Sonlar nazariyasi va sun’iy intellekt: mashinali o‘rganish algoritmlari uchun yangi yondashuvlar

Mohinur Raupova
Saidabonu Shokirova
Chirchiq davlat pedagogika universiteti

Annotatsiya: Ushbu maqola sonlar nazariyasi va sun’iy intellektning mashinali o‘rganish algoritmlariga qanday yangi yondashuvlar olib kelishi mumkinligini o‘rganadi. Sonlar nazariyasi matematik analizning fundamental qismi bo‘lib, butun sonlar, tub sonlar, modulyar arifmetika va boshqa ko‘plab bo‘limlarni o‘z ichiga oladi. Bu matematik asoslar sun’iy intellektdagi muhim masalalar, masalan, ma’lumotlarni modellashtirish, tasniflash va prognozlash uchun foydalanilayotgan mashinali o‘rganish algoritmlarida yanada samarali algoritmlarni yaratishda asosiy vosita bo‘lib xizmat qilishi mumkin. Tub sonlar va modulyar arifmetika kriptografik tizimlarning xavfsizligini ta’minlashda va samaradorligini oshirishda, neyron tarmoqlar va gradient tushish jarayonini optimallashtirishda yangi usullarni kashf qilishda foydalaniladi. Shuningdek, sonlar nazariyasining faktorizatsiya, taqsimlash va algoritmik yondashuvlari mashinali o‘rganishning asosiy bosqichlari bo‘lmish ma’lumotlar oldindan ishlov berish va tahlilni tezlashtiradi. Ushbu maqola ushbu ikki fan o‘rtasidagi bog‘liqlikni ko‘rsatib, sun’iy intellekt yondashuvlariga yangi nazariy va amaliy imkoniyatlar taqdim etishini tahlil qilgan.

Kalit so‘zlar: sonlar nazariyasi, mashinali o‘rganish, modulyar arifmetika, kriptografiya, neyron tarmoqlar, gradient tushish, faktorizatsiya algoritmlari, raqamli xavfsizlik

Number Theory and Artificial Intelligence: New Approaches for Machine Learning Algorithms

Mohinur Raupova
Saidabonu Shokirova
Chirchik State Pedagogical University

Abstract: This paper explores how number theory and artificial intelligence can bring new approaches to machine learning algorithms. Number theory is a fundamental part of mathematical analysis and includes whole numbers, prime numbers, modular arithmetic and many other branches. These mathematical foundations can serve as a key tool for creating more efficient algorithms for important problems in artificial

intelligence, such as machine learning algorithms used for data modeling, classification, and prediction. Prime numbers and modular arithmetic are used to improve the security and efficiency of cryptographic systems, to discover new methods for optimizing neural networks and gradient descent. Also, number theory's factorization, distribution, and algorithmic approaches speed up data preprocessing and analysis, which are key steps in machine learning. This article shows the connection between these two disciplines and analyzes the new theoretical and practical possibilities for artificial intelligence approaches.

Keywords: number theory, machine learning, modular arithmetic, cryptography, neural networks, gradient descent, factorization algorithms, digital security

Sun’iy intellekt sohasida hisoblash texnikasini takomillashtirish orqali yetuk EXMlar (elektron hisoblash mashinalari) yaratishga katta e’tibor qaratilmokda. Yetuk EXMlar foydalanuvchining tabiiy til so‘rovlarini qayta ishlash, axborotni turli shakllarda (belgilar, signal) qabul qilib, ijodiy jarayonlarni amalga oshirish imkoniyatiga ega. Bunday tizimlarning kelajagi, ularning insonlar bilan oson muloqoti va bilimlar bazasidan tezkor foydalanishga asoslangan. Ekspert tizimlar, bu turli sohalar (masalan, tibbiyot, geologiya, fizika) bo‘yicha axborotni saqlaydigan, maslahatchi va tahlilchi sifatida ishlayotgan sun’iy intellekt tizimlari hisoblanadi. Bu tizimlar nafaqat faktlarni foydalanuvchiga yetkazadi, balki maslahatlar beradi, kasalliklarni aniqlaydi, oldindan prognozlash va xulosalar chiqarish imkoniyatiga ega.

Ekspert tizimlar shartlar asosida ishlovchi qoidalar bazasi, ishchi xotira va xulosa chiqarish mexanizmlaridan tashkil topgan. “Agar… u holda...” qoidalari asosida qurilgan bu tizimlar masalan, avtomobilning nosoz qismlarini aniqlash kabi masalalarni hal qilishda qo‘llanadi. Ishchi xotira tizimda mavjud ma’lumotlarni vaqt o‘tishi bilan yangi faktlar bilan boyitadi yoki o‘chiradi. Shuningdek, qoidalarni tanlab ishchi xotiraga yangi faktlarni kiritish ham tizimning asosiy funksiyalaridan biridir. Bunday tizimlarning qoidalar va xulosalar bilan ishlashi masalalarni yechishning muhim qismidir.

Data Mining (DM) texnologiyalari yashirin bilimlarni kashf qilish jarayonida muhim rol o‘ynaydi. DM usullari orqali gigant hajmdagi ma’lumotlardan foydali ma’lumotlarni ajratib olish imkoniyati yaratiladi. DM ning asosiy bosqichlari gipotezalarni shakllantirish, berilganlarni yig‘ish, ma’lumotlarni tayyorlash, modellarni tanlash, parametrlarni sozlash va natijalarni tahlil qilishdan iborat. Bu usullar qaror daraxtlari, regressiya modellari va klaster tahlillarni qurishda qo‘llanib, ma’lumotlarning ichki qonuniyatlarini aniqlaydi. Tavsiflovchi masalalar assotsiativ qoidalarni aniqlash yoki ma’lumotlarni guruhlashni o‘z ichiga oladi, prognoz qiluvchi masalalar esa kelajakdagi hodisalar haqida xulosalar chiqarishga qaratiladi.

DM texnologiyasining qiyinchiliklariga katta hajmdagi xato berilganlardan foydalanish, noma'lum yoki noto‘g‘ri o‘lchovli ma'lumotlarning mavjudligi hamda avtomatlashgan jarayonni optimallashtirish kiradi. Bundan tashqari, "latent alomatlarni" topish, ya'ni yangi yashirin naqshlarni aniqlash va foydalanuvchi uchun kerakli bilimlarni samarali tanlash bugungi kun DM texnologiyalarining dolzarb masalalaridan biridir. Ayniqsa, katta hajmdagi toifalangan ma'lumotlar bilan ishlashda yangi usullarni ishlab chiqish talab etiladi.

Sun'iy intellekt tushunchasi 1956-yilda AQShda Djon Makkarti va bir guruh olimlar tomonidan o‘tkazilgan ilmiy yig‘ilish davomida shakllandi. Ilk ekspert tizimlar bu intellektual texnologiyalarning rivojlanishiga asos bo‘ldi. Ekspert tizimlarning hozirda tibbiyot, texnologiya, iqtisodiyot kabi ko‘plab sohalarda qo‘llanilayotganligi ulardan samarali foydalanish imkoniyatlarini ko‘rsatadi. Nisbatan yangi bo‘lgan Data Mining va bilimga asoslangan tizimlar esa kundalik amaliyotda faol foydalanilmoqda. Shu sababli sun'iy intellekt kelajagi, matematik va kompyuter texnologiyalari bilan birgalikda, istiqbolli va ijodiy yuksalishda davom etadi.

Sonlar nazariyasi matematikaning asosiy bo‘limlaridan biri bo‘lib, butun sonlar va ularning xossalarini o‘rganadi. Tub sonlar faqat o‘ziga va 1 ga bo‘linadigan sonlar sifatida aniqlanadi. Misol sifatida 2, 3, 5, 7 va 11 kabi sonlarni keltirish mumkin. Tub sonlar sonlar nazariyasining poydevorini tashkil etadi va ularning taqsimlanishi matematikaning fundamental masalalaridan biridir. Evklid teoremasiga ko‘ra, tub sonlar cheksiz bo‘lib, ular orasidagi masofa sonlar katta bo‘lgani sayin o‘sib boradi. Ularning xossalari algoritmik tizimlar, xususan, kriptografiyada muhim o‘rin egallaydi. RSA va boshqa shifrlash tizimlari tub sonlarga asoslangan va ulardagi katta sonlar bilan ishlash samaradorlikni oshirgan. Bu esa zamonaviy xavfsizlik tizimlarining ishonchliligini ta'minlaydi.

Modulyar arifmetika qoldiqlar asosida matematik operatsiyalarni bajaruvchi usul bo‘lib, sonlar nazariyasida o‘ziga xos mavqega ega. Masalan, $a \equiv b \pmod{n}$ ifodasi "a va b sonlari n ga bo‘lganda bir xil qoldiq qoldiradi" degan ma'noni anglatadi. Modulyar arifmetika ko‘plab sohalarda, ayniqsa, kriptografiya va kodlash tizimlarida qo‘llaniladi. RSA kriptografik tizimi modulyar arifmetikaga asoslanadi va katta sonlar bilan ishlash zaruriyatini taqozo etadi. Ushbu texnika axborot xavfsizligining eng muhim elementlaridan biri hisoblanadi.

Sonlarning tuzilishi o‘zida ko‘plab nazariy tushunchalarni birlashtiradi. Eulerning φ-funksiyasi berilgan sonning nechta bo‘luvchisi borligini aniqlash uchun ishlatiladi, masalan, agar $n = 9$ bo‘lsa, $\phi(9) = 6$, chunki 9 dan kichik va 9 ga nisbatan tub bo‘lgan sonlar soni oltitani tashkil etadi. Fermat sonlari $F_n = 2^{2^n} + 1$ formulasi bilan topiladi, Mersenne sonlari esa $M_n = 2^n - 1$ formula orqali aniqlanadi. Ushbu sonlar, ayniqsa, raqamli tizimlarda va tub sonlarni o‘rganishda muhim rol o‘ynaydi.

Diophantine tenglamalari sonlar nazariyasining qiziqarli bo‘limlaridan biri bo‘lib, bu algebraik tenglamalarda faqat butun sonli yechimlarni topishni talab qiladi. Misol sifatida Pifagor uchburchaklarida uchraydigan tenglama $x^2 + y^2 = z^2$ ni keltirish mumkin. Fermatning katta teoremasi esa har qanday $n > 2$ uchun $x^n + y^n = z^n$ ning butun sonli yechimga ega emasligini isbotlaydi. Ushbu qoidani uzoq muddat davomida matematiklar isbotlashga harakat qilishgan va nihoyat, 1994 yilda Endryu Vaylz tomonidan isbotlangan.

Sonlar nazariyasining kriptografiyadagi roli alohida ahamiyatlidir. RSA algoritmi zamonaviy axborot texnologiyalarining asosiy unsuri sifati ishlatiladi. Bu algoritm ikkita katta tub sonni ko‘paytirish orqali hosil bo‘lgan sonni ma’lumotlarni shifrlash va ochishda qo‘llaydi. Shifrlash jarayoni ommaviy kalit (e) va modulyar (n) yordamida $M^e \mod n$ operatsiyasi orqali amalga oshiriladi. Shuningdek, Elliptik egri chiziqlar kriptografiyasi (ECC) esa xavfsizlikni oshirish uchun samaraliroq usul bo‘lib, u kompyuter resurslarini tejash bilan birga kuchli himoya taqdim etadi. Bu usul ayniqsa, sekin ishlovchi tizimlarda keng qo‘llaniladi.

Analitik sonlar nazariyasi esa tub sonlarning taqsimlanishini chuqurroq o‘rganish uchun rivojlantirilgan matematik nazariyadir. Riemann zeta funksiyasi va unga bog‘liq bo‘lgan Riemann gipotezasi sonlar nazariyasining eng qiyin va ochilmagan sohalaridan biri hisoblanadi. Bu gipoteza, agar to‘g‘ri deb topilsa, butun sonlar va tub sonlar taqsimoti haqidagi tasavvurlarni tubdan o‘zgartirishi mumkin. Shuningdek, Dirichlet seriyalari va L-funksiyalar orqali turli matematik metodlar tub sonlarni tahlil qilishda qo‘llaniladi.

Algoritmik va kompyuter yordamida tadqiqotlar esa zamonaviy ilm-fanning ajralmas qismiga aylangan. Masalan, katta sonlarni faktorizatsiya qilish algoritmlari sonlar nazariyasining asosiy amaliy yutuqlaridan biridir. Faktorizatsiya jarayoni berilgan butun sonni uning kichikroq ko‘paytuvchilariga ajratishni o‘z ichiga oladi. RSA kabi yirik kriptografik tizimlarning xavfsizligi katta sonlarni faktorizatsiya qilishning murakkabligiga asoslangan. Pollard rho va Kvadrat elek algoritmlari bu sohada asosiy rol o‘ynaydi. Asosan bu yondashuvlar yordamida shifrlash va shifrni ochish amalga oshiriladi. Shuningdek, bu algoritmlar katta hajmdagi ma’lumotlarning xavfsizligini ta’minlashda muhim ahamiyatga ega.

Sonlar nazariyasi nafaqat nazariy matematika rivojida, balki zamonaviy texnologiyalar, kriptografiya va katta ma’lumotlar bilan ishlashda ham katta ahamiyatga ega. Tub sonlar va modulyar arifmetika yordamida ma’lumotlar xavfsizligi ta’minlanadi, RSA va ECC kabi algoritmlar orqali turli shifrlash tizimlari ishlab chiqiladi. Shu bilan birga, katta ma’lumotlar ustida ishlashda sonlar nazariyasi texnikalaridan foydalaniladi, bu esa global miqyosdagi axborot xavfsizligi tizimining eng muhim jihatlaridan biridir.

Sonlar nazariyasi sun’iy intellektning mashinali o‘rganish tizimlari uchun yangi va samarali algoritmlar yaratishda mustahkam poydevor bo‘lib xizmat qilmoqda. Sonlar nazariyasidagi modulyar arifmetika va tub sonlar bilan bog‘liq amallar ko‘p miqdordagi ma’lumotlarni samarali kodlash va tahlil qilish imkonini beradi. Bu, ayniqsa, kriptografiya va raqamli xavfsizlikda katta ahamiyatga ega. Neyron tarmoqlar va gradient tushish algoritmlarini optimallashtirishda sonlar nazariyasidagi chuqur bilimlar yangi algoritmik yechimlarni taklif qilishi mumkin. Ayniqsa, katta sonlarni faktorizatsiya qilish, sonlarning taqsimlanishini hisoblash va funksiyalarni optimallashtirish orqali sun’iy intellekt va mashinali o‘rganish modellarini yanada rivojlantirishga erishiladi. Shu orqali, mashinali o‘rganish algoritmlarining samaradorligini oshirish va ko‘p qatlamli ma’lumotlar ustida ishlashni osonlashtirishga erishiladi. Maqolada sonlar nazariyasining nazariy va amaliy hissasi global texnologiyalarning rivojida nechog‘li muhim ekanligi ko‘rsatib o‘tildi.

Foydalanilgan adabiyotlar

1. Apostol, T. M. (1976). Introduction to Analytic Number Theory. Springer-Verlag.

2. Silverman, J. H., & Tate, J. (1994). Rational Points on Elliptic Curves. Springer.

3. Montgomery, H. L., & Vaughan, R. C. (2006). Multiplicative Number Theory I: Classical Theory. Cambridge University Press.

4. Bishop, C. M. (2006). Pattern Recognition and Machine Learning. Springer.

5. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.

6. Nielsen, M. A. (2015). Neural Networks and Deep Learning. Determination Press.

7. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM.

8. Varian, H. R. (2014). Intermediate Microeconomics: A Modern Approach. W.W. Norton & Company.

9. Feynman, R. P., Leighton, R. B., & Sands, M. (2011). The Feynman Lectures on Physics. Basic Books.

10. Bozorov, M. N. (2019). Kriptografiya va sonlar nazariyasi asoslari. Toshkent: O‘zbekiston Milliy Universiteti nashriyoti.