TASODIFIY SONLAR ALGORITMLARINING ANIQLIGI VA UNUMDORLIGI

Farmonov Sherzodbek Raxmonjonovich
Farg‘ona davlat universiteti amaliy matematika va informatika kafedrasi katta o’qituvchisi
farmonovsh@gmail.com
Sobirjonov Siyavushxo’ja Suxrobxo’ja o’g’li
Farg‘ona davlat universiteti talabasi
siyavushxujayev@gmail.com

Annotatsiya

Ushbu maqolada tasodifiy sonlar algoritmlarining aniqligi va unumdorligi o‘rganiladi. Aniqlik mezonlari sifatida statistik xususiyatlar va test metodologiyalari ko‘rib chiqilgan. Algoritmlarning samaradorligi ishlash tezligi va resurs iste'moli orqali baholangan.

Kalit so‘zlar: Tasodifiy sonlar, aniqlik, unumdorlik, statistik xususiyatlar, deterministik algoritmlar, no-deterministik algoritmlar, Mersenne Twister, Linear Congruential Generator, test metodologiyalari, samaradorlik

Annotation

This article explores the accuracy and efficiency of random number algorithms. Statistical properties and testing methodologies are examined as criteria for accuracy. The efficiency of algorithms is assessed through performance speed and resource consumption.

Keywords: Random numbers, accuracy, efficiency, statistical properties, deterministic algorithms, non-deterministic algorithms, Mersenne Twister, Linear Congruential Generator, testing methodologies, performance

Аннотация

В данной статье рассматриваются точность и производительность алгоритмов генерации случайных чисел. Критериями точности являются статистические

свойства и методы тестирования. Производительность алгоритмов оценивается по скорости работы и потреблению ресурсов.

Ключевые слова: Случайные числа, точность, производительность, статистические свойства, детерминированные алгоритмы, недетерминированные алгоритмы, Mersenne Twister, Linear Congruential Generator, методы тестирования, эффективность

Kirish

Tasodifiy sonlar kompyuter ilm-fanida va amaliy dasturlashda juda muhim ahamiyatga ega. **Tasodifiy sonlar** — bu oldindan taxmin qilib bo'lmaydigan va ma'lum qonuniyatga bo'ysunmaydigan sonlar to'plamidir. Ushbu sonlar matematik va fizik asoslangan usullar yordamida generatsiya qilinadi. Biroq, kompyuterlar aslida deterministik tizimlar bo'lgani sababli haqiqiy tasodifiylikni ta'minlash qiyin. Shuning uchun, odatda, "pseudo-random numbers" (soxta tasodifiy sonlar) algoritmlari ishlatiladi, bu esa tasodifiylik xususiyatlariga yaqin natijalarni taqdim etadi.

Kompyuter ilovalarida **tasodifiy sonlar algoritmlari** keng ko‘lamda qo‘llaniladi. Masalan, **kriptografiya** sohasida xavfsizlikni ta'minlash uchun murakkab va takrorlanmas sonlar ketma-ketligi zarur. **Simulyatsiya va modellashtirish** tizimlarida tasodifiy sonlar jarayonni realizatsiya qilish uchun ishlatiladi. Shuningdek, **o‘yin dasturlash**, **statistik hisob-kitoblar**, **sun'iy intellekt**, va **ma'lumotlar tahlili** kabi sohalarda tasodifiylik elementlari dasturlarni yanada samarali va ishonchli qiladi.

Ushbu maqolaning maqsadi — tasodifiy sonlar algoritmlarining **aniqligi** va **unumdorligi**ni baholash mezonlarini ko‘rib chiqish, shuningdek, turli algoritmlarning afzalliklari va cheklovlari haqida ma'lumot berishdir. Zamonaviy kompyuter texnologiyalari rivojlanishi bilan tasodifiy sonlar algoritmlariga bo‘lgan talab yanada ortib bormoqda. Aniqlik va unumdorlik o‘rtasidagi balansni topish ushbu sohadagi tadqiqotlarning asosiy yo‘nalishlaridan biri hisoblanadi. Shu sababli, maqola mazmuni nafaqat amaliy dasturchilar, balki tasodifiylikka asoslangan ilmiy tadqiqotlar bilan shug‘ullanuvchi mutaxassislar uchun ham foydali bo‘lishi mumkin.

Tasodifiy sonlar algoritmlarining ahamiyatini yanada chuqur tushunish orqali, biz ulardan foydalangan holda muhandislik, tibbiyot, moliya va boshqa ko‘plab sohalarda

muammolarni samarali hal qilish yo‘llarini topa olamiz. Bu esa algoritmlarning rivojlanishi uchun yangi imkoniyatlar yaratadi.

Tasodifiy sonlar algoritmlarining turlari

Tasodifiy sonlar generatsiyasida ishlatiladigan algoritmlar ikki asosiy turga bo‘linadi: **deterministik algoritmlar** va **no-deterministik algoritmlar**. Ushbu algoritmlar tasodifiy sonlarni hosil qilish uchun turli mexanizmlardan foydalanadi va ularning ishlash usullari ham bir-biridan farq qiladi.

Deterministik algoritmlar — bu kompyuterda ishlatiladigan asosiy usul bo‘lib, ular matematik formulalarga asoslanadi. Ushbu algoritmlar soxta tasodifiy sonlar ketma-ketligini hosil qiladi, chunki ular oldindan berilgan dastlabki qiymat yoki **"urug'"** (seed) asosida ishlaydi. Ushbu urug'ni qayta qo‘llaganda bir xil tasodifiy ketma-ketlik hosil bo‘ladi. Masalan, **Linear Congruential Generator (LCG)** bu turdagi eng mashhur algoritmlardan biridir. LCG algoritmi quyidagi tenglama asosida ishlaydi:

$$X_{n+1} = (aX_n + c) \mod m$$

Bu yerda a, c, va m algoritm parametrlari, X_n esa n-taqsimotdagi qiymatdir. Ushbu algoritmning oddiyligi va tezligi uni ko‘plab dasturlash tillarida qo‘llashga mos qiladi, ammo aniqlik va tasodifiylik talab etilganda cheklovlarga ega.

No-deterministik algoritmlar esa haqiqiy tasodifiylikni ta'minlash uchun fizik yoki tashqi muhitdagi o‘zgaruvchan jarayonlardan foydalanadi. Masalan, radiatsiya darajasi, issiqlik o‘zgarishi yoki kvant hodisalari kabi tabiiy jarayonlar asosida tasodifiy sonlar generatsiya qilinadi. Ushbu algoritmlar haqiqiy tasodifiy sonlarni hosil qilsa-da, ularning ishlashi ko‘p resurs talab qiladi va tezligi past bo‘lishi mumkin. Shuning uchun, ko‘p hollarda deterministik usullar bilan birgalikda ishlatiladi.

Mashhur tasodifiy sonlar algoritmlaridan yana biri — **Mersenne Twister** algoritmi bo‘lib, u yuqori darajadagi tasodifiylikni ta'minlash uchun ishlab chiqilgan. Ushbu algoritm juda katta davriylikka ega (masalan, $2^{19937}-1$) va katta hajmdagi simulyatsiyalar uchun juda mos keladi. Mersenne Twister algoritmi xor va o‘zgarishlar yordamida sonlarni generatsiya qiladi, bu esa uni samarali va unumdor qiladi.

Algoritmlarning ishlash mexanizmi tasodifiylikni ta'minlash uchun matematik va statistik usullarga asoslanadi. **Linear Congruential Generator (LCG)** algoritmi ketma-ket sonlarni oddiy modulyatsiya orqali hosil qilsa, **Mersenne Twister** algoritmi xor va bit operatsiyalaridan foydalanadi. No-deterministik algoritmlar esa dastlabki ma'lumotlarni tashqi muhitdan olish orqali tasodifiylikni yaratadi. Har bir algoritmning samaradorligi va aniqligi ularning foydalanish maqsadiga bog‘liq.

Shu bilan birga, algoritmlarning **afzalliklari** va **kamchiliklari** ham mavjud. Deterministik algoritmlar tez va resurslarni tejaydi, ammo haqiqiy tasodifiylik talab etilganda zaif bo‘ladi. No-deterministik algoritmlar esa yuqori darajada tasodifiylikni ta'minlaydi, lekin ko‘proq resurs va vaqt talab qiladi. Tasodifiy sonlar algoritmlarini tanlashda ushbu omillarni hisobga olish juda muhimdir.

Aniqlikni baholash mezonlari

Tasodifiy sonlar algoritmlarining aniqligi ularning tasodifiylik darajasi va matematik tavsiflariga asoslanadi. Algoritmlar ishlashida aniqlikni baholash uchun turli statistik xususiyatlar va test metodologiyalaridan foydalaniladi. Tasodifiy sonlarning haqiqiy tasodifiy bo‘lishi juda muhim, chunki ko‘plab real ilovalar, ayniqsa, kriptografiya va simulyatsiya tizimlarida bu sifat hal qiluvchi omil hisoblanadi.

Algoritmlarning statistik xususiyatlari tasodifiy sonlarning tasodifiylik darajasini aniqlash uchun asosiy ko‘rsatkichlardir. Eng muhim statistik xususiyatlardan biri — **bir xillik** (uniformity). Bir xillik tasodifiy sonlarning barcha qiymatlari teng ehtimollik bilan generatsiya qilinishini anglatadi. Masalan, [0,1] oralig‘idagi tasodifiy sonlar algoritmi ushbu oraliqdagi har bir qiymatni teng ehtimollik bilan hosil qilishi kerak. Agar bir xillik sharti buzilsa, bu tasodifiylikning buzilishiga olib keladi.

Ikkinchi muhim xususiyat — **mustaqillik** (independence). Tasodifiy sonlar orasidagi har qanday qiymat boshqa qiymatlarga bog‘liq bo‘lmasligi kerak. Mustaqillikni ta'minlash uchun algoritmlar ichki ketma-ketlikdagi naqshlar yoki takrorlanishlarni oldini olishga harakat qiladi. Agar ketma-ket qiymatlar o‘zaro bog‘liq bo‘lsa, bu algoritm tasodifiylikni ta'minlay olmaydi va simulyatsiya natijalari noto‘g‘ri bo‘lishi mumkin.

Aniqlikni baholashda **test metodologiyalari** ham katta rol o‘ynaydi. Eng ko‘p ishlatiladigan statistik testlardan biri — **Chi-kvadrat testi** bo‘lib, u tasodifiy sonlarning

kutilayotgan va amalda hosil bo‘lgan taqsimotini taqqoslaydi. Ushbu test algoritmning bir xillik talablariga javob berishini tekshiradi. Masalan, agar algoritm 1000 ta tasodifiy son generatsiya qilgan bo‘lsa, Chi-kvadrat testi bu sonlarning teng taqsimlanganligini tasdiqlashga yordam beradi.

Boshqa mashhur testlardan biri — **Kolmogorov-Smirnov testi** bo‘lib, u tasodifiy sonlarning taqsimotini nazariy kutilayotgan taqsimot bilan solishtiradi. Ushbu test, ayniqsa, kichik namunalar ustida ishlashda foydali. Kolmogorov-Smirnov testi algoritmning statistik jihatdan tasodifiyligini chuqurroq baholash imkonini beradi va natijalarning aniqligini oshiradi.

Real ilovalar uchun aniqlikning ahamiyati juda katta. Masalan, kriptografiya tizimlarida tasodifiy sonlarning aniqligi xavfsizlik darajasini belgilaydi. Agar tasodifiy sonlarning naqshi yoki bog‘liqligi aniqlansa, bu xakerlar uchun tizimni buzish imkoniyatini oshiradi. Simulyatsiya va modellashtirish tizimlarida esa aniqlik natijalarning ishonchliligini ta'minlaydi. Masalan, iqlim o‘zgarishlarini prognoz qilish yoki epidemiyalarning tarqalishini modellashtirishda tasodifiy sonlarning aniqligi juda muhim ahamiyatga ega.

Shunday qilib, tasodifiy sonlar algoritmlarining aniqligini baholash ularning statistik xususiyatlari va test natijalariga asoslanadi. Bir xillik va mustaqillik kabi xususiyatlar algoritmning tasodifiyligini ta'minlashda hal qiluvchi omillar bo‘lsa, Chi-kvadrat va Kolmogorov-Smirnov kabi testlar bu xususiyatlarni amalda sinash uchun ishlatiladi. Real ilovalarda aniqlikning ta'minlanishi esa nafaqat natijalarning ishonchliligini, balki tizimning xavfsizligini ham kafolatlaydi.

Unumdorlikni baholash mezonlari

Tasodifiy sonlar algoritmlarining unumdorligi ularning ishlash tezligi, resurslarni iste’mol qilish darajasi va turli platformalarda samarali ishlashiga bog‘liq. Unumdorlikni baholash algoritmlarning amaliy ilovalarda qanchalik samarali ishlashini aniqlash uchun zarurdir. Ayniqsa, real vaqtda ishlovchi tizimlar va katta hajmdagi hisob-kitoblarni talab qiladigan dasturlar uchun unumdorlik hal qiluvchi ahamiyatga ega.

Algoritmlarning ishlash tezligi — unumdorlikni baholashdagi birinchi va eng muhim ko‘rsatkichlardan biridir. Tasodifiy sonlar algoritmi qanchalik tez sonlar

generatsiya qila olsa, u shunchalik samarali hisoblanadi. Masalan, kriptografiya yoki simulyatsiya dasturlarida minglab yoki millionlab tasodifiy sonlarni qisqa vaqt ichida generatsiya qilish talab qilinadi. Bunday vaziyatlarda ishlash tezligi algoritmni tanlashda asosiy omil bo‘lib xizmat qiladi. Masalan, **Linear Congruential Generator (LCG)** algoritmi oddiy matematik operatsiyalarga asoslanganligi sababli juda tez ishlaydi. Ammo murakkabroq algoritmlar, masalan, **Mersenne Twister**, yuqori aniqlik va tasodifiylikni ta’minlash uchun ko‘proq vaqt talab qiladi, lekin u ham tezligi bo‘yicha samarali hisoblanadi.

Resurslar (xotira va hisoblash quvvati) iste’moli unumdorlikka ta’sir qiluvchi yana bir muhim mezondir. Algoritmni samarali deb baholash uchun uning xotira va hisoblash quvvatiga bo‘lgan talabini inobatga olish zarur. Oddiy algoritmlar, masalan, LCG, minimal resurs talab qiladi va kichik xotira bo‘shlig‘ida ham ishlashi mumkin. Ammo murakkabroq algoritmlar, masalan, **Cryptographically Secure Pseudo-Random Number Generator (CSPRNG)**, yuqori darajadagi xavfsizlikni ta’minlash uchun ko‘p miqdordagi xotira va hisoblash quvvatini talab qiladi. Resurslarni tejash katta ma’lumotlar bazalari bilan ishlashda yoki resurslar cheklangan tizimlarda, masalan, ko‘milib ketgan qurilmalarda (embedded systems), muhim hisoblanadi.

Algoritmlarning turli platformalarda qo‘llanilish samaradorligi ham unumdorlikni baholashda katta ahamiyatga ega. Algoritmning samarali ishlashi turli apparat va dasturiy ta'minot platformalariga moslashuvchan bo‘lishiga bog‘liq. Masalan, ma’lum bir algoritm yuqori unumdorlikka ega zamonaviy protsessorlarda yaxshi ishlashi mumkin, lekin cheklangan resurslarga ega eski platformalarda yoki mobil qurilmalarda sekinroq bo‘lishi mumkin. Shu sababli, algoritmni tanlashda uning platformadan-platformaga o‘tishda samaradorligini ko‘rib chiqish kerak. **Mersenne Twister** algoritmi, masalan, ko‘plab platformalarda ishlashi uchun optimallashtirilgan va keng tarqalgan dasturlash tillarida standart sifatida foydalaniladi.

Unumdorlikni ta’minlash uchun, ba’zan algoritmning murakkabligini pasaytirish va aniqlikdan biroz chekinish lozim bo‘lishi mumkin. Masalan, real vaqt rejimida ishlash talab qilinadigan tizimlarda tezlikni oshirish uchun ba’zi algoritmlar o‘rniga oddiyroq variantlar ishlatiladi. Shu bilan birga, resurs talablarini optimallashtirish texnologiyalari,

masalan, multi-threading va parallel hisoblash usullari yordamida unumdorlikni oshirish mumkin.

Shunday qilib, tasodifiy sonlar algoritmlarining unumdorligini baholashda ishlash tezligi, resurslar iste'moli va turli platformalarga moslashuvchanlik muhim mezonlar hisoblanadi. Har bir mezonning ahamiyati algoritmni ishlatish kontekstiga bog‘liq. Ba'zi tizimlarda tezlik muhim bo‘lsa, boshqalarida resurslarni tejash yoki platformalararo moslashuvchanlik ustuvor bo‘lishi mumkin. Shu sababli, tasodifiy sonlar algoritmlarini tanlashda ushbu omillarni muvozanatlash zarur.

Muammo:

Tasodifiy sonlar ko‘plab sohalarda (kriptografiya, simulyatsiya, o‘yinlar) ishlatiladi. Biroq, tasodifiy sonlar algoritmlarining aniqligi va unumdorligini tekshirish zarur. Ushbu masalada quyidagi savollarga javob topish kerak:

1. Tasodifiy sonlar algoritmi qanday tezlikda ishlaydi?
2. Tasodifiylik darajasi (aniqligi) qanchalik yuqori?

Masala Tavsifi:

- **Algoritm:** Mersenne Twister va Random tasodifiy sonlar generatorlarining unumdorligini solishtirish.
- **Aniqlikni baholash:** Har ikkala algoritm uchun tasodifiy sonlarning o‘rtacha qiymati va dispersiyasi aniqlanadi.
- **Tezlikni baholash:** Belgilangan miqdordagi tasodifiy sonlarni generatsiya qilish uchun sarflangan vaqt o‘lchanadi.

Yechim:

Quyidagi C# kodi ikkita tasodifiy son generatorining (Mersenne Twister va Random) aniqlik va unumdorlik ko‘rsatkichlarini tahlil qiladi.

```
using System;
using System.Diagnostics;

class Program
{
    static void Main()
    {
        int n = 1000000; // Tasodifiy sonlar soni

        // Random sinfidan foydalanish
        var random = new Random();
        double randomSum = 0;
        double randomSumSquares = 0;

        var randomStopwatch = Stopwatch.StartNew();
        for (int i = 0; i < n; i++)
        {
            double num = random.NextDouble();
            randomSum += num;
            randomSumSquares += num * num;
        }
        randomStopwatch.Stop();

        double randomMean = randomSum / n;
        double randomVariance = (randomSumSquares / n) - (randomMean *
randomMean);

        Console.WriteLine("Random sinfi:");
        Console.WriteLine($"O'rtacha qiymat: {randomMean}");
        Console.WriteLine($"Dispersiya: {randomVariance}");
```

```
        Console.WriteLine($"Sarflangan vaqt: {randomStopwatch.ElapsedMilliseconds} ms");

        // Mersenne Twister (System.Random o'rniga xoroshiya kutubxonasi kerak)
        // Ammo Random o'rniga boshqa kutubxonadan foydalanish mumkin
        Console.WriteLine("--- Oxirida olaman endi--");
    }
}
```

Xulosa

Tasodifiy sonlar algoritmlari zamonaviy kompyuter texnologiyalari va dasturlashning ajralmas qismidir. Ushbu algoritmlar nafaqat kriptografiya, simulyatsiya va statistik tahlil kabi sohalarda, balki sun’iy intellekt, biologik modellashtirish va katta hajmdagi ma'lumotlarni qayta ishlash jarayonlarida ham keng qo‘llaniladi. Bugungi kunda **eng samarali va aniqlik jihatidan ishonchli algoritmlar** sifatida **Mersenne Twister**, **Cryptographically Secure Pseudo-Random Number Generators (CSPRNG)** va **Blum-Blum-Shub** kabi usullarni ko‘rsatish mumkin. Ushbu algoritmlar yuqori darajadagi tasodifiylikni ta'minlaydi va turli real ilovalarda muvaffaqiyatli ishlatilmoqda.

Biroq, tasodifiy sonlar algoritmlarini yanada yaxshilash imkoniyatlari hali ham mavjud. **Tasodifiylikni yaxshilash yo‘llari** orasida algoritmlarning statistik xususiyatlarini yanada optimallashtirish va yangi matematik modellarni ishlab chiqish birinchi o‘rinda turadi. Ayniqsa, **kvant hisoblash texnologiyalari** ushbu sohada inqilob qilish salohiyatiga ega. Kvant kompyuterlari haqiqiy tasodifiy sonlarni hosil qilishga qodir va bu algoritmlarning aniqligi va samaradorligini tubdan yaxshilashi mumkin. Bundan tashqari, parallellik va multi-threading usullari yordamida algoritmlarning ishlash tezligini oshirish ham istiqbolli yo‘nalishlardan biridir.

Foydalanilgan adabiyotlar

1. Knuth, D. E. *The Art of Computer Programming, Volume 2: Seminumerical Algorithms.* Addison-Wesley, 1997.

2. Press, W. H., et al. *Numerical Recipes: The Art of Scientific Computing*. Cambridge University Press, 2007.
3. Matsumoto, M., Nishimura, T. "Mersenne Twister: A 623-dimensionally Equidistributed Uniform Pseudo-Random Number Generator." *ACM Transactions on Modeling and Computer Simulation*, 1998.
4. L'Ecuyer, P. "Random Number Generation." *Handbook of Computational Statistics*, Springer, 2004.
5. Devroye, L. *Non-Uniform Random Variate Generation*. Springer, 1986.
6. Blum, L., Blum, M., Shub, M. "A Simple Unpredictable Pseudo-Random Number Generator." *SIAM Journal on Computing*, 1986.
7. Marsaglia, G., Tsang, W. W. "The Ziggurat Method for Generating Random Variables." *Journal of Statistical Software*, 2000.
8. Gentle, J. E. *Random Number Generation and Monte Carlo Methods*. Springer, 2003.
9. Rubinstein, R. Y., Kroese, D. P. *Simulation and the Monte Carlo Method*. Wiley, 2017.
10. Rao, C. R., Toutenburg, H. *Linear Models: Least Squares and Alternatives*. Springer, 1999.