეზულტატები (3.5) და (3.6) მომენტებში გამოსასვლელ უჯრედებზე მიმდევრობით შესრულებული გაზომვების შედეგად. (გამოსავლის გაჩენა ორ ნაბიჯზე იმ შესაძლებლობასთან ერთად, რომლებიც მომხმარებელს საშუალებას აძლევს ჩაატაროს ექსპერიმენტი ყოველი ნაბიჯის შემდეგ, საკმარისია იმისათვის, რომ შესრულდეს ლოკალურობის პირობა ბელის თეორემაში).

ორი ბიტი (3.3)-ში შესაძლებელია აგრეთვე გამოყენებული იქნას როგორც „გასაღები“ „კვანტური კრიპტოგრაფიისათვის“ (ბენეტი, 1983 [8])

ნებისმიერი სასრული ფიზიკური სისტემის სრული მოდელირება

კვანტური კომპიუტერის დინამიკა თუმცაღა მათი აგებულების თანახმად „სასრულია“, ჯერაც არაა ფიზიკური ერთი არსებითი მიზეზის გამო: მათი ევოლუცია მკაცრად უნიტარულია. მიუხედავად ამისა, თერმოდინამიკის (1.3) მესამე საწყისიდან გამომდინარეობს, რომ არავითარი რეალიზებადი ფიზიკური სისტემა არ შეიძლება მიყვანილ იქნას მდგომარეობაში, რომელიც არაა კორელიციაში გარე სისტემებთან, რამდენადაც მისი ენტროპია ასეთ შემთხვევაში იქნებოდა ნულოვანი. ამიტომ ნებისმიერი რეალიზებადი ფიზიკური სისტემა ურთიერთქმედებს სხვა სისტემებთან განსაზღვრულ მდგომარეობებში, მაგრამ მისი დინამიური კავშირის ეფექტი გარე სისტემებთან არ შეიძლება ნულამდე შემცირდეს სასრული პროცესით, რამდენადაც ამ კორელაციის თავისუფლების ხარისხების ტემპერატურა ნულამდე შემცირდებოდა. ამიტომ

შეუძლებელია არსებობდეს ხერხი, რომელიც სისტემას მიიყვანს ისეთ მდგომარეობაში, რომლის დროსაც ევოლუციის ოპერატორი არ ურევდეს ერთმანეთში შინაგანი და გარეგანი თავისუფლების ხარისხებს.

ამიტომ სასრულრეალიზებადი ფიზიკური სისტემის L-განზომილებიანი $\mathcal{H}$ მდგომარეობათა სივრცის ჭეშმარიტი აღწერა არ შეიძლება განხორციელდეს $\mathcal{H}$-ში მდგომარეობათა ვექტორების საშუალებით, არამედ გამოყენებული უნდა იქნას ρ_a^b სიმკვრივის მატრიცი. პრინციპში, ნებადართულია სიმკვრივის ყველა მატრიცები, გარდა სუფთა მდგომარეობათა შემთხვევებისა. ასეთი სისტემის დინამიკა აღიწერება არა უნიტარული ოპერატორით, არამედ სუპერგაბნევის S მატრიცით:

$$\rho_a^b(T) = \sum_{c,d} S_{ad}^{bc} \rho_c^d(0). \tag{3.7}$$

აღნიშვნის ღირსია ის გარემოება, რომ ჩვენ არ ვიცავთ მთლიანობაში სამყაროს არაუნიტარულ დინამიკას, რაც იქნებოდა ერესი, რომელიც ეწინააღმდეგება კვანტურ თეორიას. (3.7) განტოლება არის $\mathcal{H}$-ში უნიტარული ევოლუციის პროექცია $\mathcal{H}\times\mathcal{H}'$ სივრცეზე, სადაც $\mathcal{H}'$ არის დანარჩენი სამყაროს გარკვეული ნაწილი. უხეშად რომ ვთქვათ (სისტემები შორსაა წონასწორობებისაგან), $\mathcal{H}'$,,სითბური რეზერვუარის“ როლს თამაშობს.

ამრიგად, სუპერგაბნევის ზოგადი ოპერატორი არის

$$S_{ad}^{bc} = \sum_{e',f',g'} U_{ae'}^{cf'} U_{ag'}^{bc'} \bar{\rho}_{f'}^{g'} \tag{3.8}$$

გამოსახულება, სადაც $U_{ab'}^{cd'}$ არის უნიტარული ოპერატორი $\mathcal{H}\times\mathcal{H}'$-ზე, ისეთი, რომ

$$\sum_{c,d'} U_{ab'}^{cd'} U_{ad'}^{ef'} = \delta_a^e \delta_{b'}^{f'}. \tag{3.9}$$

სუპერგაბნევის ოპერატორი არ იშლება $\mathcal{H}$ და $\mathcal{H}'$-ზე განსაზღვრული ოპერატორების ნამრავლად (ზედა და ქვედა ინდექსი აღნიშნავს კომპლექსურად შეუღლებას), $\bar{\rho}_{a'}^{b'}$ “თითქმის არის სითბური რეზერვუარი” სიმკვრივის მატრიცი. ასეთი განსაზღვრება იქნებოდა ზუსტი, თუკი სისტემა - სითბური რეზერვუარი და მოწყობილობა, რომელსაც სისტემა მიყავს საწყის მდგომარეობაში, აქამდე არ კორელირებდნენ. გადავწეროთ (3.8) $\mathcal{H}'$ ბაზისში, რომელშიც $\bar{\rho}$ დიაგონალურია

$$S_{ad}^{bc} = \sum_{e',f'} P_{f'} U_{ae'}^{cf'} U_{ag'}^{bc'} \bar{\rho}_{f'}^{g'},$$
$$\sum_{a'} P_{a'} = 1, \tag{3.10}$$

სადაც $\bar{\rho}$ ალბათობები $p_{a'}$-ს საკუთრივ მნიშვნელობებია, ყველა სუპერგაბნევის მატრიცების (3.8) ანდა (3.10) სიმრავლე G ძევს $\mathcal{H}\times\mathcal{H}^{*}\times\mathcal{H}^{*}\times\mathcal{H}$ სივრცის იმ $\mathcal{I}$ ქვესივრცეში, რომლის ელემენტები აკმაყოფილებენ ტოლობას

$$\sum_a S_{ad}^{bc} = \delta_c^b. \tag{3.11}$$

ნებისმიერი ელემენტი G-დან აკმაყოფილებს შეზღუდვას

$$0 \leq \sum_{a,b,c,d} \rho_b^{(1)} S_{ad}^{bc} \rho_c^{(2)^d} \leq 1, \tag{3.12}$$

ყოველი $\rho^{(l)}$ და $\rho^{(2)}$ სიმკვრივის მატრიცებისათვის.

(3.12) უტოლობის მარცხენა მხარე შეიძლება გადაიქცეს ტოლობად მხოლოდ მაშინ, თუ მდგომარეობები $\mathcal{H}$-დან წარმოქმნიან არაცარიელი გადაკვეთის მქონე ქვესიმრავლეებს, იმის ნულოვანი ალბათობით, რომ სითბურმა ხმაურმა შეიძლება გამოიწვიოს გადასვლები მათ შორის. ეს შეუძლებელია მხოლოდ მაშინ, თუ არ არის სუპერშერჩევის წესი, რომელიც კრძალავს ასეთ გადასვლებს; გამოვრიცხავთ რა ამის შესაძლებლობას, ჩვენ არ ვზღუდავთ ზოგადობას იმიტომ, რომ მხოლოდ ერთი სუპერშერჩევის თვისების მქონე სექტორი დროის ყოველ მომენტში შესაძლოა რეალიზებული იქნას, როგორც ფიზიკური სისტემა. მარჯვენა უტოლობა გადაიქცევა ტოლობად მხოლოდ ოპერატორების უნიტარულობის შემთხვევაში

$$S_{ad}^{bc} = U_a^c U_d^b, \tag{3.13}$$

რომელიც არაფიზიკურია, რადგან წარმოადგენს სრულად არადისიპაციურ სისტემას. ფიზიკურად რეალიზებადი ელემენტების G სიმრავლე ღიაა $\mathcal{J}$-ში. უფრო მეტიც, ნებისმიერი Q-გამოთვლადი $S^{(1)}$-ის და $S^{(2)}$-ის ამოზნექილი წრფივი კომბინაცია

$$p_1 S^{(1)} + p_2 S^{(2)}, \tag{3.14}$$

სადაც p_1 და p_2 ნებისმიერი ალბათობებია, ისევ გამოთვლადია შემთხვევით რიცხვთა (3.2) გენერატორის თვისებებიდან გამომდინარე. გამოვთვლით რა (3.10)-ის მსგავს უნიტარულ გარდაქმნებს, შესაძლებელი იქნება გამოვთვალოთ ნებისმიერი ელემენტი G-ს თვლადი, ყველგან მკვრივი ქვესიმრავლიდან. მაგრამ ნებისმიერი წერტილი სასრულგანზომილებიანი ვექტორული სივრცის ნებისმიერ ღია მიდამოდან შეიძლება წარმოდგენილი იქნას როგორც ამ სივრცის ნებისმიერი მკვრივი ქვესიმრავლის ელემენტების სასრული ამოზნექილი წრფივი კომბინაცია. აქედან გამომდინარე Q-ს შეუძლია მოახდინოს სასრულგანზომილებიანი მდგომარეობათა სივრცის მქონე ნებისმიერი ფიზიკური სისტემის სრული მოდელირება. ამიტომ კვანტური თეორია ჩიორჩ-ტიურინგის (1.2) პრინციპთან თავსებადია.

სწორია თუ არა საკითხი, რომ ფიზიკური სამყაროს ყველა სასრული სისტემების მოდელირება მსგავსი სახით შეიძლება კვანტურ Q კომპიუტერის მეშვეობით, ანუ სრულდება თუ არა (1.2) ბუნებაში, ღია უნდა დარჩეს მანამ, სანამ არ იქნება მდგომარეობათა სივრცის და სამყაროს დინამიკის უფრო ღრმა გაგება. ის მცირედი, რაც ცნობილია, როგორც ჩანს ადასტურებს ამ პრინციპს. თუ შავი ხვრელის თერმოდინამიკური თეორია ნდობას იმსახურებს, მაშინ არავითარ სისტემას, რომლის ზედაპირიც შემოსაზღვრულია გარკვეული A ფართით, არ შეიძლება გააჩნდეს

$$N(A) = \exp\left(\frac{Ac^3}{4\hbar G}\right) \quad (3.15)$$

სასრულ რიცხვზე უფრო მეტი (ბეკენშტეინი, 1981 [3]) განსხვავებული შესაძლო მდგომარეობები (სადაც $\hbar$ არის პლანკის მუდმივა, G–გრავიტაციული კონსტანტა, ხოლო c კი სინათლის სიჩქარეა), ანუ შესაბამის ბაზისში სისტემა შესაძლოა სრულად აღიწეროს $N(A)$ – განზომილებიანი სივრცის გამოყენებით და შესაბამისად სრულად მოდელირდება Q-ს მეშვეობით.

პარალელური გამოთვლები მიმდევრობით კომპიუტერზე

კვანტური თეორია პარალელურად ურთიერთმოქმედი სამყაროთა თეორიაა. არსებობს გარემოებანი, რომლის დროსაც სხვადასხვა სამყაროში შესრულებული გამოთვლები შესაძლებელია კომბინირებულ იქნას Q-ს მეშვეობით, რომელიც პარალელური დაშუშავების შესაძლებლობას იძლევა. განვიხილოთ კვანტური პროგრამა

$$\frac{1}{\sqrt{N}}\sum_{i=1}^{N}|\pi(f,2,3),i,0>, \quad (3.16)$$

რომელიც ყველა N სამყაროში გამოითვლის $f(i)$-ს ყოველი i-თვის 1-დან N-მდე. წრფივობიდან და (2.11)-დან გამომდინარეობს, რომ (3.16)-ის შესრულების შემდეგ Q ჩერდება

$$\frac{1}{\sqrt{N}}\sum_{i=1}^{N}|\pi(f,2,3),i,f(i)> \quad (3.17)$$

მდგომარეობაში, თუმცაღა ეს გამოთვლა მოითხოვს ზუსტად იგივე დროს, მეხიერების მოცულობას და აღჭურვილობას, რასაც (2.11). (3.17) შეიცავს ცალკეული გამოთვლების საკმაოდ დიდ რიცხვს. სამწუხაროდ, თითოეულ სამყაროში ხელმისაწვდომია არაუმეტეს ერთი ამ შედეგთაგანი. თუ (3.16) მრავალჯერ სრულდება, საშუალო დრო, რომელიც $f(i)$-ების ყველა N მნიშვნელობების გამოსათვლელადაა საჭირო და რომელსაც აღვნიშნავთ f-ით, არ არის ნაკლები იმ დროზე, რაც (2.11)-ში გვქონდა ყველა მათგანის თანმიმდევრობით გამოსათვლელად. ახლა ვაჩვენებთ, რომ ნებისმიერი არატრივიალური N-ჯერადად დაპარალელებადი $G(f)$ ყველა შესაძლო f ფუნქციების გამოთვლის დროის მათემატიკური ლოდინი კვანტური პარალელიზმის მეშვეობით, ისეთის, როგორიცაა (3.16)-ში, არ შეიძლება იყოს უფრო მცირე, ვიდრე ის დრო, რომელიც საჭიროა მათი მიმდევრობით შესასრულებლად (2.11)-ის მეშვეობით.

სიმარტივისთვის ვიგულისხმოთ, რომ τ (2.11)-ის შესრულებისას არაა i-ზე დამოკიდებული და დრო, რომელიც საჭიროა ყველა f-ის კომბინირებისათვის, რომ მოხდეს $G(f)$-ის ფორმირება, ძალიან მცირეა. ეხლა დავუშვათ, რომ არსებობს პროგრამა ς, რომელიც თითოეული f ფუნქციისათვის ამოიღებს $G(f)$-ის მნიშვნელობას (3.17)-დან საკმაოდ მცირე დროში $|\beta|^2$ ალბათობით. ე.ი. ς მოქმედებს შემდეგნაირად:

$$\frac{1}{\sqrt{N}}\sum_{i=1}^{N}|1,f(i)> \rightarrow \beta\Big|0,G(\boldsymbol{f})> +\sqrt{1-|\beta|^2}|1>\Big|\lambda(\boldsymbol{f})>, \qquad (3.18)$$

სადაც $|\lambda(\boldsymbol{f})>$ მდგომარეობები არ შეიცავენ ინფორმაციას *G(f)*-ზე. მაშინ პირველი უჯრედი შეიძლება გაიზომოს. თუ შეიცავს 0-ს, მაშინ მეორე უჯრედი უნდა შეიცავდეს *G(f)*-ს. სხვანაირად (3.17)-ში ინფორმაცია დაკარგული იქნება და მოგვიწევს მისი თავიდან გამოთვლა. უნიტარულობა მოიცავს

$$\frac{1}{n}\sum_{i=1}^{N}\delta\big(f(i),g(i)\big)=|\beta|^2\delta\big(G(\boldsymbol{f}),G(g)\big)-(1-|\beta|^2)<\lambda(\boldsymbol{f})|\lambda(\boldsymbol{g})> \qquad (3.19)$$

ტოლობას ნებისმიერი *g(i)* და *f(i)* ფუნქციებისათვის.

თუ *G(f)* არ არის კონსტანტა, მაშინ ნებისმიერი *f(i)* ფუნქციისათვის არსებობს მეორე ფუნქცია *g(i)*, ისეთი რომ *G(g)≠ G(f)*, მაგრამ *g(i)=f(i)* *i*-ის ყველა მნიშვნელობებისათვის 1-დან *N*-მდე, გარდა ერთი მნიშვნელობისა. ამ შემთხვევაში

$$1-\frac{1}{N}=(1-|\beta|^2)<\lambda(\boldsymbol{f})|\lambda(\boldsymbol{g})>, \qquad (3.20)$$

რაც გვაძლევს, რომ $|\beta|^2<1/N$. ამრიგად, *G(**f**)*-ის გამოსათვლელად საჭიროა დრო $\frac{\pi}{|\beta|^2}=N_\tau$-ის ტოლი მაინც იყოს. აქედან გამოდის, რომ კვანტური პარალელიზმი არ შეიძლება გამოყენებულ იქნას ალგორითმების განპარალელების საშუალო დროის შესამცირებლად.

კვანტური პარალელიზმის მაგალითად *n=2* შემთხვევაში განვიხილოთ

$$G(f)\equiv f(0)\oplus f(1), \qquad (3.21)$$

(იხ. განტოლება (2.12)) მაშინ (3.17) მდგომარეობას, რომელიც კვანტურ პარალელურ გამოთვლებს ახლავს, აქვს სახე

$$\frac{1}{\sqrt{2}}(|0,f(0)>+|1,f(1)>). \qquad (3.22)$$

ς პროგრამა, რომელიც ამ მდგომარეობის „დეკოდირებისათვისაა“ ვარგისი, აწარმოებს ნებისმიერი არაგადაგვარებადი და დაკვირვებადი სიდიდის გაზომვას საკუთრივი მდგომარეობებით:

$$\left.\begin{aligned}|zero>&\equiv\frac{1}{2}(|0,0>-|0,1>+|1,0>-|1,1>,\\ |one>&\equiv\frac{1}{2}(|0,0>-|0,1>-|1,0>+|1,1>,\\ |fail>&\equiv\frac{1}{2}(|0,0>+|0,1>+|1,0>+|1,1>,\\ |error>&\equiv\frac{1}{2}(|0,0>+|0,1>-|1,0>-|1,1>.\end{aligned}\right\} \qquad (3.23)$$

ასეთი დაკვირვებადი სიდიდე არსებობს, რამდენადაც (3.23) მდგომარეობები წარმოქმნიან ორთონორმირებულ სიმრავლეს. უფრო მეტიც, გაზომვები შესაძლებელია შესრულდეს ფიქსირებულ დროში, რომელიც არ არის დამოკიდებული *f*-ის გამოსათვლელი ალგორითმის შესრულების დროზე. თუ გაზომვის რეზულტატია “zero” (ე.ი. საკუთრივი მნიშვნელობა, რომელიც შეესაბამება $|zero>$-ს) ან “one”, მაშინ შეიძლება დავასკვნათ, რომ

$f(0)\oplus f(1)$ უდრის შესაბამისად ნულს ან ერთს. როგორიც არ უნდა იყოს f ფუნქცია , ½ -ის ტოლი ალბათობით გამოსავალი იქნება "fail", რომლის დროსაც $f(0)\oplus f(1)$ მნიშვნელობაზე არ შეიძლება არავითარი დასკვნის გაკეთება. გამოსასვლელზე "error"-ის გამოჩენის ალბათობა შესაძლებელია გახდეს რაგინდ მცირე *f*-ის ბუნებისგან დამოუკიდებელად.

ამ მაგალითში გამოთვლის დროა $N\tau$. ამასთანავე, *N>2*-თვის ჩვენთვის უცნობია ისეთი მაგალითი, რომლის მუშაობის საშუალო დრო $(N^2-2N+2)\tau$-ზე ნაკლებია და ამიტომ ვვარაუდობთ, რომ ქვევიდან ეს შეფასება ოპტიმალურია. ამის გარდა, თუმცაღა არსებობენ არატრივიალური მაგალითები კვანტურად განპარალელებადი ალგორითმებისა ყველა *N*-თვის (იმ შემთხვევაში, როდესაც *N*>0-ზე), ოღონდ არც ერთი მათგანისათვის *G(f)* ფუნქციის განსაზღვრის არე არ წარმოადგენს *f* ფუნქციის 2^N შესაძლო გრაფიკების სიმრავლეს.

პრაქტიკულ გამოთვლად ამოცანებში, განსაკუთრებით რეალური დროის გამოთვლებში, ყოველთვის არაა საჭირო პროგრამის გამოთვლის საშუალო დროის მინიმიზირება: ხშირად მოითხოვება მინიმალური ან მაქსიმალური დროის, ან, რაიმე უფრო რთული ზომის სიდიდის მინიმიზირება. ასეთ შემთხვევაში კვანტურ პარალელიზმს შეუძლია თავისი სიტყვა თქვას. მოვიყვანთ ამის ორ მაგალითს:

(1) დავუშვათ, რომ საფონდო ბირჟაზე (3.17) ხვალინდელი ცვლილებების შეფასების პროგრამაა მისი დღევანდელი მდგომარეობით, ხოლო *G(f)* განსაზღვრავს ინვესტიციების საუკეთესო სტრატეგიას. თუ τ ერთი დღეა და *N=2,* ამ პროგრამის კლასიკური ვერსია ორ დღეს მუშაობს, რის გამოც გამოუსადეგარია. თუ კვანტური ვერსია სრულდება ყოველდღე, მაშინ საშუალოდ ერთ დღეს ორი უჯრედიდან ერთი შეიცავს გაზომვის რეზულტატს „1", რომელიც შეესაბამება "fail"-ს (წარუმატებლობას). ასეთ დღეებში ინვესტირება არ ღირს. მაგრამ ასეთივე საშუალო სიხშირით ფუნქცია *G(f),* რომელიც ორი კლასიკური "პროცესორი-დღის" გამოთვლების შედეგებს აერთიანებს, გამოითვლებოდა ერთ დღეში. *N* ჯერადი პარალელური ამოცანის ქვეამოცანები, განაწილებული N^2-2N+2 სამყაროებს შორის, უკიდურეს შემთხვევაში ერთერთ მათგანში მაინც მოგვცემს საბოლოო შედეგს.

(2) ახლა განვიხილოთ ინფორმაციის პარალელური დამუშავების ამოცანა, რომელიც ხმაურის გავლენით ინფორმაცია მახინჯდება. მაგალითად, ფიქსირებული τ დროის შუალედში მოითხოვება რაღაც *N*-ჯერადი განპარალელებადი *G(f)* ფუნქციის გამოთვლა. ხელმისაწვდომია *NR*-პროცესორი, რომელთაგან თითოეულმა სითბური ხმაურის მიზეზით შეიძლება მოგვცეს წყვეტა და ა.შ. *p* ალბათობით. სიმარტივისათვის ვიგულისხმოთ რომ

მოწყობილობის ასეთი შეცდომის აღმოჩენა საიმედოა. ამოცანა მდგომარეობს q შეფერხებების საერთო სიხშირის მინიმიზირებაში. "კლასიკურად" (ე.ი. კვანტური პარალელიზმის გამოყენების გარეშე) q-ს მინიმიზირება შეიძლება R-ჯერადი სიჭარბის ხარჯზე: R პროცესორი პროგრამირდება თითოეული N პარალელური ქვეამოცანის შესასრულებლად. მთლიანობაში მანქანა მოგვცემს შეფერხებას მაშინ, თუ ყველა R პროცესორი, რომელიც რაიმე ქვეამოცანას ასრულებს, მოგვცემს შეფერხებას. ეს ხდება

$$q_{classical} = 1 - (1 - p^R)^N \tag{3.24}$$

ალბათობით. ამასთან, კვანტური პარალელიზმის გამოყენების შემთხვევაში თითოეულს NR პროცესორთაგან შეიძლება მივცეთ ყველა N ამოცანა. ყოველი მათგანი შეიძლება განხორციელდეს ორი დამოუკიდებელი მიზეზის გამო: *(i)* ალბათობით p მოხდება აპარატურული შეფერხება, *(ii)* ალბათობით, რომელიც განვსაზღვრეთ გარკვეული $G(f)$-თვის, როგორც $\frac{1}{N^2 - 2N + 2}$, პროცესი დასრულდება იმ სამყაროში, რომელშიც პასუხი არ მიიღება. მოითხოვება, რომ NR პროცესორთაგან ერთმა მაინც იმუშაოს წარმატებით, ამიტომ შეფერხების სიხშირეს აქვს მნიშვნელობა

$$q_{quantum} = \left[1 - \frac{1-p}{N^2 - 2N + 2}\right]^{NR}, \tag{3.25}$$

რომელიც p-ს, N-ის და R-ის გარკვეული მნიშვნელობისათვის შეიძლება იყოს უფრო მცირე, ვიდრე (3.24).

უფრო სწრაფი კომპიუტერები

ოდესმე ტექნოლოგიურად შესაძლებელი გახდება კვანტური კომპიუტერის აგება და შესაძლოა ფუნდამენტურ კომპონენტად გამოყენებულ იქნას კვანტური ნაკადები [17]. მოსალოდნელია, რომ ასეთი კომპიუტერების გამოთვლითი სწრაფქმედება იქნება ეფექტური და ტიურინგის მსგავსი მანქანების სწრაფქმედებაზე აღმატებული (იგულისხმება ერთნაირი ტექნოლოგიებით აგებული მანქანები). ეს შეიძლება უცნაურად მოგვეჩვენოს, რამდენადაც ვაჩვენეთ, რომ არავითარი რეკურსიული ფუნქცია არ შეიძლება Q-მანქანაზე კვანტური პროგრამის მიერ უფრო სწრაფად იქნას ამოხსნილი, ვიდრე მის გარეშე, იგულისხმება ამოხსნის საშუალო დრო. მით უმეტეს Q-ს იდეალიზაციისას მხედველობაში არ იღებენ იმ წმინდა ტექნოლოგიურ ფაქტს, რომლის თანახმადაც ყოველთვის უფრო ადვილია იდენტური სისტემების ძალიან დიდი რაოდენობა მიიყვანო პრაქტიკულად ერთ მდგომარეობამდე, ვიდრე თითოეული მათგანი საკუთარ მდგომარეობამდე. ამიტომ შესაძლებელია

გამოყენებული იქნას R-ის სიჭარბე გაცილებით უფრო ეფექტურად პარალელური კვანტური პროგრამებისათვის, ვიდრე კლასიკურისათვის.

შედეგები კვანტური თეორიის ინტერპრეტაციისათვის

უფრო ადრინდელ ნაშრომში (დოიჩი, 1985 [12], შეადარეთ აგრეთვე ალბერტი, 1983 [1]), ნაჩვენები იყო, თუ როგორ შეიძლებოდა კვანტური თეორიის ევერეტისეული ინტერპრეტაციის (მრავალი სამყაროს სურათი) გადამწყვეტი ექსპერიმატალური შემოწმება კვანტური კომპიუტერის გამოყენებით (და ამრიგად, წინააღმდეგობაში მოსვლა საყოველთაოდ გავრცელებულ რწმენასთან, რომ იგი ექსპერიმატულად არ განსხვავდება სხვა ინტერპრეტაციებისაგან). მაგრამ ასეთი ცდების ჩატარება მოითხოვს როგორც კვანტური კომპიუტერების აგებას, ასევე ხელოვნური ინტელექტის პროგრამების დამუშავებას. კვანტური კომპიუტერების მუშაობის ახსნისას, ჩვენ, როდესაც ეს აუცილებელი იყო, ვეყრდნობოდით ევერეტის ონტოლოგიას.

რა თქმა უნდა ეს ახსნები შეიძლება ყოველთვის "გადავიყვანოთ" ჩვეულებრივ ინტერპრეტაციაში, მაგრამ ამ დროს სრულიად იკარგება მათი ახსნა-განმარტებითი ძალა. დავუშვათ, რომ კვანტური კომპიუტერი დაპროგრამებული იყო ისე, როგორც ეს აღწერილია საფონდო ბირჟის ამოცანაში. ყოველდღიურად იგი იღებს განსხვავებულ მონაცემებს. ევერეტის ინტერპრეტაცია კარგად ხსნის როგორ იქცევა კომპიუტერი, თუ მან გადასცა ქვეამოცანები თავის ასლებს სხვა სამყაროებში. როგორ აიხსნება ჩვეულებრივი ინტერპრეტაციით სწორი პასუხების არსებობა იმ დღეებში, როდესაც კომპიუტერი წარმატებით ასრულებს ორ პროცესორ-დღის სამუშაოს? სადაა გამოთვლილი ეს პასუხი?

4. შემდგომი კავშირები ფიზიკასა და კომპიუტერულ მეცნიერებას შორის

სირთულის კვანტური თეორია

სირთულის თეორია ძირითადად დაკავშირებულია ფუნქციების გამოთვლაზე დადებულ შეზღუდვებთან: რომელი ფუნქციები შეიძლება გამოითვალოს, რამდენად სწრაფად და რა მოცულობის მეხსიერების გამოყენებით. კვანტური კომპიუტერების, ისევე როგორც კლასიკური ალბათური კომპიუტერების შემთხვევაში, ისმის კითხვა "როგორი ალბათობით"? ჩვენ უკვე ვიცით, რომ გამოთვლის მინიმალური დრო Q-სათვის შეიძლება იყოს ნაკლები ვიდრე T-თვის. სირთულის თეორია Q-თვის იძლევა შემდგომი კვლევის ჩატარების საშუალებას.

სირთულის თეორიის ნაკლებად პრაქტიკული, მაგრამ პოტენციურად უფრო მნიშვნელოვანი გამოყენება – ფიზიკურ სისტემებში სირთულის

სპონტანური ზრდის გაგების ცდაშია, მაგალითად, სიცოცხლის ევოლუციისა და ცოდნისა ადამიანის შესახებ. ბენეტმა (1983, [12]) განიხილა რამდენიმე განსხვავებული სირთულის საზომი ("სიღრმე" ან "ცოდნა"), რაც ადრე იყო შემოთავაზებული. მათ უმეტესობას ფატალური ნაკლი გააჩნიათ, რომელიც იმაში მდგომარეობს, რომ ისინი უმაღლეს "სირთულეს" ანიჭებენ სრულიად შემთხვევით მდგომარეობას. ამგვარად, ისინი ვერ ანსხვავებენ ჭეშმარიტ ცოდნას ინფორმაციის შინაარსისაგან. ბენეტმა გადაჭრა ეს პრობლემა. მისი "ლოგიკური სიღრმე" არის, უხეშად რომ ვთქვათ, ყველაზე მოკლე T-როგრამის მუშაობის დრო, რომელიც ითვლის ცარიელი შესასვლელიდან გამომდინარე მოცემულ ψ მდგომარეობას. ბიოლოგიურ ტერმინოლოგიაში ლოგიკური სიღრმე ზომავს იმ ევოლუციას, რომელიც საჭიროა უმარტივესი ψ-ს წარმოქმნისათვის შესაძლო წინამორბედებისაგან. ერთი შეხედვით შეიძლება მოგვეჩვენოს, რომ ბენეტის კონსტრუქცია კარგავს თავის ფიზიკურ საფუძველს, როდესაც სცდება ტიურინგის მანქანების მკაცრად დეტერმინირებული ფიზიკის საზღვრებს. ფიზიკურ რეალობაში შემთხვევითი მდგომარეობების უდიდესი ნაწილი ჩნდება არა "გრძელი პროგრამებიდან" (ე.ი. წინამორბედებისაგან, რომელთა სირთულე ახლოა მათ საკუთარ სირთულესთან), არამედ მოკლე პროგრამებიდან, რომლებიც არადეტერმინირებულ მოწყობილობებთან არიან შერწყმულნი.

მიუხედავად ამისა, არსებობს ბენეტის იდეის კვანტური ანალოგი, რომელიც ამ პრობლემას წყვეტს. განვსაზღვროთ კვანტური მდგომარეობის Q ლოგიკური სიღრმე, როგორც ყველაზე მოკლე Q პროგრამის შესრულების დრო, რომელიც (ეს პროგრამა) წარმოშობს ამ მდგომარეობას (ან შესაძლოა, როგორც ამას ბენეტი აკეთებდა, ავიღოთ ყველა ასეთი პროგრამის შესრულების საშუალო ჰარმონიული დრო). შემთხვევითი რიცხვები სწრაფად შეიძლება წარმოიქმნას მოკლე Q პროგრამებით.

უნდა აღინიშნოს, რომ Q-ლოგიკური სიღრმე არაა დაკვირვებადი პრინციპშიც კი, იმიტომ, რომ იგი შეიცავს ინფორმაციას ყველა სამყაროს შესახებ. მაგრამ მას გააჩნია ფიზიკური აზრი: Q- ლოგიკური სიღრმე ინფორმაციის კარგი საზომია, რადგანაც იგი წონას ანიჭებს მხოლოდ სირთულეს, რომელიც არსებობს ყველა სამყაროში და მაშასადამე "იძულებით" მოთავსებულია ყველგან ღრმა პროცესის სახით. დაკვირვებადი რთული მდგომარეობები, რომლებიც განსხვავებულია განსხვავებულ სამყაროებში წარმოადგენენ არა ჭეშმარიტად ღრმა, არამედ მხოლოდ შემთხვევით მდგომარეობებს, რადგანაც Q ლოგიკური სიღრმე – კვანტური მდგომარეობის (ვექტორის) თვისებაა, არ მოითხოვება, რომ კვანტურ ქვესისტემას ჰქონდეს ზუსტად განსაზღვრული Q-ლოგიკური სიღმე (თუმცა ხშირად სასურველია აპროქსიმაციის კარგი ხარისხი). ეს მოსალოდნელია, რადგანაც ინფორმაცია

სისტემაში შეიძლება იყოს კორელაციებში სხვა სისტემებთან. ამის ნათელი მაგალითია–კვანტური კრიპტოგრაფია.

კავშირები ჩიორჩ-ტიურინგის პრინციპსა და ფიზიკის სხვა დარგებს შორის

ჩვენ ვნახეთ, რომ კვანტური თეორია უზრუნველყოფს ჩიორჩ-ტიურინგის პრინციპის (1.2) მკაცრ ფორმას მხოლოდ თერმოდინამიკის (1.3) მესამე კანონის ჭეშმარიტების დაშვებისას. ამ დამოკიდებულების უკეთ გაგება შეიძლება, თუ განვიხილავთ ჩიორჩ-ტიურინგის პრინციპს, როგორც უფრო ფუნდამენტურს და მესამე კანონს გამოვიყვანთ ამ პრინციპიდან და კვანტური თეორიიდან.

ის გარემოება, რომ კლასიკური ფიზიკა არ უზრუნველყოფს (1.2)-ს, იძლევა საფუძველს შემდგომი ნაბიჯების გასაკეთებლად. ზოგიერთი თავისებურებანი, რომლებიც განასხვავებენ კვანტურ თეორიას კლასიკური ფიზიკისაგან (მაგალითად, დაკვირვებადი სიდიდეების დისკრეტულობა) შეიძლება გამოყვანილი იქნას მხოლოდ (1.2)-დან და თერმოდინამიკის კანონებიდან. ამიტომ ახალი პრინციპი გვაძლევს უილერის პრობლემის ნაწილობრივ გადაწყვეტას მაინც: "რატომ უნდა არსებობდეს კვანტური თეორია?" (Why did quantum theory have to be? იხ. მაგ. მ. უილერი, 1985 [22]).

სხვადასხვაგვარი "დროის ისრები", რომლებიც არსებობს ფიზიკის სხვადასხვა დარგებში, შეიძლება შეკავშირდნენ და წარმოდგენილი იქნას, როგორც იმავე ეფექტების სხვა გამოვლინებები. მაგრამ ითვლება, რომ "ფსიქოლოგიური" ან "გნოსეოლოგიური" დროის ისარი–გამონაკლისია. ბენეტამდე (1973) [6] აგრეთვე ითვლებოდა, რომ გამოთვლები თავისი არსით შეუქცევადია და ამიტომ დროის ფსიქოლოგიური ისარი აუცილებლად მიმართულია იმ მხარეს, სადაც ენტროპია იზრდება. ეს აზრი ამჟამად შეირყა, რადგანაც ნავარაუდევი კავშირი მცდარია.

დროის ფსიქოლოგიური ისრის ფიზიკაში დაბრუნების ერთადერთი გზაა – ბუნების სხვა ახალი პრინციპის პოსტულირება, რომელიც უშუალოდ დაეფუძნება Q-ლოგიკურ სიღრმეს.

გონივრულად გვეჩვენება აზრი იმის შესახებ, რომ სამყაროს Q-ლოგიკური სიღრმე თავდაპირველად მინიმალურია. ახალი პრინციპის უფრო ოპტიმისტური ვარიანტი შეიძლება მოითხოვდეს, რომ Q-ლოგიკური სიღრმე იყოს არაკლებადი. არ იქნება გონივრული ვიმედოვნოთ, რომ თერმოდინამიკის მეორე კანონი შესაძლებელია გამოვიყვანოთ Q-ლოგიკური სიღრმეზე ამ სახის შეზღუდვების დადების შემდეგ. ეს დაამყარებდა ჭეშმარიტ კავშირებს ფსიქოლოგიურ (ან ეპისტომოლოგიურ ან ევოლუციურ) და თერმოდინამიკურ "დროის ისრებს" შორის.

ფიზიკის პროგრამირება

ჩიორჩ-ტიურინგის პრინციპის ფიზიკის კანონად აღქმა არ ნიშნავს იმას, რომ კომპიუტერული მეცნიერება უბრალოდ ფიზიკის ნაწილია. ეს თვალსაზრისი აქცევს ექსპერიმენტულ ფიზიკის გარკვეულ ნაწილს კომპიუტერულ მეცნიერების ქვედარგად.

უნივერსალური კვანტური Q-კომპიუტერის არსებობიდან გამომდინარეობს, რომ არსებობს პროგრამა ყოველი ფიზიკური პროცესისათვის. კერძოდ Q-ს შეუძლია ჩაატაროს ნებისმიერი ფიზიკური ექსპერიმენტი. ზოგიერთ შემთხვევებში (მაგ. კონსტანტების ან ურთიერთქმედების ფორმების გაზომვისას) ამას არავითარი სარგებლობა არ მოაქვს, რადგანაც პროგრამის დასაწერად ცნობილი უნდა იყოს შედეგი. მაგალითად, როდესაც თვით კვანტური თეორია მოწმდება, ყოველი ექსპერიმენტი არის Q-პროგრამის შესრულება. Q-ზე შემდეგი ალგოლ-68 პროგრამის მუშაობა არის აინშტაინ-პოდოლსკი-როზენის ექსპერიმენტის ჩატარება

```
begin
        int n=8*random;
        bool x,y;
        x:=y:=false;
        V(8,y)
        x eorab y;
        if V (n,y )≠
          V (n,x)
           then print (("კვანტური
თეორია უარყოფილია."))
           else print (("კვანტური
თეორია მიღებულია."))
fi
End
```

კვანტური კომპიუტერები აყენებენ პროგრამირების ენების დამუშავების საინტერესო პრობლემებს, რომლებსაც აქ არ განვიხილავთ. ვიტყვით მხოლოდ, რომ შეიძლება დაიწეროს პროგრამები, რომლებიც შეამოწმებდნენ (სირთულის ზრდის მიხედვით) ბელის უტოლობას, კვანტური დინამიკის წრფივობას და ევერეტის ინტერპრეტაციას. მათი დაწერა მკითხველისთვის მიგვინდვია.

მადლობას მოვახსენებთ დოქტორ ბენეტს, რომელმაც მიგვანიშნა, რომ ჩიორჩ-ტიურინგის ჰიპოთეზას ფიზიკური აზრი აქვს, კ. პენროუზსა და კ. ვოლფს საინტერესო დისკუსიებისათვის კვანტური კომპიუტერების შესახებ და პროფ. რ. პენროუზს, ამ სტატიის შავი ვარიანტის წაკითხვისა და შემოთავაზებული შესწორებისათვის.

ლიტერატურა

[1] Albert, D.Z. 1983 *Phys.Lett*. A **98**, 249.

[2] Bekenstein, J.D. 1973 *Phys.Rev*. D 7, 2333.

[3] Bekenstein, J.D. 1981 *Phys.Rev*. D 23, 287.

[4] Bell, J.S. 1964 *Physica* **1**, 195.

[5] Benioff, P.A. 1982 *Int.J.theor.Phys*. **21**, 177.

[6] Bennet, C.H. 1973 *IBM Jl Res.Dev*. **17**,525.

[7] Bennet, C.H. 1981 *SIAM Jl Comput*. **10**, 96.

[8] Bennet, C.H. 1983 On various measures of complexity, especially "logical depth". Lecture at Aspen. IBM Report.

[9] Bennet, C.H., Brassard, G., Breidbart, S. & Wiesner, S. 1983 Advances in cryptography. In *Procedings of Crypto* 82. New York: Plenum.

[10] Chaitin, G.J. 1977 *IBM Jl Res. Dev*. **21**, 350.

[11] Church, J. 1936 *Am.J.Math*. **58**, 435.

[12] Deutsch, D. 1985 *Int.J.Theor.Phys*. **24**, 1

[13] d'Espagnat, B. 1976 *Conceptual foundations of quantum mechanics* (second edn). Reading, Massachusetts: W.A. Benjamin.

[14] Feynman, R.P. 1982 *Int.J.theor.Phys*. **21**,467.

[15] Gandy, R. 1980 *In The Kleene symposium* (ed. J. Barwise, H.J. Keisler & K. Kunen), pp. 123-148. Amsterdam: North Holland.

[16] Hofstadter, D.R. J 1979 *Gödel,Escher,Bach: an eternal golden braid*. New York: Random House.

[17] Leggett, A.J. 1985 In *Quantum discussions,proceedings of the Oxford quantum gravity conference* 1984 (ed.R.Penrose & C.Isham). Oxford University press.

[18] Likharev, K.K. 1982 *int.J.theor.Phys*. **21**,311.

[19] Popper, K.R. 1959 *The logic of scientific discovery*. London: Hutchinson.

[20] Toffoli, T.J. 1979 *J.Comput.Syst.Sci*. **15**, 213.

[21] Turing, A.M. 1936 *Proc.Lond.math.Soc.Ser*.2,**442**,230.

[22] Wheeler, J.A. 1985 In *NATO Advanced Study Institute Workshop on Frontiers of Nonequilibrium Physics 1984.* New York: Plenum.

ლიტერატურა

პირველ თავში გამოყენებული ლიტერატურა

1.1. М.Гери, Д.Джонсон, *Вычислительные машины и трудноpешаемые задачи*. М. Мир, 1982.
1.2. А.Китаев, А.Шень, М.Вялый. *Классические и квантовые вычисления*. М., МЦНМО, 1999.
1.3. А.И.Кострикин, Ю.И.Манин, *Линейная алгебра и геометрия*. М.,Наука,1986.
1.4. Ю.В.матиясевич, *10-я проблема Гильберта: диофантовы уравнения в XX веке*. წიგნში *Математические события XX века*. М., Фазис, 2003
1.5. P.W.Shor. Algorithms for quantum computation:Discrete log and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science.I.E.E.C. pp.124-134, 1994.
1.6. E.Rieffel, W.Polak. *An introduction to quantum computing for non-physicsts.Los alamos Physics Preprint Archive*, quant-ph/9809016.
1.7. R.Landauer. *IBM J. Resw. Develop*. 3,183, 1961.
1.8. R.Feynman. *Quantum mechanical computations*. Optics News. February 1985, N11,p.11.
1.9. C.H. Bennett. *Logical Reversibility of computation*. IBM J.Res.Dev. 6, p.525-532, 1979.
1.10. D.Deutsch. *Quantum thery, the Church-Turing principle and the universal quantum computer. Proceedings of the Royal Society of London*. Ser.A 400, pp.97-117, 1985.
1.11. P.Benioff. *Models of quantum Turing Mach*ines.Los Alamos Physics Preprint Archive, quant-ph/9708054.
1.12. E.Bernstein, U.V.Vazirani. *Quantum complexity theor*y. Society for Industrial and Applied Mathematics Journal on Computing. Vol.26, No.5, pp.1411-1473.
1.13. D.DiVincenzo. *Quantum computation*. Sciences 270, pp.255-261,1995.
1.14. A.Barenco,C.Bennett,R.Cleve,D.DiVincenzo, N.Margulus, P.Shor, T.Sleator, J.Smolin, H.Weinfurter. *Elementary gates for quantum computation*. Phys.Rev. A, 3457-3467,1995.
1.15. R.L. Rivest, A.Shamir, L.Adleman. *On digital signatures and public key cryptosystems*. Comm. ACM, vol.21, N2, pp.120-126, Feb.1978.
1.16. S.Braunstein (Ed). *Quantum Computing: where do we want to go tomorrow?* Wiley-VCH, 2000
1.17. R.Brylinski, *Universal Quantum Gates.* წიგნში *Mathematics of Quantum Computation*, Ed. R.Brylinski, G.Chen. Chapman & Hall/CRC, 2002.

მეორე თავში გამოყენებული ლიტერატურა

2.1. R.P. Feynman, Quantum mechanical computers, *Optics News*, February 1985. Reprinted in *Foundations of Physics*, Vol. 16, no. 6, 1986, pp. 507-531.

2.2. M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

2.3. Б. Б. Кадомцев. *Динамика и информация*. Редакция журнала «Успехи Физических Наук», Москва, 1997. B.B. Kadomtsev. *Dynamics andInformation.* Published by «Upekhi Fizicheskikh Nauk», Moscow, 1997.

2.4. S. Stenholm, K.-A. Suominen, *QuantumApproach to Informatics*, (John Wiley and Sons, Inc., New Jersey, 2005).

2.5. J.I. Cirac and P. Zoller. Quantum Computation with Cold trapped ions. Phys. Rev. Lett. **74**, 4094-4097, 1995.

2.6. D.F.V. James. Quantum dynamics of cold trapped ions with application to quantum computation. *Appl. Phys.* B **66,** 181-190, 1998.

2.7. D. J. Wineland, C. Monroe,W. M. Itano, D. Leibfried, B. E. King, and D. M. Meekhof, Experimental Issues in Coherent Quantum-State Manipulation of Trapped Atomic Ions, *J. Res. Natl. Inst. Stand. Technol.* **103**, 259-328 (1998).

2.8. D. Leibfried, R. Blatt, C. Monroe, D. Wineland, Quantum dynamics of single trapped ions, *Rev. Mod. Phys.*Vol.75, 281-324 (2003).

2.9. H. Häffner, C.F. Roos, R. Blatt, Quantum computing with trapped ions, Physics Reports, Vol. 469, 155-203 (2008).

2.10. L. Mandel, E. Wolf. *Optical Coherence and Quantum Optics* (Cambridge University press, 1995).

2.11. Scully M.O., and Zubairy M.S. *Quantum Optics* (Cambridge University press, Cambridge, 1997).

2.12. Delone N.B., Krainov V.P. *Atoms in Strong Light Fields* (Springer-Verlag, Berlin, Heidelberg, 1985).

2.13. Cohen-Tannoudji C., Dupont-Roc J., Grynberg G. *Atom-Photon Interactions* (WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim, 2004).

2.14. Быков В.П. Основные особенности сжатого света, *Успехи физических наук*, т. 161, 145-173 (1991).

2.15. Allen L., Eberly J.H. *Optical Resonance and Two-Level Atoms* (Wiley, New York, 1975).

2.16. Летохов В.С., Чеботаев В.П.. *Нелинейная лазерная спектроскопия сверхвысокого разрешения* (Наука, Москва, 1990).

2.17. Huges R.J., James D.F.V., Gomez J.J., Gulley M.S., Holzcheiter M.H., Kwiat P.G., Lamoreaux S.K., Peterson C.G., Sandberg V.D., Schauer M.M., Simmons C.M., Thorburn C.E., Tupa D., Wang P.Z., White A.G. The Los Alamos Trapped Ion Quantum Computer, *Fortschr. Phys.* **46**, 329-361 (1998).

სსიპ კიბერნეტიკის ინსტიტუტი
სანდრო ეულის ქ. 5, თბილისი 0186, საქართველო
ტელ. +995 32 187633; +995 32 187055.
ფაქსი +995 32 545931
ელ-ფოსტა ic@cybernet.ge, ინტერნეტ–მისამართი http://www.cybernet.ge/

G. Giorgadze, Z. Melikishvili. Quantum computations. Tbilisi, Institute of Cybernetics, 2009. In the book, quantum theory of computation is considered as an effective model for solving complicated problems. Classical and quantum description of computation processes is given, for which aim a suitable mathematical and physical tools are developed. A model of a quantum computer is constructed and one possible physical realization is indicated for it.

The book is based on the course "Quantum computations" delivered at the Tbilisi State University and on materials of a research program on the theory quantum computing which has been developed for several years at the Institute of Cybernetics and later jointly with the Laboratory of Information Technologies at the Joint Institute for Nuclear Research in Dubna.

The book can serve as an introduction to quantum computation for readers interested in this new area of science.

Authors:

G. Giorgarze – Head of the Mathematical Cybernetics Department

Z. Melikishvili – Head of the Coherent Optics and Electronics Department

Address:
Institute of Cybernetics
Sandro Euli str. 5, Tbilisi 0186, Georgia
e-mail ic@cybernet.ge