6-amaliy ish

Mavzu: Soxta tasodifiy raqamlar generatorini va uning dasturiy ta'minotini yaratish

Ishning maqsadi: psevdo tasodifiy sonlar generatorlarini bilish ko'nikma va ko'nikmalarni egallash.

Nazariy qism

Birinchidan, tasodifiy sonlarni yaratish nazariyasining asosiy tushunchalarining ta'riflarini beramiz.

Ta'rif 1. Tasodifiy son-tasodifiy o'zgaruvchining amalga oshirilishini ifodalovchi son [6].

Ta'rif 2. Deterministik algoritm-bir xil kirish qiymatlarida bir xil chiqish qiymatlarini qaytaradigan algoritm.

Ta'rif 3. Soxta tasodifiy son-tasodifiy son sifatida ishlatiladigan deterministik algoritm tomonidan olingan son.

Ta'rif 4. Jismoniy tasodifiy son (haqiqiy tasodifiy) – ba'zi jismoniy hodisalar asosida olingan tasodifiy son.

Odatda, tasodifiy sonni yaratish ikki bosqichdan iborat:

1. normallashtirilgan tasodifiy sonni yaratish (ya'ni 0 dan 1 gacha teng taqsimlangan);

2. r\_i normallashtirilgan tasodifiy sonlarni berilgan taqsimot qonuni bo'yicha yoki kerakli oraliqda taqsimlangan tasodifiy x sonlarga aylantirish.

Ta'rif 5. Tasodifiy bit generatori (gsb) — bu statistik jihatdan mustaqil va xolis bitlarning ketma-ketligini chiqaradigan (ya'ni taqsimot qonuniga bo'ysunadigan)qurilma yoki algoritm

Tasodifiy bit generatori bir tekis taqsimlangan tasodifiy sonlarni yaratish uchun ishlatilishi mumkin. Masalan, [0;n] oralig'idagi tasodifiy butun sonni [lg n] + 1 uzunlikdagi tasodifiy bitlarning hosil bo'lgan ketma-ketligidan uni tegishli hisoblash tizimiga aylantirish orqali olish mumkin. Agar olingan butun son n dan katta bo'lsa, uni tashlab yuborish va boshqa bit ketma-ketligini yaratish mumkin.

Shuning uchun, biz tasodifiy sonlar generatori atamasini tasodifiy bit generatori atamasi bilan teng ravishda ishlatamiz.

Tasodifiy sonlar generatorlari raqamlarni olish usuli bo'yicha quyidagilarga bo'linadi:

\* uskuna;

\* jadvalli;

\* algoritmik.

Jadval generatorlari tasodifiy sonlar manbai sifatida tasdiqlangan o'zaro bog'liq bo'lmagan raqamlarni o'z ichiga olgan oldindan tayyorlangan jadvallardan foydalanadilar va bu tushunchani qat'iy tushunishda generator emas. Ushbu usulning kamchiliklari aniq: raqamlarni saqlash uchun tashqi manbadan foydalanish, cheklangan ketma-ketlik, qiymatlarni oldindan belgilash. Jadval usuliga misol sifatida kitobni keltirish mumkin.

Tasodifiy ketma-ketliklarning apparat generatorlari (haqiqiy) entropiya manbasiga ega bo'lishi kerak. O'zaro bog'liq bo'lmagan va statistik jihatdan mustaqil raqamlarni yaratadigan entropiya manbalaridan foydalanadigan generatorlarni ishlab chiqish juda qiyin vazifadir. Bundan tashqari, ko'pgina kriptografik dasturlar uchun bunday GPSCH o'rganish mavzusi va qarama-qarshi tomonning ta'siri bo'lmasligi kerak. Kriptografik jihatdan barqaror tasodifiy sonlar generatorlari to'rtinchi bo'limda muhokama qilinadi.

Algoritmik generator-bu fizik generator va deterministik algoritmning kombinatsiyasi. Bunday generator fizik generator chiqishidan olingan cheklangan ma'lumotlar to'plamidan foydalanib, asl sonlarning o'zgarishi bilan uzun sonlar ketma-ketligini hosil qiladi. Ushbu turdagi generatorlar boshqa turdagi tasodifiy sonlar generatorlariga nisbatan aniq afzalliklari tufayli katta qiziqish uyg'otadi. Algoritmik GPSCHLARNING xususiyatlari, afzalliklari va kamchiliklarini tahlil qilish ushbu kitobning asosiy mavzusidir.

#include <iostream>

unsigned int PRNG()

{

// Bizning boshlang'ich raqamimiz 4 541

static unsigned int seed = 4541;

// Biz boshlang'ich raqamni olamiz va uning yordami bilan yangi qiymat hosil qilamiz.

// Juda katta raqamlardan foydalanish (va ortiqcha to'ldirish) tufayli keyingi raqamni avvalgisiga asoslanib taxmin qilish juda qiyin

seed = (8253729 \* seed + 2396403);

// Boshlang'ich raqamni oling va 0 dan 32767 gacha bo'lgan qiymatni qaytaring

return seed % 32768;

}

int main()

{

// 100 ta tasodifiy sonni chiqarish

for (int count=0; count < 100; ++count)

{

std::cout << PRNG() << "\t";

// Agar biz 5 ta raqamni chiqargan bo'lsak, unda biz yangi satr belgisini joylashtiramiz

if ((count+1) % 5 == 0)

std::cout << "\n";

}

}

Shakl: - Ketma-ketlikni yaratish oynasi

№ Generator parametrlari

a=4, b=7, c=9, d=5, m=13

a=3, b=5, c=9, d=7, m=11

a=7, b=7, c=4, d=3, m=31

a=4, b=7, c=9, d=5, m=17

a=7, b=5, c=9, d=8, m=13

a=4, b=7, c=9, d=5, m=13

a=11, b=6, c=9, d=5, m=17

a=8, b=7, c=11, d=4, m=19

a=6, b=3, c=9, d=8, m=19

a=4, b=7, c=9, d=5, m=13

a=8, b=7, c=9, d=5, m=11

a=4, b=7, c=9, d=5, m=23

a=4, b=5, c=9, d=5, m=13

a=6, b=7, c=9, d=11, m=17

a=6, b=8, c=4, d=3, m=19

a=11, b=7, c=8, d=5, m=23

a=11, b=7, c=9, d=8, m=29

a=7, b=7, c=7, d=5, m=29

a=9, b=7, c=9, d=5, m=23

a=5, b=7, c=11, d=5, m=31

a=8, b=7, c=9, d=11, m=17

a=12, b=7, c=8, d=10, m=19

a=12, b=7, c=3, d=10, m=19

a=7, b=11, c=5, d=9, m=23

a=12, b=5, c=9, d=7, m=17

a=7, b=4, c=8, d=11, m=31

a=10, b=6, c=12, d=11, m=29

Vazifa

1. Yuqoridagi parametrlardan foydalanib, mos keladigan osilatorlar asosida ketma-ketliklar yarating va davrni hisoblang.

Xavfsizlik masalalari

1. Psevdo tasodifiy ketma-ketliklarni yaratadigan generatorlarga qanday talablar qo'yiladi?

2. Soxta tasodifiy ketma-ketliklarni yaratadigan kriptografik algoritmlarni sanab o'ting.

3. Soxta tasodifiy ketma-ketlikni shakllantirish uchun kriptografiyada chiziqli mos keladigan generatorlardan foydalanish mumkinmi?

4. Blokli shifrlash algoritmlari psevdo tasodifiy ketma-ketlikni yaratish uchun generator sifatida ishlatilishi mumkinmi?