TASODIFIY SONLARGA DOIR ALGORITMLARNING AXBOROT TEXNOLOGIYALARIDA DOLZARBLIGI

Farmonov Sherzodbek Raxmonjonovich
Farg'ona davlat universiteti amaliy matematika va informatika kafedrasi katta o'qituvchisi
e-mail: farmonovsh@gmail.com
Mirzayev Asadbek Marifjon o'g'li
Farg'ona davlat universiteti talabasi
e-mail: mirzayevasadbek7177@gmail.com

Anotatsiya

Ushbu maqolada tasodifiy sonlar va ularni yaratish algoritmlari haqida batafsil ma'lumot berilgan. Tasodifiy sonlarning ikki asosiy turi – **haqiqiy tasodifiy sonlar** va **psevdo-tasodifiy sonlar** tahlil qilinib, ularning ishlash prinsiplari yoritilgan. Maqolada Lineyer kongruent usuli, Mersenne Twister, XORShift va kriptografik xavfsiz generatorlar kabi mashhur algoritmlar va ularning afzallik va kamchiliklari ko'rib chiqilgan. Shuningdek, tasodifiy sonlar algoritmlarining kriptografiya, statistika, kompyuter o'yinlari va sun'iy intellekt kabi sohalarda keng qo'llanilishi misollar orqali tushuntirilgan.

Kalit so'zlar: Tasodifiy sonlar, statistik, tartibsiz, Haqiqiy tasodifiy son, tabiiy jarayonlar, radioaktiv parchalanish, psevdotasodifiy sonlar, generatorlar, psevdotasodifiy son generatorlari, kriptografoya, algoritm, shifrlash algoritmlari, statistik modellashtirish, Monte-Karlo simulyatsiyasi, tasodifiy tanlash

Annotation.

This article provides detailed information about random numbers and their generation algorithms. Two main types of random numbers - true random numbers and pseudo-random numbers are analyzed and their working principles are explained. The article examines popular algorithms such as the Linear Congruent Method, Mersenne Twister, XORShift, and cryptographically secure generators and their advantages and disadvantages. Also, the widespread use of random number algorithms in fields such as cryptography, statistics, computer games, and artificial intelligence is explained through examples.

Keywords: Random numbers, statistical, random, True random number, natural processes, radioactive decay, pseudorandom numbers, generators, pseudorandom number generators, cryptography, algorithm, encryption algorithms, statistical modeling, Monte Carlo simulation, random selection

Аннотация.

В этой статье представлена подробная информация о случайных числах

и алгоритмах их генерации. Анализируются два основных типа случайных чисел - истинные случайные числа и псевдослучайные числа, и объясняются принципы их работы. В статье рассматриваются популярные алгоритмы, такие как линейно-конгруэнтный метод, Mersenne Twister, XORShift и криптографически защищенные генераторы, а также их преимущества и недостатки. Кроме того, на примерах объясняется широкое использование алгоритмов случайных чисел в таких областях, как криптография, статистика, компьютерные игры и искусственный интеллект.

Ключевые слова: случайные числа, статистика, случайное число, истинно случайное число, естественные процессы, радиоактивный распад, псевдослучайные числа, генераторы, генераторы псевдослучайных чисел, криптография, алгоритм, алгоритмы шифрования, статистическое моделирование, моделирование Монте-Карло, случайный выбор.

Tasodifiy sonlar va ularni generatsiya qilish algoritmlari zamonaviy kompyuter texnologiyalarida muhim o‘rin tutadi. Ular kriptografiya, modellashtirish, o‘yinlar, statistika va sun’iy intellekt kabi turli sohalarda keng qo‘llaniladi. Masalan, xavfsiz parollar yaratish, fizika hodisalarini modellashtirish yoki o‘yinlardagi tasodifiy voqealar tasviri kabi jarayonlarda tasodifiylik tushunchasi asosiy rol o‘ynaydi. Kompyuterlar o‘z tabiati bilan deterministik bo‘lgani sababli, ular haqiqiy tasodifiy sonlarni hosil qila olmaydi. Shuning uchun tasodifiy sonlarni yaratish algoritmlari ishlab chiqilgan. Ushbu algoritmlar yordamida ko‘rinishidan tasodifiy bo‘lgan, ammo matematik jihatdan hisoblab topiladigan sonlar hosil qilinadi. Bunday sonlar psevdo-tasodifiy sonlar deb ataladi. Shu bilan birga, maxsus apparat qurilmalar yordamida haqiqiy tasodifiy sonlar ham olinishi mumkin.

Tasodifiy sonlarning turlari

1.Haqiqiy tasodifiy sonlar generatorlari (TRNG - True Random Number Generators)

Bu sonlar tabiiy jarayonlar, masalan, kvant fizikasi yoki fizik hodisalar orqali hosil qilinadi. Misol tariqasida, mikroprotsessorlardagi elektr shovqin, radioaktiv parchalanish yoki atmosferadagi tovush signallarini keltirish mumkin. Ushbu tasodifiy sonlar haqiqiy ma’noda oldindan bashorat qilib bo‘lmaydigan tarzda hosil bo‘ladi.

Ishlash prinsipi:

- TRNG algoritmlari **tabiiy jarayonlar** orqali tasodifiy ma’lumotlarni yig‘adi. Masalan:
  - **Elektr shovqinlari** – mikroprotsessorlar va elektron sxemalarning elektr signallaridagi kichik tebranishlar.

- **Atmosfera tovushlari** – atrofdagi tabiiy tovushlarning beqarorliklari.
- **Lazer nuri yoki yorug‘lik shovqini** – optik qurilmalardagi tasodifiy signallar.
- **Radioaktiv parchalanish** – radioaktiv elementlarning parchalanish tezligi.

Afzalliklari:

- To‘liq oldindan bashorat qilib bo‘lmaydi.
- Xavfsizlik tizimlari uchun juda mos keladi.

Kamchiliklari:

- Maxsus apparatlar talab qiladi.
- Sekin ishlashi mumkin.

Qo‘llanilishi:

- Kriptografiya (ma’lumotlarni shifrlash).
- O‘ta xavfsiz kalitlarni generatsiya qilish.

Misol: Intel protsessorlarida joylashgan **Intel RNG** (Random Number Generator) TRNG hisoblanadi.

2.Psevdo-tasodifiy sonlar generatorlari (PRNG - Pseudo-Random Number Generators)

Bu sonlar maxsus algoritmlar orqali kompyuter dasturlari yordamida hosil qilinadi. Ular haqiqiy tasodifiy sonlar kabi ko‘rinsa ham, aslida, aniq bir boshlang‘ich qiymatga (seed) asoslanadi va oldindan hisoblash imkoniyatiga ega. Ushbu sonlar deterministik bo‘lib, kompyuter xotirasi va hisoblash quvvatidan foydalangan holda yaratiladi.

Ishlash prinsipi:

1. PRNG algoritmlariga boshlang‘ich qiymat (**seed**) beriladi.
2. Ushbu seed qiymat asosida matematik operatsiyalar ketma-ketligi orqali yangi sonlar generatsiya qilinadi.
3. PRNG'lar sonlarni hosil qilish uchun **modulo**, **ko‘paytirish**, **bit siljitish** kabi operatsiyalardan foydalanadi.

Eng mashhur PRNG algoritmlari:

Lineyer kongruent generator (LCG)

LCG – eng oddiy va tezkor algoritmlardan biri bo‘lib, quyidagi formula orqali ishlaydi:

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

Bu yerda:

- X_n – joriy qiymat,
- a – ko‘paytiruvchi,
- c – qo‘shimcha qiymat,
- m – modulo (chegaralangan son).

Ishlash tartibi:

1. Boshlang‘ich qiymat X_0 beriladi.
2. Formula orqali keyingi X_{n+1} qiymat hisoblanadi.
3. Hosil bo‘lgan qiymatlar sikl hosil qilguncha davom etadi.

Afzalliklari:

- Oddiy va tez ishlaydi.

Kamchiliklari:

- Sonlar tezda takrorlana boshlashi mumkin.
- Tasodifiylik darajasi past.

Misol: C# yoki Python kabi tillarda kichik loyihalar uchun ishlatiladi.

Mersenne Twister

Mersenne Twister – PRNG'larning eng mashhurlaridan biri bo‘lib, 1997-yilda ishlab chiqilgan. U uzun sikl (takrorlanish) va yuqori sifatli tasodifiy sonlarni hosil qiladi.

Xususiyatlari:

- Sikl uzunligi: $2^{19937} - 1$
- Tezkor va samarali algoritm.
- Statistik xususiyatlari yuqori.

Afzalliklari:

- Katta miqdordagi sonlarni samarali generatsiya qiladi.
- Ilmiy hisoblashlar va modellashtirish uchun mos keladi.

Kamchiliklari:

- Kriptografiya uchun xavfsiz emas, chunki bashorat qilinishi mumkin.

Qo‘llanilishi:

- Kompyuter o‘yinlari, simulyatsiyalar va statistik dasturlarda keng ishlatiladi.

XORShift algoritmi

XORShift algoritmi psevdo-tasodifiy sonlarni yaratishda **XOR (mantiqiy OR)** va **bit siljitish** (shift) operatsiyalaridan foydalanadi.

Formula:

X=X *xor* ***(x<<a);*** ***X=X*** *xor* ***(x>>b);*** ***X=X*** *xor* ***(x<<c);***

Afzalliklari:

- Oddiy va tezkor.
- Katta xotira talab qilmaydi.

Kamchiliklari:

- Ba’zi statistik testlarda yaxshi natija bermasligi mumkin.

Qo‘llanilishi:

- O‘yinlar va dasturlar uchun kichik loyihalarda qo‘llaniladi.

Kriptografik xavfsiz PRNG (CSPRNG)

Kriptografik xavfsiz generatorlar psevdo-tasodifiy sonlarni yaratishda **kriptografik algoritmlar**dan foydalanadi. Ularning asosiy xususiyati – oldindan bashorat qilib bo‘lmasligi va xavfsizlikni ta'minlashidir.

Ishlash prinsipi:

- Kriptografik xesh-funksiyalar (SHA, MD5) va shifrlash algoritmlari (AES) asosida ishlaydi.
- Har bir bosqichda ma’lumotlar murakkab matematik operatsiyalar yordamida o‘zgartiriladi.

Afzalliklari:

- Xavfsiz va oldindan aytib bo‘lmaydi.
- Kriptografiya tizimlari uchun mos.

Kamchiliklari:

- Tezligi nisbatan past.

Misol:

Windows OS'da: *CryptGenRandom*

Linux OS'da: */dev/random*

Tasodifiy sonlar algoritmlarining qo'llanilish sohalari

Tasodifiy sonlar va ularni yaratish algoritmlari quyidagi sohalarda keng qo‘llaniladi:

1. **Kriptografiya:**
   - Ma'lumotlarni shifrlash uchun xavfsiz kalitlar yaratishda, parollar generatsiyasida va xavfsiz aloqa tizimlarida ishlatiladi.
   - Masalan: SSL/TLS protokollari, RSA kabi shifrlash tizimlari.
2. **Kompyuter o‘yinlari:**
   - O‘yin ichidagi hodisalar, masalan, dushmanlar paydo bo‘lishi, bonuslar yoki tanga hosil bo‘lishini tasodifiylashtirishda qo‘llaniladi.
3. **Statistik modellashtirish va simulyatsiya:**
   - Monte-Karlo usuli kabi statistik metodlar tasodifiy sonlardan foydalanadi.
   - Moliya, fizika, meteorologiya va logistika sohalarida prognozlar yaratish uchun ishlatiladi.
4. **Sun’iy intellekt va mashinani o‘rganish:**
   - Neyron tarmoqlarining boshlang‘ich vaznlarini tasodifiy qiymatlar bilan berishda, gradient tushish algoritmlarida qo‘llaniladi.
5. **Ilmiy tadqiqotlar va eksperimentlar:**
   - Tasodifiy namuna olish, modellashtirish va eksperiment natijalarini aniqlashda ishlatiladi.

Masala:

Foydalanuvchiga kunlik reja yaratish dasturini ishlab chiqamiz. Reja har soat

uchun tasodifiy mashg'ulotni tanlaydi, lekin bir xil mashg'ulot bir necha soatga qo'yilmasligi kerak.

C# dasturlash kodida masalaning yechimi:

```
using System;
using System.Collections.Generic;
class Program
{
    static void Main(string[] args)
    {
        // Mashg'ulotlar ro'yxati
        List<string> activities = new List<string>
        {
            "Sport bilan shug'ullanish",
            "Kitob o'qish",
            "Dasturlash mashqlari qilish",
            "Tashqariga chiqib sayr qilish",
            "Film tomosha qilish",
            "Ovqat tayyorlash",
            "Oilaviy suhbat",
            "Onlayn kurs o'rganish"
        };

        // Tasodifiy son generatorini yaratamiz
        Random random = new Random();

        // Kundalik reja uchun soatlar
        Dictionary<int, string> dailySchedule = new Dictionary<int, string>();

        // Mashg'ulotlarni takrorlanmasdan tasodifiy ravishda taqsimlash
        for (int hour = 8; hour <= 20; hour++) // 8:00 dan 20:00 gacha
        {
            if (activities.Count == 0)
            {
                Console.WriteLine("Mashg'ulotlar ro'yxati tugadi!");
                break;
            }

            int randomIndex = random.Next(0, activities.Count);
            string selectedActivity = activities[randomIndex];

            dailySchedule.Add(hour, selectedActivity);
            activities.RemoveAt(randomIndex); // Takrorlanishni oldini olish uchun mashg'ulotni o'chiramiz
        }

        // Kundalik rejani chiqaramiz
        Console.WriteLine("Bugungi kundalik rejangiz:");
        foreach (var item in dailySchedule)
        {
            Console.WriteLine($"{item.Key}:00 - {item.Value}");
```

```
        }

        Console.WriteLine("\nMashg'ulotlaringiz muvaffaqiyatli o'tsin!");
    }
}
```

1- natija:

```
Mashg'ulotlar ro'yxati tugadi!
Bugungi kundalik rejangiz:
8:00 - Dasturlash mashqlari qilish
9:00 - Film tomosha qilish
10:00 - Ovqat tayyorlash
11:00 - Tashqariga chiqib sayr qilish
12:00 - Onlayn kurs o'rganish
13:00 - Oilaviy suhbat
14:00 - Sport bilan shug'ullanish
15:00 - Kitob o'qish

Mashg'ulotlaringiz muvaffaqiyatli o'tsin!
```

2-natija:

```
Mashg'ulotlar ro'yxati tugadi!
Bugungi kundalik rejangiz:
8:00 - Oilaviy suhbat
9:00 - Onlayn kurs o'rganish
10:00 - Tashqariga chiqib sayr qilish
11:00 - Ovqat tayyorlash
12:00 - Sport bilan shug'ullanish
13:00 - Film tomosha qilish
14:00 - Kitob o'qish
15:00 - Dasturlash mashqlari qilish

Mashg'ulotlaringiz muvaffaqiyatli o'tsin!
```

Tasodifiy sonlarni yaratishda haqiqiy va psevdo-tasodifiy algoritmlar qo‘llaniladi. Haqiqiy tasodifiy generatorlar tabiiy jarayonlardan foydalanadi, ammo ularning ishlashi sekin va maxsus apparat talab qiladi. Psevdo-tasodifiy generatorlar esa matematik algoritmlar yordamida samarali sonlar hosil qiladi.

Foydalanilgan adabiyotlar:

1. Knuth, D. E. (1997). The Art of Computer Programming, Volume 2: Seminumerical Algorithms. 3rd ed. Addison-Wesley.
2. L’Ecuyer, P. (2001). "A review of uniform random number generators." ACM Computing Surveys (CSUR), 33(1), 1–31.
3. Devroye, L. (1986). Non-Uniform Random Variate Generation. Springer-Verlag.

4. Shannon, C. E. (1949). "Communication theory of secrecy systems." The Bell System Technical Journal, 28(4), 656-715.
5. Aristidou, A., & Quas, A. (2019). "Random Number Generators in Quantum Computing: A Review." Quantum Information Processing, 18(7), 218.
6. Jäckel, P. (2002). Monte Carlo Methods in Finance. Wiley.
7. Moser, D. L., & Smith, D. J. (2006). "A new approach to pseudo-random number generation." Computers & Mathematics with Applications, 51(7), 1047–1059.
8. Marsaglia, G. (2003). "The Marsaglia Random Number Generators." Journal of Statistical Software, 8(5), 1-12.
9. Farmonov, S., & Nazirov, A. (2023). C# DASTURLASH TILIDA GRAY KODI BILAN ISHLASH. B CENTRAL ASIAN JOURNAL OF EDUCATION AND INNOVATION (T. 2, Выпуск 12, сс. 71–74). Zenodo.
10. Farmonov, S., & Toirov, S. (2023). NETDA DASTURLASHNING ZAMONAVIY TEXNOLOGIYALARINI O'RGANISH. *Theoretical aspects in the formation of pedagogical sciences*, *2*(22), 90-96
11. Farmonov Sherzodbek Raxmonjonovich, & Rustamova Humoraxon Sultonbek qizi. (2024). C# DASTURLASH TILIDA TO'PLAMLAR BILAN ISHLASH. Ta'lim Innovatsiyasi Va Integratsiyasi, 11(10), 210–214. Retrieved from http://web-journal.ru/index.php/ilmiy/article/view/2480.
12. Farmonov, S. R., & qizi Xomidova, M. A. (2024). C# VA JAVA DASTURLASH TILLARIDA FAYLLAR BILAN ISHLASHNING TURLI USULLARINING SAMARADORLIGI HAQIDA. *Zamonaviy fan va ta'lim yangiliklari xalqaro ilmiy jurnal*, *1*(9), 45-51.
13. Farmonov, S. (2023). C# DASTURLASH TILIDA GRAY KODI BILAN ISHLASH. *Центральноазиатский журнал образования и инноваций*, *2*(12 Part 2), 71-74.