KVANT HISOBLASH: KELAJAK TEXNOLOGIYASINING ASOSI

Toshkent viloyati Olmaliq shahar
7-U.O'.T. M fizika fan o'qituvchisi
Negmatullayeva Nazima Karimovna

Annotatsiya: Ushbu maqolada kvant hisoblash – bu zamonaviy fizika va axborot texnologiyalarining eng qiziqarli sohalaridan biri bo‘lib, klassik kompyuterlar chegaralaridan tashqariga chiqish imkonini beradi. Ushbu maqolada kvant kompyuterlarining ishlash prinsiplari, ularning asosiy tarkibiy qismlari – kubitlar (kvant bitlari), superpozitsiya va kvant aloqasi (entanglement) kabi muhim tushunchalar tushuntiriladi. Bundan tashqari, kvant hisoblashning kriptografiya, sun’iy intellekt, tibbiyot va modellashtirish sohalarida qo‘llanilishi, shuningdek, ushbu texnologiyaning kelajakdagi istiqbollari va qiyinchiliklari haqida so‘z boradi.

Kalit so‘zlar: Kvant kompyuteri, kubit (kvant biti), superpozitsiya, kvant aloqasi (entanglement), kvant algoritmlari, shor algoritmi, Grover algoritmi, kvant kriptografiyasi, kvant hisoblashning amaliy qo‘llanilishi, klassik va kvant hisoblash farqlari, kvant ustunlik (quantum supremacy), noise (kvant shovqinlari) va dekogerentsiya, kvant dasturlash tillari (Qiskit, Cirq), kvant simulyatsiyasi, kvant tarmoqlari (quantum internet)

Annotation: This article introduces quantum computing, one of the most exciting areas of modern physics and information technology, which allows us to go beyond the boundaries of classical computers. This article explains the principles of operation of quantum computers, their main components - qubits (quantum bits), superposition and quantum entanglement. In addition, we will discuss the applications of quantum computing in cryptography, artificial intelligence, medicine and modeling, as well as the future prospects and challenges of this technology.

Key words: quantum computer, qubit (quantum bit), superposition, quantum entanglement, quantum algorithms, Shor's algorithm, Grover's algorithm, quantum cryptography, practical applications of quantum computing, differences between classical and quantum computing, quantum supremacy, noise and decoherence, quantum

programming languages (Qiskit, Cirq), quantum simulation, quantum networks (quantum internet)

Аннотация: В этой статье квантовые вычисления рассматриваются как одно из самых интересных направлений современной физики и информационных технологий, позволяющее нам выйти за рамки классических компьютеров. В статье объясняются принципы работы квантовых компьютеров, их основные компоненты — кубиты (квантовые биты), суперпозиция и квантовая запутанность. Кроме того, будут обсуждаться применение квантовых вычислений в криптографии, искусственном интеллекте, медицине и моделировании, а также будущие перспективы и проблемы этой технологии.

Ключевые слова: Квантовый компьютер, кубит (квантовый бит), суперпозиция, квантовая запутанность, квантовые алгоритмы, алгоритм Шора, алгоритм Гровера, квантовая криптография, практическое применение квантовых вычислений, различия между классическими и квантовыми вычислениями, квантовое превосходство, шум и декогеренция, квантовые языки программирования (Qiskit, Cirq), квантовое моделирование, квантовые сети (квантовый интернет)

Kirish. Zamonaviy texnologik taraqqiyot insoniyatni yangi ilmiy bosqichlarga olib chiqmoqda. Ayniqsa, kompyuter texnologiyalarida kuzatilayotgan yuksalishlar, sun’iy intellekt va ma’lumotlar bilan ishlash sohasidagi ilg‘or yondashuvlar bilan chambarchas bog‘liq. Shunday yo‘nalishlardan biri bu — kvant hisoblash bo‘lib, u an’anaviy kompyuter texnologiyalariga nisbatan tubdan farq qiluvchi ishlash mexanizmi va imkoniyatlarga ega.

Kvant hisoblash — bu kvant mexanikasi qonunlariga asoslangan axborotni qayta ishlash texnologiyasi bo‘lib, murakkab matematik muammolarni, katta hajmdagi ma’lumotlarni va modellashtirish jarayonlarini an’anaviy kompyuterga qaraganda tezroq va samaraliroq bajarishga qodir. Dastlab fundamental fizika doirasida nazariy tushuncha sifatida vujudga kelgan ushbu soha, bugungi kunda global miqyosda raqobat va izlanish markaziga aylangan.

Kvant hisoblash texnologiyasining rivojlanishi — kriptografiya, farmatsevtika, sun’iy intellekt, modellashtirish, iqlim o‘zgarishini bashorat qilish kabi ko‘plab strategik yo‘nalishlarda inqilobiy burilishlar qilishga imkon beradi. Shu sababli, mazkur maqolada kvant hisoblashning nazariy asoslari, texnologik afzalliklari hamda kelajakdagi amaliy qo‘llanilishi masalalari yoritiladi.

Mavzuga oid adabiyotlar. Nielsen, M.A., Chuang, I.L. (2010). *Quantum Computation and Quantum Information*. — Cambridge University Press. “Kvant hisoblashning nazariy asoslari, kubitlar, superpozitsiya, kvant algoritmlari haqida keng qamrovli darslik”. Shor, P.W. (1997). *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*. — SIAM Journal on Computing, 26(5), 1484–1509. “Shor algoritmi orqali kvant kompyuterlarning kriptografiyadagi ustunligi isbotlangan ilmiy maqola”. Afzalov M., Normurodov S. (2022). *Kvant texnologiyalari va axborot xavfsizligi*. — Toshkent: Fan nashriyoti. “O‘zbekistonda kvant hisoblash va kriptografiya bo‘yicha yozilgan ilmiy-amaliy qo‘llanma”. Jalolov M. (2023). *Kvant hisoblash asoslari: o‘zbek tilidagi izohli qo‘llanma*. — Toshkent: Ilm-Ziyo.” Mahalliy auditoriyaga mo‘ljallangan, kubitlar va kvant aloqasi haqida amaliy izohlar”. Kvant xavfsizlik, post-quantum cryptography bo‘yicha xalqaro tadqiqotlar manbai. Kvant algoritmlari va matematik modellarga asoslangan o‘quv qo‘llanma. Nilsen va Chuangning ta’kidlashicha: kvant hisoblash klassik hisoblash nazariyasiga qaraganda ancha murakkab va kuchliroq hisoblash modelidir, ayniqsa superpozitsiya va entanglement (kvant chirmashuvi) orqali axborotni qayta ishlashda muhim ahamiyat kasb etadi[1]

Tadqiqot metodologiyasi. Bugungi axborot asrida hisoblash tizimlari hayotimizning ajralmas bo‘lagiga aylanib ulgurgan. Biroq an’anaviy kompyuter texnologiyalari murakkab matematik hisob-kitoblar, katta hajmdagi ma’lumotlarni qayta ishlash yoki zamonaviy kriptografiyani buzish kabi masalalarda cheklovlarga ega. Aynan shu nuqtada, yaqin kelajak texnologiyalarining asosi sifatida kvant hisoblash konsepsiyasi ilgari surilmoqda. Kvant kompyuteri — bu ma’lumotni qayta ishlashda klassik bitlar o‘rniga

[1] Nielsen M.A., Chuang I.L. Kvant hisoblash va kvant axborot. — Cambridge: Cambridge University Press, 2010.

kubitlar (quantum bits) dan foydalanadigan qurilmadir. Kubitlarning asosiy xususiyati shundaki, ular superpozitsiya holatida bo‘lib, ya’ni 0 va 1 holatlarni bir vaqtda ifodalay oladi. Bu esa kvant kompyuterlariga murakkab masalalarni parallel ravishda hisoblash imkonini beradi.

Bundan tashqari, kvant aloqasi (quantum entanglement) tushunchasi orqali kvant zarrachalari orasida masofadan qat’iy nazar real vaqtli aloqani ta’minlash mumkin bo‘ladi. Bu hodisa kvant kompyuterlari va kvant kriptografiyasi uchun tamoman yangi, yuqori darajadagi xavfsizlik tizimlarini yaratish imkonini beradi. Kvant hisoblash sohasidagi muhim yutuqlardan biri bu — Shor algoritmi bo‘lib, u an’anaviy kompyuterlar uchun juda murakkab bo‘lgan sonlarni faktorizatsiya qilish masalasini kvant hisoblash orqali tezda yechishga imkon beradi. Bu esa mavjud kriptografik tizimlar uchun jiddiy tahdid, shu bilan birga, yangi imkoniyatlar demakdir. Mazkur maqolada kvant hisoblashning asosiy tamoyillari, afzalliklari va global texnologik inqilobdagi o‘rni yoritiladi. Shuningdek, kvant kompyuterlarining kelajakdagi qo‘llanilishi, xavfsizlik, algoritmlar va amaliyotda qo‘llanilishiga doir fikrlar tahlil qilinadi.

Tahlil va natijalar. Kvant hisoblash — bu klassik hisoblashning chegaralarini kengaytirishga qaratilgan, fizikadagi kvant nazariyasiga asoslangan mutlaqo yangi paradigmadir. Bugungi texnologik rivojlanish shiddati fonida, ayniqsa, sun’iy intellekt, katta hajmdagi ma’lumotlarni qayta ishlash (Big Data), kriptografiya va simulyatsiya sohalarida kvant kompyuterlariga bo‘lgan ehtiyoj keskin ortmoqda.

Tahlillar shuni ko‘rsatmoqdaki:

1. Kubitlar va superpozitsiya orqali axborotni bir vaqtning o‘zida bir nechta holatda saqlash va hisoblash imkoniyati kvant kompyuterlarning hisoblash kuchini sezilarli darajada oshiradi. Bu klassik kompyuterlarda yillar davom etadigan hisob-kitoblarni soniyalar ichida amalga oshirish imkonini beradi.

2. Shor algoritmi orqali raqamlarni faktorizatsiya qilish muammosining kvant yechimi mavjud kriptografik tizimlar uchun real xavf tug‘diradi. Bu esa post-kvant xavfsizlikka tayyorlanishni taqozo etadi.

3. Kvant aloqasi (entanglement) esa xavfsiz va nazorat qilinmaydigan axborot uzatish texnologiyalarini joriy etish imkonini beradi. Bu kelajakda kvant internetining shakllanishi uchun zamin yaratadi.

4. So‘nggi yillarda Google, IBM, Microsoft, Amazon kabi texnologik gigantlarning kvant kompyuterlar yaratish borasidagi sa’y-harakatlari ushbu sohaning yaqin kelajakda keng qo‘llanilishini bashorat qilish imkonini bermoqda.

5. O‘zbekiston ilm-fanida ham bu yo‘nalish bo‘yicha dastlabki qadamlar qo‘yilmoqda. Mahalliy olimlar tomonidan kvant texnologiyalari va axborot xavfsizligi yo‘nalishida maqolalar va o‘quv qo‘llanmalar yaratilmoqda.

Xulosa sifatida aytish mumkinki, kvant hisoblash bugungi va ertangi kunning texnologiyasi bo‘lib, u nafaqat hisoblash imkoniyatlarini tubdan o‘zgartiradi, balki butun axborot xavfsizligi, kommunikatsiya, modellashtirish va ilmiy tadqiqotlar sohasida yangi bosqichni boshlab beradi. Ilmiy salohiyatni oshirish, yosh avlodni ushbu soha bilan tanishtirish va milliy texnologik mustaqillikni ta’minlash uchun kvant texnologiyalarini rivojlantirish strategik ahamiyatga ega. Shor algoritmi shuni nazarda tutadiki, kvant kompyuterlarning real kuchini namoyish etgan birinchi misollardan biridir. [2]U klassik kompyuterlar uchun juda murakkab bo‘lgan sonlarni faktorizatsiya qilish masalasini polynomial vaqt ichida hal qilishga imkon beradi Kvant hisoblash zamonaviy texnologik taraqqiyotning eng istiqbolli yo‘nalishlaridan biridir. Ushbu texnologiya klassik kompyuterlar hal qila olmaydigan murakkab masalalarning yechimida, ayniqsa, raqamli xavfsizlik, sun’iy intellekt, biotexnologiya va moliyaviy model tizimlarida katta inqilob qilish imkoniyatiga ega. Tadqiqot natijalari shuni ko‘rsatadiki, kvant kompyuterlar yordamida:

- hisoblash jarayoni sezilarli darajada tezlashadi;

[2] Shor P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM J. on Computing. — 1997. — Vol. 26, No. 5. — P. 1484–1509

- klassik kriptotizimlar zaiflashadi va yangi — post-kvant kriptografiyasi zarur bo‘ladi;

- kvant aloqasi orqali xavfsiz axborot uzatish yo‘llari yuzaga keladi;

- ilm-fan va ishlab chiqarishdagi modellash va prognozlash masalalari samarali yechim topadi.

O‘zbekiston oliy ta’lim muassasalarida kvant hisoblashga oid alohida kurslar va magistratura yo‘nalishlari joriy etilishi lozim, mahalliy olimlar va dasturchilarni kvant dasturlash, algoritmlar va texnologiyalar bilan shug‘ullanishga jalb etish va grant asosida ilmiy loyihalarni moliyalashtirish taklif etiladi. Xalqaro tajribani o‘rganish maqsadida yirik texnologik kompaniyalar (IBM, Google, Microsoft) bilan hamkorlik aloqalari o‘rnatilishi maqsadga muvofiq.

Foydalanilgan adabiyotlar ro‘yxati

1. Yanofsky, N.S., Mannucci, M.A. (2008). *Quantum Computing for Computer Scientists*. — Cambridge University Press.

2. Kaye, P., Laflamme, R., Mosca, M. (2007). *An Introduction to Quantum Computing*. — Oxford University Press.

3. Gruska, J. (1999). *Quantum Computing*. — McGraw-Hill.

4. Oskin, M., Chong, F.T., Kubiatowicz, J. (2002). *A Practical Architecture for Reliable Quantum Computers*. — IEEE Computer.

5. Deutsch, D. (1985). *Quantum theory, the Church–Turing principle and the universal quantum computer*.

6. Moqutov A. (2022). *Kvant informatika: Dastlabki tushunchalar*. — Samarqand: Zarafshon nashriyoti

7. National Institute of Standards and Technology (NIST) – https://www.nist.gov/

8. Microsoft Quantum Documentation – https://learn.microsoft.com/en-us/azure/quantum/