



DOI

10.66073/ReFocus-Conf/
0910248



QR-kod
maqolaning DOI
sahifasini
ochadi

SAHIFALAR

1210–1214

TIL

O'zbek

IQTIBOS UCHUN

Saparova Aysanem Ajiniyazovna.
Raqamli texnologiyalar va sun'iy
intellekt tizimlarida qo'llaniladigan
zamonaviy algebraik tuzilmalar va
algoritmalar // «O'zbekiston olimi
ayollarining mamlakat taraqqiyotiga
qo'shayotgan hissasi» mavzusidagi
xalqaro ilmiy-amaliy konferensiya
materiallari (Nukus, 2026-yil 9–10-
oktyabr). – Nukus, 2026. – B. 1210–
1214. – DOI: [https://doi.org/](https://doi.org/10.66073/ReFocus-Conf/0910248)
10.66073/ReFocus-Conf/0910248



«O'zbekiston olimi ayollarining
mamlakat taraqqiyotiga
qo'shayotgan hissasi»

XALQARO ILMIY-AMALIY
KONFERENSIYA
NUKUS, 9–10-OKTYABR 2026

RAQAMLI TEXNOLOGIYALAR VA SUN'IY INTELLEKT TIZIMLARIDA QO'LLANILADIGAN ZAMONAVIY ALGEBRAIK TUZILMALAR VA ALGORITMLAR

Saparova Aysanem Ajiniyazovna

*Qoraqalpoq davlat universiteti, Matematika fakulteti,
Matematik tahlil kafedrası, assistent o'qituvchisi
E-mail: saparovaaysanem09@gmail.com*

Annotatsiya: Maqolada raqamli texnologiyalar va sun'iy intellekt (SI) tizimlarining matematik asosini tashkil etuvchi zamonaviy algebraik tuzilmalar hamda ular bilan bog'liq algoritmalar tahlil qilinadi. Tadqiqotda gruppalar, halqalar, chekli maydonlar, vektor fazolari, matritsalar va Boolean algebra kabi tuzilmalarning hisoblash jarayonlaridagi o'rni tizimli ravishda ko'rib chiqildi. Ayniqsa, chekli maydonlar asosidagi amallar kriptografiya va xatolarni tuzatuvchi kodlarda, matritsa va vektor fazolari esa mashinaviy o'rganish modellarida ma'lumotlarni ifodalash hamda transformatsiya qilishda muhim ekanligi asoslandi. Algebraik algoritmalarining afzalligi ularning aniq formal qoidalarga tayangan holda katta hajmdagi ma'lumotlar bilan takrorlanuvchi va avtomatlashtiriladigan hisoblashlarni amalga oshirish imkonini berishidir. Ishda algebraik tuzilma–algoritm–amaliy vazifa bog'lanishini ko'rsatuvchi tizimli model taklif etilib, raqamli texnologiyalar va SI tizimlarini ishlab chiqishda matematik abstraksiyalardan foydalanish yo'nalishlari umumlashtirildi.

Kalit so'zlar: algebraik tuzilmalar, gruppalar, halqa, chekli maydon, vektor fazosi, matritsa, Boolean algebra, algoritm, sun'iy intellekt, mashinaviy o'rganish, kriptografiya, kodlash nazariyasi.

Kirish (adabiyotlar sharhi)

Raqamli transformatsiyaning jadallashuvi hisoblash jarayonlarini faqat dasturiy vositalar darajasida emas, balki ularning matematik asoslarini ham chuqur o'rganishni talab etmoqda. Zamonaviy raqamli tizimlarda ma'lumotlarni kodlash, uzatish, himoyalash, tasniflash va transformatsiya qilish kabi vazifalar qat'iy matematik operatsiyalar orqali bajariladi. Shu nuqtai nazardan algebraik tuzilmalar algoritmalarining barqarorligi, takrorlanuvchanligi va formal tekshiriluvchanligini ta'minlaydigan muhim vositalardan biri hisoblanadi.

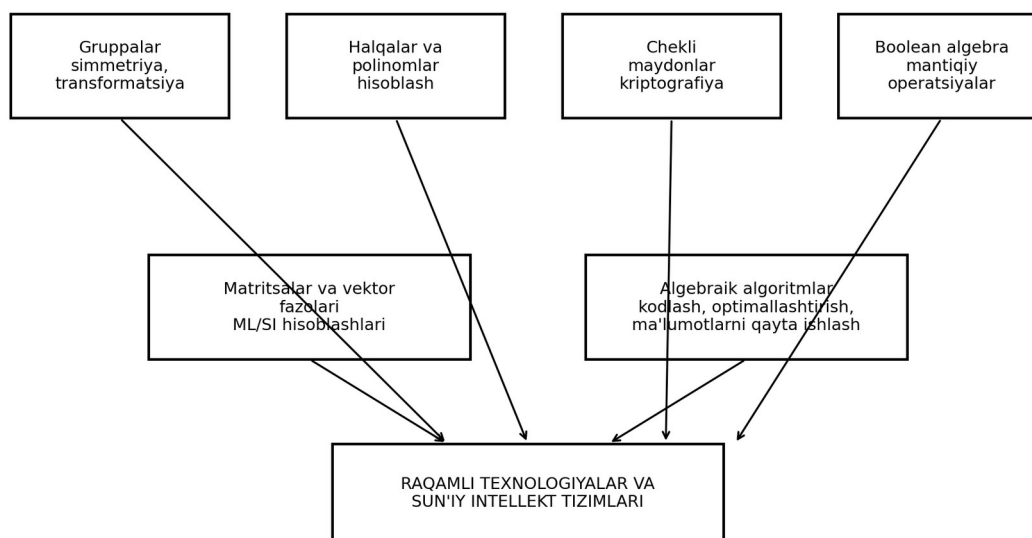
Zamonaviy kriptografiya nazariyasida gruppalar, halqalar va chekli maydonlar asosiy matematik apparat sifatida qo'llanadi. Underwood zamonaviy kriptografiyaning algebra, sonlar nazariyasi va murakkablik nazariyasi bilan uzviy bog'liqligini ko'rsatadi [1]. Chekli maydonlar arifmetikasi esa kriptografiya, kodlash nazariyasi va axborot xavfsizligi masalalarida keng qo'llanadi [2]. 2023-yilda e'lon qilingan tadqiqotlarda polinom halqalari, chekli maydonlar va matritsalar kriptografik primitivlarning algebraik xususiyatlarini tahlil qilishda ishlatilishi ko'rsatilgan [3].

SI tizimlarida esa algebraik yondashuvlar ma'lumotlarni vektor va matritsa ko'rinishida ifodalash, chiziqli transformatsiyalarni bajarish, parametrlarni optimallashtirish va mantiqiy qarorlarni formal ifodalash bilan bog'liq. Shu sababli algebraik tuzilmalarni faqat nazariy matematika obyekti sifatida emas, balki zamonaviy hisoblash tizimlarining amaliy komponenti sifatida o'rganish dolzarbdir.

Materiallar va uslublar

Tadqiqotning metodologik asosini algebraik tuzilmalar va algoritmlarning raqamli texnologiyalar hamda SI tizimlaridagi qo'llanishini tizimli tahlil qilish tashkil etdi. Adabiyotlarni tahlil qilish, taqqoslash, formalizatsiya, abstraksiyalash va strukturaviy modellashtirish usullaridan foydalanildi. Asosiy e'tibor quyidagi tuzilmalarga qaratildi: gruppalar, halqalar, chekli maydonlar, vektor fazolari, matritsalar va Boolean algebra.

Algebraik yondashuvda har bir amaliy masala uch bosqichda ko'rib chiqildi: 1) ma'lumot yoki jarayonni mos algebraik tuzilma orqali ifodalash; 2) masalaga mos algoritmik amalni tanlash; 3) hosil bo'lgan natijani raqamli tizimning amaliy vazifasiga mos talqin qilish. Bunday yondashuv turli sohalaridagi algoritmlarni yagona matematik nuqtai nazardan taqqoslash imkonini beradi.



1-rasm. Algebraik tuzilmalar va ularning raqamli texnologiyalar hamda SI tizimlaridagi funksional bog'lanishi

Natijalar

Tahlil natijasida algebraik tuzilmalarning raqamli texnologiyalardagi vazifalari o'zaro farqlanishi aniqlandi. Gruppalar simmetriya va qayta tashkil etish operatsiyalarini formal ifodalashga qulay bo'lsa, halqalar va polinomlar algebraik hisoblashlar, kodlash va kriptografik konstruksiyalarda muhim o'rin egallaydi. Chekli maydonlar esa elementlari soni chekli bo'lgan aniq algebraik muhitni yaratib, raqamli hisoblashlarda modulli operatsiyalarni samarali bajarish imkonini beradi.

Vektor fazolari va matritsalar SI tizimlarida alohida ahamiyatga ega. Mashinaviy o'rganishdagi ko'plab amallar kiruvchi ma'lumotlarni vektor sifatida ifodalash, ularni matritsalar orqali o'zgartirish va natijaviy vektorlarni hisoblashga borib taqaladi. Masalan, chiziqli qatlam uchun $y = Wx + b$ ifodasi matritsa va vektorlar ustidagi algebraik operatsiyalarni ifodalaydi. Bu modelning o'zi barcha SI usullarini qamrab olmasa-da, ko'plab neyron tarmoq hisoblashlarining asosiy algebraik komponentini ko'rsatadi.

Boolean algebra raqamli qurilmalar va mantiqiy algoritmlarda 0 va 1 qiymatlar ustidagi amallarni formal ifodalashga xizmat qiladi. AND, OR va NOT operatsiyalari orqali mantiqiy shartlar, raqamli sxemalar va ayrim qaror qabul qilish jarayonlari modellashiriladi. Shu bilan birga, algebraik strukturalar dasturiy ta'minotdagi ma'lumot turlarini qat'iy belgilash, formal verifikatsiya va kriptografik protokollarni tahlil qilish uchun ham nazariy asos beradi.

1-jadval. Zamonaviy algebraik tuzilmalarning raqamli texnologiyalar va SI tizimlaridagi asosiy qo'llanishlari

Algebraik tuzilma	Asosiy operatsiya	Algoritmik qo'llanish	Amaliy yo'nalish
Gruppa	Kompozitsiya, teskari element	Transformatsiyalar va simmetriya algoritmlari	Kriptografiya, kombinatorika
Halqa/polinom halqasi	Qo'shish va ko'paytirish	Polinomlar bilan hisoblash, algebraik modellash	Kodlash, kriptografiya
Chekli maydon	Maydon arifmetikasi	Modulli va chekli arifmetik algoritmlar	Kriptografiya, kodlash
Vektor fazosi/matritsa	Chiziqli kombinatsiya, matritsa ko'paytmasi	Transformatsiya, optimallashtirish, parametrlar hisoblash	SI, mashinaviy o'rganish
Boolean algebra	AND, OR, NOT	Mantiqiy ifodalarni hisoblash	Raqamli tizimlar, qaror qabul qilish

Jadvalda, algebraik tuzilmalar bitta alohida texnologiya bilan cheklanmaydi. Ularning har biri muayyan turdagi hisoblashni formal va izchil tashkil etishga imkon beradi. Masalan, chekli maydon arifmetikasi kriptografik algoritmlarda ma'lumotlarni cheklangan algebraik muhitda qayta ishlash uchun zarur bo'lsa, vektor fazolari va matritsalar katta o'lchamli ma'lumotlarni SI modellariga uzatishning tabiiy matematik shaklini beradi.

Algebraik algoritmlarning muhim xususiyati — ularning aniqligi va formal qoidalarga bo'ysunishidir. Algoritmning har bir bosqichi algebraik amal sifatida ifodalanishi mumkin bo'lsa, hisoblashning to'g'riligini tekshirish, murakkabligini baholash va dasturiy realizatsiyasini standartlashtirish osonlashadi. Chekli maydonlar bo'yicha zamonaviy tadqiqotlarda samarali ko'paytirish, polinomlar bilan ishlash va kriptografik qo'llanishlar alohida yo'nalish sifatida o'rganilmoqda [2].

Kriptografik primitivlarda algebraik yondashuvning yana bir jihati — chiziqli va nochiziqli transformatsiyalarni formal tavsiflash imkoniyatidir. Subroto tomonidan taklif etilgan algebraik yondashuvda polinom halqalari, chekli

maydonlar va matritsaviy konstruksiyalar simmetrik kriptografik qatlamlarni tahlil qilishda qo'llangan [3]. Bu natija algebraik strukturalarning raqamli xavfsizlik bilan bog'liqligini ko'rsatadi.

SI tizimlarida esa algebraik algoritmlarning qo'llanishi ma'lumotlarni matematik fazoga o'tkazishdan boshlanadi. Belgilar, tasvirlar, sensor ma'lumotlari yoki boshqa obyektlar sonli vektorlar ko'rinishida ifodalangach, ularning o'zaro munosabati matritsa va vektor operatsiyalari orqali qayta ishlanadi. Shunday qilib, algebraik model SI tizimining yuqori darajadagi algoritmlariga matematik tayanch vazifasini bajaradi.

Muhokama

Tadqiqot natijalari zamonaviy algebraik tuzilmalar va algoritmlarni raqamli texnologiyalar hamda SI tizimlarida uchta asosiy qatlamda ko'rish mumkinligini ko'rsatadi: ma'lumotlarni ifodalash, hisoblashni bajarish va natijani tekshirish. Birinchi qatlamda vektorlar, matritsalar va Boolean qiymatlar ustunlik qilsa, ikkinchi qatlamda maydon, halqa va gruppamallari qo'llanadi. Uchinchi qatlamda esa algebraik xossalardan foydalanib, algoritmning izchilligi va formal to'g'riligi tahlil qilinadi.

Shuningdek, algebraik yondashuvlar katta hajmdagi ma'lumotlarni qayta ishlashda algoritmlarning samaradorligini baholash uchun ham muhimdir. Amaliy tizimlarda faqat matematik jihatdan to'g'ri algoritm yetarli emas; uning hisoblash murakkabligi, xotira talabi va parallel bajarilish imkoniyati ham hisobga olinadi. Shu sababli kelgusidagi tadqiqotlarda algebraik tuzilmaning nazariy xossalari bilan bir qatorda algoritmning hisoblash murakkabligini ham birgalikda o'rganish maqsadga muvofiq.

Alohida istiqbolli yo'nalish — algebraik usullarni SI modellarining ishonchliligi va formal tekshirilishi bilan bog'lashdir. Algebraik ifodalar orqali ayrim transformatsiyalarni formal tavsiflash, cheklovlarni ifodalash va hisoblash jarayonini nazorat qilish mumkin. Bunday yondashuv SI tizimlarining shaffofligi va tekshiriluvchanligini oshirishga xizmat qilishi mumkin, biroq uning amaliy samarasi tanlangan model va masala turiga bog'liq.

Xulosa va tavsiyalar

Zamonaviy algebraik tuzilmalar raqamli texnologiyalar va sun'iy intellekt tizimlarining matematik poydevorlaridan biridir. Tadqiqotda gruppalar, halqalar, chekli maydonlar, vektor fazolari, matritsalar va Boolean algebra kabi tuzilmalarning raqamli hisoblashdagi funksiyalari umumlashtirildi. Natijalar shuni ko'rsatdiki, chekli maydonlar va polinomlar kriptografiya hamda kodlash masalalarida, vektor fazolari va matritsalar SI hisoblashlarida, Boolean algebra esa mantiqiy va raqamli jarayonlarda muhim ahamiyatga ega.

Amaliy nuqtai nazardan, oliy ta'limda algebra fanlarini raqamli texnologiyalar va SI misollariga bog'lab o'qitish, algebraik algoritmlarning dasturiy realizatsiyasini ko'rsatish hamda ularning hisoblash murakkabligini taqqoslash tavsiya etiladi. Kelgusida chekli maydonlar, polinomlar va matritsalar asosidagi algoritmlarning SI, kriptografiya va raqamli signalni qayta ishlashdagi samaradorligini tajribaviy baholash istiqbolli yo'nalish hisoblanadi.

Foydalanilgan adabiyotlar

1. Underwood R. G. Cryptography for Secure Encryption. Cham: Springer, 2022. 302 p. DOI: 10.1007/978-3-030-97902-7.
2. Mesnager S., Zhou Z. (eds.). Arithmetic of Finite Fields: 9th International Workshop, WAIFI 2022, Revised Selected Papers. Cham: Springer, 2023. 349 p. DOI: 10.1007/978-3-031-22944-2.
3. Subroto R. C. An algebraic approach to symmetric linear layers in cryptographic primitives // Cryptography and Communications. 2023. Vol. 15. P. 1053–1067. DOI: 10.1007/s12095-023-00630-w.
4. Aggarwal D., Döttling N., Dujmovic J., Hajiabadi M., Malavolta G., Obremski M. et al. Algebraic Restriction Codes and Their Applications // Algorithmica. 2023. Vol. 85. P. 3602–3648. DOI: 10.1007/s00453-023-01150-y.
5. Abdurazzokov J. S-Box Generation Algorithm by Constructing the Non-Singular Adjacency Matrix Using the Genetic Algorithm // American Journal of Science, Engineering and Technology. 2024. Vol. 9, No. 1. P. 1–8.
6. Borges J., Fernández-Córdoba C., Pujol J., Rifà J., Villanueva M. Z2Z4-Linear Codes. Cham: Springer, 2022. 245 p. DOI: 10.1007/978-3-031-05441-9.