



## საქართველოს მეცნიერებათა ეროვნული აკადემია

ქართული ენციკლოპედიის ი. აბაშიძის სახელობის მთავარი სამეცნიერო რედაქცია

### კვანტური ინფორმატიკა

კვანტური ინფორმატიკა, მეცნიერების დარგი, რომელიც შეისწავლის რთული კვანტური სისტემების დინამიკის ზოგად კანონზომიერებებსა და პრინციპებს. ჩამოყალიბდა კვანტური მექანიკის, ალგორითმების თეორიისა და ინფორმაციის თეორიის მიჯნაზე. კ. ი. მოიცავს კვანტური გამოთვლებისა და კვანტური ალგორითმების საკითხებს, კვანტური კომპიუტერების ფიზიკას, კვანტურ კრიპტოგრაფიასა და ინფორმაციის კვანტურ თეორიას.

კვანტური ინფორმაცია იზომება ქუბიტებში (ინგლ. quantum bit). ქუბიტებს შეუძლია იყოს მდგომარეობაში, რ-იც 0 და 1 მნიშვნელობების სუპერპოზიციას: ნაცვლად ორი ფიქსირებული მდგომარეობისა, ქუბიტი ა ალბათობით იქნება კლასიკური 0-ის შესაბამის მდგომარეობასა (რ-იც აღინიშნება  $|0\rangle$ ) და 1-ა ალბათობით მდგომარეობაში  $|1\rangle$ , რ-იც შესაბამეა კლასიკურ 1-ს. ამას უწოდებენ კვანტურ პარალელიზმს. შესაბამისად, ქუბიტის შესაძლო მდგომარეობათა სიმრავლე კონტინუუმი.

კვანტური კომპიუტერი არის სისტემა, რ-შიც გამოთვლები ხორციელდება კვანტური მექანიკის კანონებით. ოპერაციები ამ სისტემებში, ისევე როგორც ნებისმიერ კვანტურ სისტემაში, არის უნიტარული გარდაქმნები ამ სისტემის მდგომარეობათა სივრცეში. კვანტურ კომპიუტერში არსებობს ოპერაციათა ბაზისი; მათი კომბინირებით მიიღება გამოთვლებისთვის საჭირო ყველა გარდაქმნა. გარდაქმნების (კვანტური გამოთვლების) პროცესში წარმოქმნილი მონაცემები წარმოადგენს კვანტურ ინფორმაციას, რ-იც გამოთვლის პროცესის დასრულებისას გარდაიქმნება კლასიკურ ინფორმაციად კვანტური რ ე გ ი ს ტ რ ი ს (კვანტური კომპიუტერის მეხსიერების) საბოლოო მდგომარეობის გამოშვით. გამოთვლის შედეგი, ისევე, როგორც ნებისმიერი გამოშვა კვანტურ სისტემაში, მხოლოდ გარკვეული ალბათობითაა ჭეშმარიტი (და არა ზუსტი, როგორც კლასიკურ შემთხვევაში),

მაგრამ გამოთვლების რამდენჯერმე განმეორება ამ ალბათობას ზრდის და საიმედო შედეგს გვაძლევს (ნებისმიერი სიზუსტით).

უმნიშვნელოვანესი მოვლენა, რ-საც კ. ი. შეისწავლის, არის კვანტურ მდგომარეობათა გადახლართვა (ინგლ. entangled). გადახლართვა დამახასიათებელია სისტემებისთვის, რ-ებშიც ინფორმაცია სისტემის ერთი ნაწილის მდგომარეობის შესახებ მაშინვე ცალსახად (ან ნაწილობრივ) გვაძლევს ინფორმაციას დანარჩენი ნაწილების მდგომარეობაზე, ანუ გადახლართვის შედეგად შედგენილი სისტემებისთვის დამახასიათებელია არალოკალურობა. კვანტურ სისტემებში ინფორმაცია ყოველთვის არასრულია (კლასიკური აზრით). ამიტომ კორელირებული (მაგ., მუდმივობის კანონების შედეგად ან პაულის პრინციპის შესაბამისად) ნაწილებისგან შედგენილი სისტემების მდგომარეობები გადახლართული უნდა იყოს.

1981-85 რ. ფეინმანმა (აშშ) და დ. დოიჩმა (ინგლ.) აჩვენეს, რომ გადახლართულ მდგომარეობათა არსებობა და კვანტური პარალელიზმი შეიძლება გამოვიყენოთ კომპიუტერული გამოთვლების სიჩქარის რადიკალური გაუმჯობესებისთვის. კვანტური კომპიუტერი ბევრად მძლავრი (სწრაფი და ეფექტური) იქნება კლასიკურ გამოთვლელ მონწყობილობასთან შედარებით. კვანტური გამოთვლები პრინციპულ უპირატესობას იძლევა მაგ., ნატურალური რიცხვის მარტივ თანამამრავლე ბადე და შლის პოვნისას. 1994 პ. შორმა (აშშ) შეადგინა ალგორითმი კვანტური კომპიუტერისთვის, რ-იც ამ ამოცანას სწრაფად (პოლინომურ დროში) ხსნის. ანალოგიური სწრაფი კვანტური ალგორითმი მონაცემთა ბაზაში ჩანანერის პოვნის ამოცანისთვის 1996 შეადგინა ლ. გროუვერმა (აშშ).

XXI ს. დასაწყისში კვანტური კრიპტოგრაფიული სისტემების განვითარებამ მიაღწია კომერციულ დონეს და აქტიურად გამოიყენება საიდუმლო ინფორმაციის საიმედო დაცვისათვის. მნიშვნელოვანია, რომ პრინციპულად შეუძლებელი ხდება კვანტურ მონაცემებში ფარულად შეღწევა. გადახლართულ მდგომარეობათა ტექნოლოგია გულისხმობს ათეულამდე ნაწილაკის (ან კვაზინაწილაკის - ფოტონების, ელექტრონების ან ე. წ. კუპერის წყვილები) მდგომარეობები, ელექტრონებისა და ბირთვების სპინები) გადახლართულ მდგომარეობათა საიმედო მომზადების, შედარება-შემოწმების და თვისებათა შესწავლის შესაძლებლობას. ეს რეალიზებულია ზოგიერთ მოქმედ ხელსაწყოში - კვანტური კომპიუტერის მოქმედ პროტოტიპებში [მცირეჭუბიტან (10-მდე ქუბიტი) კვანტურ პროცესორებში]. მრავალნაწილაკოვანი სისტემების კომპიუტერული მოდელირება გულისხმობს ქიმიური პროცესების და რთული სისტემების კვანტური ყოფაქცევის - (პიპოთეტურ) სიმულაციებს. ჯერჯერობით მოდელირება ხდება კვანტური კომპიუტერის მხოლოდ კლასიკური სიმულატორების გამოყენებით.

კვანტური კომპიუტერის აგების ძირითადი ტექნიკური დაბრკოლებაა დეკოჰერენტიზაციის მოვლენა - კვანტური სუპერპოზიციების დაშლა, რ-იც მიკროსისტემების მაკროსისტემებზე

გავლენის შედეგად ხდება. თუ დეკოპერენტიზაციის სინქარე არ აღემატება გარკვეულ ზღვრულ მნიშვნელობას, მაშინ შეცდომების გასწორებისათვის კვანტური კოდების გამოყენება იძლევა იმის საშუალებას (თეორიულად), რომ კვანტური სისტემა გახდეს სტაბილური. ამისთვის კვანტური რეგისტრის ზომები უნდა გაიზარდოს რამდენიმე რიგით.

ს ა ქ ა რ თ ვ ე ლ ო შ ი კ. ი-ის მიმართულებით მუშაობა მიმდინარეობს სტუ-ის კიბერნეტიკის ინსტიტუტსა (გ. გიორგაძე, ზ. მელიქიშვილი და სხვ. იკვლევენ როგორც კ. ი-ის ფუნდამენტურ პრობლემებს, ასევე მუშაობენ კვანტური კომპიუტერის ფიზიკური რეალიზაციის შესაძლებლობაზე) და ნ. მუსხელიშვილის სახ. გამოთვლითი მათემატიკის ინ-ტში (ვ. კვარაცხელია და სხვ.), თსუ-ის ი. ვეკუას სახ. გამოყენებითი მათემატიკის ინ-ტში ეფექტური ალგორითმების შედგენაზე მუშაობს თ. ვაშაყმაძე, ზუსტი და საბუნებისმეტყველო მეცნ. ფაკ-ტზე – ა. კვინიხიძე და სხვ. ინტენსიურად მიმდინარეობს ერთობლივი კვლევები საზღვარგარეთის წამყვან ცენტრებთან.

ლიტ.: გ ი ო რ გ ა ძ ე გ., მ ე ლ ი ქ ი შ ვ ი ლ ი ზ., კვანტური გამოთვლები, თბ., 2009; Я к о в л е в В. П., Квантовая информатика, М., 2008.

**გ. გიორგაძე**

---