

GALUA NAZARIYASINING SUN'IIY INTELLEKT VA KVANT HISOBLASHDAGI ISTIQBOLLARI

Xolov Komil Normamatovich

dotsent,

Axborot texnologiyalari va menejment universiteti,

O'zbekiston, Qarshi shahri

Bobilov Nodirbek Xolturayevich

katta o'qituvchi,

Axborot texnologiyalari va menejment universiteti,

O'zbekiston, Qarshi shahri

Jo'rayeva Sitara Muqim qizi

magistrant,

Axborot texnologiyalari va menejment universiteti,

O'zbekiston, Qarshi shahri.

Annotatsiya: Mazkur maqolada Galua nazariyasining sun'iy intellekt, kvant hisoblash va kriptografiyadagi istiqbollari tahlil qilinadi. Chekli maydonlar va algebraik strukturalarning zamonaviy hisoblash tizimlaridagi o'rni yoritiladi.

Аннотация: В статье анализируются перспективы теории Галуа в области искусственного интеллекта, квантовых вычислений и криптографии. Рассматривается роль конечных полей и алгебраических структур в современных вычислительных системах.

Abstract: This article analyzes the prospects of Galois theory in artificial intelligence, quantum computing, and cryptography. The role of finite fields and algebraic structures in modern computational systems is discussed.

Kalit so'zlar: Galua nazariyasi, chekli maydonlar, sun'iy intellekt, kvant hisoblash, kriptografiya.

Ключевые слова: теория Галуа, конечные поля, искусственный интеллект, квантовые вычисления, криптография.

Keywords: Galois theory, finite fields, artificial intelligence, quantum computing, cryptography.

Introduction (Kirish)

Galua nazariyasi zamonaviy algebraning fundamental yo'nalishlaridan biri bo'lib, algebraik tenglamalarni gruppalar va maydon kengaytmalari



orqali o'rganadi. Ushbu nazariya polinom tenglamalar va algebraik strukturalar o'rtasidagi chuqur bog'liqlikni ochib beradi.

So'nggi yillarda Galua nazariyasining sun'iy intellekt, kriptografiya, kodlash nazariyasi va kvant hisoblash sohalaridagi ahamiyati ortib bormoqda. Ayniqsa chekli maydonlar va algebraik strukturalar axborot xavfsizligi, xatolarni tuzatish tizimlari hamda murakkab hisoblash jarayonlarida keng qo'llanilmoqda.

Mazkur maqolada Galua nazariyasining sun'iy intellekt va kvant hisoblashdagi istiqbollari, shuningdek chekli maydonlarning zamonaviy hisoblash tizimlaridagi o'rni tahlil qilinadi.

Methods (Metodlar)

Mazkur tadqiqotda Galua nazariyasi va unga bog'liq algebraik strukturalarni o'rganishda nazariy, tahliliy va qiyosiy metodlardan kompleks foydalanildi. Tadqiqotning asosiy yondashuvi abstrakt algebra prinsiplari asosida shakllantirildi, bunda gruppalar nazariyasi, maydonlar nazariyasi va chekli maydonlar xossalari tizimli ravishda tahlil qilindi.

Nazariy qismda Galua nazariyasining asosiy tushunchalari - maydon kengaytmalari, Galua gruppalari va keltirilmaydigan polinomlar - matematik strukturaviy yondashuv asosida o'rganildi. Ushbu bosqichda algebraik tenglamalarning yechiluvchanligi va simmetrik xossalari tahlil qilindi.

Tahliliy qismda chekli maydonlar $GF(p)$ va $GF(p^n)$ ning algebraik xossalari hamda ularning kodlash nazariyasi va kriptografiyadagi o'rni o'rganildi. Reed-Solomon va BCH kodlari hamda RSA, AES va ECC algoritmalarining matematik asoslari strukturaviy jihatdan tahlil qilindi.

Shuningdek, simvolik hisoblash usullari qo'llanilib, Galua maydonlaridagi algebraik amallarni avtomatik bajarish imkoniyatlari o'rganildi. Maple, Mathematica va SageMath kabi kompyuter algebra tizimlari yordamida polinomlar ustida amallar, faktorizatsiya jarayonlari va maydon elementlari bilan ishlash modellashtirildi.

Qiyosiy tahlil metodida kriptografik va kodlash tizimlarining samaradorligi, xavfsizlik darajasi va hisoblash murakkabligi solishtirildi. Ushbu yondashuv turli algoritmlar orasidagi matematik farqlarni aniqlash va ularning amaliy qo'llanish sohalarini baholash imkonini berdi.

Umuman olganda, tadqiqotda qo'llanilgan metodlar Galua nazariyasini nazariy va amaliy jihatdan chuqur o'rganishga hamda uning zamonaviy informatika tizimlaridagi o'rnini asoslashga xizmat qildi.



Results (Natijalar)

Tadqiqot davomida Galua nazariyasining zamonaviy hisoblash tizimlaridagi o'rni tahlil qilindi. Olingan natijalar shuni ko'rsatadiki, chekli maydonlar va algebraik strukturalar kriptografiya, kodlash nazariyasi hamda simvolik hisoblash tizimlarining asosiy matematik bazasini tashkil etadi.

Kriptografik algoritmlar tahlili natijasida RSA, AES va ECC turli matematik muammolarga asoslanganligi aniqlandi. Ularning xavfsizlik va hisoblash samaradorligi quyidagi tarzda farqlanadi:

Kriptografik algoritmlar taqqoslash

Algoritm	Matematik asos	Xavfsizlik darajasi	Tezlik	Kalit uzunligi
RSA	Sonlar nazariyasi	Yuqori	Nisbatan sekin	Katta
AES	Galua maydoni $GF(2^8)$	Juda yuqori	Juda tez	O'rtacha
ECC	Elliptik egri chiziqlar	Juda yuqori	Tez	Kichik

Jadvaldan ko'rinadiki, AES va ECC algoritmlari Galua maydonlari va algebraik strukturalardan samarali foydalanishi sababli zamonaviy tizimlarda yuqori samaradorlikka ega.

Simvolik hisoblash tizimlari (Maple, Mathematica, SageMath) yordamida Galua maydonlarida amallar bajarilishi tahlil qilindi. Natijalar shuni ko'rsatdiki, ushbu tizimlar polinomlarni faktorizatsiya qilish, maydon elementlari ustida amallar bajarish va algebraik strukturalarni avtomatik tekshirishni sezilarli darajada yengillashtiradi.

Umuman olganda, Galua nazariyasi zamonaviy hisoblash tizimlarining fundamental matematik asoslaridan biri ekanligi tasdiqlandi. U kriptografik xavfsizlikni oshirish, kodlash tizimlarida xatolarni tuzatish va simvolik hisoblash jarayonlarini optimallashtirishda muhim rol o'ynaydi.

Analysis (Tahlil)

Tahlil natijalari Galua nazariyasining nazariy algebra bilan cheklanib qolmasdan, zamonaviy informatika va axborot texnologiyalarida ham muhim o'rin egallashini ko'rsatdi. Chekli maydonlar asosidagi algebraik modellar kriptografik tizimlarning xavfsizligini oshirish va kodlash jarayonlarida xatolarni kamaytirishda samarali hisoblanadi.

Shuningdek, simvolik hisoblash tizimlari murakkab algebraik strukturalarni avtomatik tahlil qilish imkonini berib, Galua nazariyasining amaliy qo'llanilish



doirasini kengaytiradi. Kvant hisoblash va sun'iy intellekt sohalarida esa ushbu nazariya asosida yangi matematik modellarni ishlab chiqish istiqbollari mavjud.

Discussion (Muhokama)

Olingan natijalar shuni ko'rsatadiki, Galua nazariyasi zamonaviy algebraik yondashuvlarning markaziy bo'g'ini bo'lib, u nafaqat nazariy matematika, balki amaliy informatika tizimlarida ham muhim rol o'ynaydi. Chekli maydonlar va algebraik strukturalarning kriptografik algoritmlar va kodlash tizimlaridagi qo'llanilishi ularning universalligini tasdiqlaydi.

Kriptografik algoritmlar tahlilida RSA, AES va ECC o'rtasidagi farqlar ularning turli matematik asoslarga tayanishi bilan izohlanadi. RSA sonlar nazariyasiga asoslangan bo'lib, hisoblash murakkabligi yuqori, lekin klassik xavfsizlik modeli sifatida keng qo'llaniladi. AES esa Galua maydoni $GF(2^8)$ arifmetikasiga asoslanganligi sababli tezkor va samarali hisoblanadi. ECC esa elliptik egri chiziqlar algebrasiga tayanib, kichik kalit uzunligida yuqori xavfsizlik darajasini ta'minlaydi.

Quyidagi taqqoslash ushbu farqlarni yanada aniq ko'rsatadi:

Muhokama uchun taqqoslash

Mezoni	RSA	AES	ECC
Matematik asos	Sonlar nazariyasi	Galua maydoni	Elliptik egri chiziqlar
Hisoblash tezligi	Past	Juda yuqori	Yuqori
Xavfsizlik modeli	Klassik	Simmetrik blok shifrlash	Zamonaviy (kichik kalitli)
Amaliy qo'llanish	Bank, PKI	Ma'lumot shifrlash	Mobil va IoT tizimlar

Simvolik hisoblash tizimlari bo'yicha tahlil shuni ko'rsatdiki, *Maple*, *Mathematica* va *SageMath* kabi vositalar Galua nazariyasini amaliy hisoblash darajasiga olib chiqishda muhim ahamiyatga ega. Bu tizimlar yordamida polinomlar ustida amallar bajarish, chekli maydon elementlarini tekshirish va algebraik strukturalarni avtomatik tahlil qilish mumkin bo'lib, bu nazariy hisob-kitoblarni sezilarli darajada yengillashtiradi.

Muhokama natijalaridan ko'rinadiki, Galua nazariyasi turli sohalarini birlashtiruvchi universal matematik asos sifatida namoyon bo'ladi. U kriptografiyada xavfsizlikni oshirish, kodlash nazariyasida xatolarni kamaytirish va simvolik hisoblashda algoritmik samaradorlikni ta'minlash imkonini beradi.



Umuman olganda, Galua nazariyasi asosidagi algebraik strukturalar zamonaviy axborot texnologiyalarining rivojlanishida muhim o‘rin tutadi va ularning amaliy ahamiyati kelajakda yanada ortib borishi kutiladi.

Conclusion (Xulosa)

Mazkur maqolada Galua nazariyasining zamonaviy informatika, sun'iy intellekt va kvant hisoblashdagi istiqbollari o‘rganildi. Natijalar shuni ko‘rsatadiki, Galua nazariyasi chekli maydonlar va algebraik strukturalar orqali kriptografiya hamda kodlash nazariyasining asosiy matematik bazasini tashkil etadi.

Shuningdek, ushbu nazariya simvolik hisoblash va zamonaviy algoritmik tizimlarda muhim amaliy ahamiyatga ega ekanligi aniqlandi. Kelgusida Galua nazariyasiga asoslangan yangi algoritmlar ishlab chiqilishi kutilmoqda.

Adabiyotlar ro‘yxati:

1. Artin E. *Galois Theory*. Dover Publications, 1998.
2. Dummit D., Foote R. *Abstract Algebra*. Wiley, 2003.
3. Stewart I. *Galois Theory*. Chapman and Hall/CRC, 2004.
4. Lidl R., Niederreiter H. *Finite Fields*. Cambridge University Press, 1997.
5. MacWilliams F.J., Sloane N.J.A. *The Theory of Error-Correcting Codes*. North-Holland, 1977.
6. Stallings W. *Cryptography and Network Security*. Pearson, 2017.
7. Serre J.P. *A Course in Arithmetic*. Springer, 1973.
8. Gallian J.A. *Contemporary Abstract Algebra*. Cengage Learning, 2016.

