Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «САРАТОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

ТЕОРИЯ ПСЕВДОСЛУЧАЙНЫХ ГЕНЕРАТОРОВ ОТЧЕТ ПО ПРАКТИЧЕСКОМУ КУРСУ

| студента 4 курса 431 группы |
|--|
| факультета компьютерных наук и информационных технологий |
| Мухи Семена Андреевича |
| фамилия, имя, отчество |
| Научный руководитель |
| Ст. преподаватель |
| Слеповичев |
| подпись, дата |

Саратов 2024

Задание 2. Преобразование ПСЧ к заданному распределению

Необходимо создать программу, преобразовывающую ПСЧ в другую последовательность ПСЧ с заданным распределением. Входные параметры для алгоритмов передаются с помощью файла, название которого указывается в строке параметров запуска программы (p1, p2, p3). Преобразованные числа записываются в файл distr-xx.dat, где <xx> – код распределения. На вход в качестве последовательности ПСЧ подаётся последовательность, сгенерированная с помощью аддитивного генератора с входными параметрами: /g:add /n:10000 /i:128;9;49.

1. Стандартное равномерное распределение с заданным интервалом

Описание алгоритма:

Функция распределения $0 \le x < 1$: f(x) = 1

Если стандартное равномерное случайное число U получено методом, установленным в предыдущем параграфе, то равномерное случайное число должно быть получено в соответствии со следующей формулой: Y = b * U + a.

Параметры запуска программы:

/d:st /p1:0 /p2:1 /f:out.txt

Исходный текст алгоритма:

```
u = x[i] % 1024
y = p2 * u + p1
y = format(y, '.4f')
res.append(y)
return res
```

135.0000 38.0000 101.0000 19.0000 75.0000 140.0000 95.0000 162.0000 13.0000 201.0000 43.0000 198.0000 28.0000 158.0000 170.0000 146.0000 247. 00 166.0000 455.0000 844.0000 940.0000 308.0000 124.0000 866.0000 359.0000 304.0000 367.0000 944.0000 940.0000 558.0000 209.0000 286.0000 71.000 80.0000 29.0000 469.0000 5.0000 567.0000 213.0000 837.0000 445.0000 11.0000 631.0000 911.0000 659.0000 23.0000 1005.0000 898.0000 416.0000 912.0000 427.0000 856.0000 44.0000 498.0000 256.0000 94.0000 931.0000 595.0000 947.0000 219.0000 303.0000 578.0000 102.0000 436.0000 000 792.0000 484.0000 546.0000 292.0000 966.0000 874.0000 663.0000 951.0000 758.0000 240.0000 45.0000 888.0000 873.0000 755.0000 306.0000 238 3.0000 385.0000 728.0000 52.0000 712.0000 865.0000 185.0000 833.0000 159.0000 35.0000 656.0000 714.0000 571.0000 92.0000 668.0000 981.0000 2 $000\ 740.0000\ 24.0000\ 245.0000\ 976.0000\ 976.0000\ 181.0000\ 812.0000\ 893.0000\ 190.0000\ 586.0000\ 708.0000\ 683.0000\ 670.0000\ 105.0000\ 944.0000\ 556.0000\ 971.0000\ 860.0000\ 712.0000\ 362.0000\ 523.0000\ 87.$ 916,0000 914,0000 738,0000 665,0000 362,0000 419,0000 353,0000 765,0000 806,0000 577,0000 455,0000 127,0000 615,0000 141,0000 581,0000 516,00 00 344.0000 160.0000 928.0000 182.0000 70.0000 946.0000 246.0000 635.0000 781.0000 711.0000 508.0000 713.0000 4.0000 893.0000 70.0000 977.000 $000\ 222.0000\ 777.0000\ 946.0000\ 559.0000\ 45.0000\ 537.0000\ 402.0000\ 327.0000\ 483.0000\ 547.0000\ 456.0000\ 421.0000\ 982.0000\ 443.0000\ 985.0000\ 13.\\0000\ 153.0000\ 633.0000\ 735.0000\ 904.0000\ 991.0000\ 57.0000\ 787.0000\ 9.0000\ 322.0000\ 211.0000\ 893.0000\ 660.0000\ 566.0000\ 388.0000\ 210.0000\ 401$ $000\ 742.0000\ 52.0000\ 1011.0000\ 295.0000\ 118.0000\ 68.0000\ 856.0000\ 810.0000\ 984.0000\ 63.0000\ 757.0000\ 764.0000\ 443.0000\ 967.0000\ 614.0000\ 59.6000\ 935.0000\ 716.0000\ 62.0000\ 814.0000\ 676.0000\ 514.0000\ 573.0000\ 392.0000\ 224.0000\ 314.0000\ 272.0000\ 36.0000\ 488.0000\ 215.0000\ 634.0006$ $0000\ 718.0000\ 494.0000\ 717.0000\ 177.0000\ 177.0000\ 794.0000\ 360.0000\ 385.0000\ 667.0000\ 192.0000\ 256.0000\ 363.0000\ 173.0000\ 627.0000\ 360.0000\ 472.0000\ 42.0000\ 272.0000\ 192.0000\$ 664.0000 665.0000 484.0000 934.0000 756.0000 868.0000 289.0000 779.0000 510.0000 301.0000 384.0000 660.0000 920.0000 510.0000 510.0000 67.000 6000 600002.0000 146.0000 548.0000 15.0000 47.0000 928.0000 21.0000 352.0000 173.0000 317.0000 582.0000 711.0000 693.0000 52.0000 786.0000 827.0000 25.0000 995.0000 650.0000 782.0000 131.0000 828.0000 442.0000 356.0000 58.0000 330.0000 960.0000 81.0000 212.0000 138.0000 625.0000 373.0000 21 463.0000 971.0000 131.0000 860.0000 324.0000 125.0000 444.0000 445.0000 481.0000 844.0000 725.0000 625.0000 253.0000 287.0000 103.0000 981.00 0000 404,0000 79,0000 272,0000 479,0000 994,0000 8,0000 475,0000 25,0000 766,0000 607,0000 851,0000 933,0000 414,0000 385,0000 882,0000 422,6 Стр 1, стлб 1 100% Windows (CRLF)

2. Треугольное распределение

Описание алгоритма:

Функция распределения
$$a - b \le x < a + b$$
: $f(x) = \frac{b - |a - x|}{b^2}$

Если стандартные случайные числа U1 и U2 независимо получены методом генерации стандартного равномерного числа, то случайное число Y, подчиняющееся треугольному распределению, определяют по формуле: Y = a + b * (U1 + U2 - 1).

Параметры запуска программы:

/d:tr /p1:1 /p2:2 /f:out.txt

Результат работы программы:

$$u1 = x[i - 1] % 1024$$

 $u2 = x[i] % 1024$
 $y = p1 + p2 * (u1 + u2 - 1)$
 $y = format(y, '.4f')$
res.append(y)

return res

Результат работы программы:

3. Общее экспоненциальное распределение

Описание алгоритма:

Функция распределения $x \ge a$, $f(x) = \frac{1}{b} * exp(-\frac{x-a}{b})$

Случайное число, соответствующее экспоненциальному распределению, получают по формуле: Y = -b * ln(U) + a.

Параметры запуска программы:

/d:ex /p1:1 /p2:2 /f:out.txt

Исходный текст алгоритма:

return res

Sath-Ec.dat-Encouser

Basia Tipsaza Gepusar Bag Capsaza

Radio Tipsaza Gepusar Bag Cap

4. Нормальное распределение

Описание алгоритма:

Функция распределения
$$f(x) = \frac{1}{\sqrt{2\pi b}} exp\{-1/2b2(x-a)2\}$$

Преобразование:

$$y1, y2 = nr(x1, x2, a, b)$$
: $y1 = a + b * \sqrt{-2 \ln \ln (1 - U(x1))} \cos(2\pi U(x2))y2 = a$

Параметры запуска программы:

/d:nr /p1:1 /p2:2 /f:out.txt

Исходный текст алгоритма:

return res

Пример запуска программы:

Office Action Companies | Part |

5. Гамма распределение

Описание алгоритма:

Случайное число Y, подчиняющееся гамма распределению, определяют по формуле: $Y = a - bln\{(1 - U_i)(1 - U_{i+1})\}$.

Параметры запуска программы:

/d:gm /p1:2 /p2:3 /f:out.txt

Исходный текст алгоритма:

```
def gm(p1, p2, p3, file name):
    x = []
    with open(file name) as f:
        for line in f:
             for a in line.split():
                 x.append(int(a))
    res = []
    left border = 1
    right border = len(x)
    for i in range(left border, right border):
        u = []
        for j in range(p3):
            u.append(x[i - j] % 1024)
        u mult = 1
        for j in range(len(u)):
            u \text{ mult} = u \text{ mult} * (1 - u[j])
        y = p1 - p2 * math.log1p(math.fabs(u mult))
        y = format(y, '.4f')
        res.append(y)
    return res
```

Результат работы программы:

distr-gm.dat – Блокно

6. Логнормальное распределение

Описание алгоритма:

Функция распределения
$$f(x) = \frac{1}{\left(\sqrt{2\pi\left\{\frac{x-a}{b}\right\}}\right)\exp(xp\left\{-\frac{1}{2}\left(\frac{x-a}{b}\right)2\right\})} \ge a$$

Преобразование:

$$y1, y2 = lognorm(x1, x2, a, b): z1, z2 = norm(x1, x2, 0, 1, m)y1 = a + exp(b - z1)y$$

Стр 1, стлб 12340 100% Windows (CRLF) UTF-8

Случайное число Y, подчиняющееся логнормальному распределению, определяют по формуле: Y = a + exp(b - U).

Параметры запуска программы:

/d:ln /p1:1 /p2:2 /f:out.txt

Исходный текст алгоритма:

```
def ln(p1, p2, file name):
    x = []
    with open(file name) as f:
        for line in f:
            for a in line.split():
                x.append(int(a))
    res = []
```

```
left_border = 0
right_border = len(x)
for i in range(left_border, right_border):
    u = x[i] % 1024
    y = math.exp(p2 - u) + p1
    y = format(y, '.4f')
    res.append(y)
return res
```

distr-In.dat – Блокнот

Pakin Fipaekka Popksat Bug Cnpaekka

| 7.4764 8.1199 7.6956 8.2532 7.8672 7.4448 7.7344 7.3079 8.2958 7.0721 8.0852 7.0900 8.1897 7.3326 7.2588 7.4072 6.8054 7.7212 6.5667 7.8806 6.9315 7.827 ^
2974 8.1477 5.9656 6.4643 5.1207 7.1377 6.1685 8.0438 4.8748 3.9078 6.5459 5.7754 6.2234 8.0507 4.2186 5.1815 6.4643 3.9953 4.7300 5.7152 4.0622 7.2283 |
70 5.1006 8.2661 8.02695 4.7264 7.0014 3.8739 8.2674 4.8710 6.2962 8.2958 7.9482 5.8270 5.9948 5.5880 7.2040 8.1408 4.3204 8.1303 5.6084 8.3864 5.0017 7.1980 5. |
8.2745 4.7776 4.7924 5.6922 4.6614 5.9930 3.8851 8.3316 5.0886 5.6669 3.4215 5.6240 7.9754 6.3221 5.6785 4.3273 4.8222 8.2603 7.0603 5.2308 6.1033 7.774 |
3264 8.1408 4.3938 4.6793 5.2308 7.7541 4.8484 3.8349 6.8956 5.0766 7.3326 4.6650 5.9270 4.5941 5.2639 5.7014 4.0802 4.0593 6.7210 6.5612 7.5848 7.0190 |
14.8672 7.1317 7.4891 3.8349 4.7856 5.2556 5.9366 3.8543 4.3731 7.3079 7.3017 7.5720 7.0603 4.0652 6.3325 4.3896 5.8317 6.6876 5.9126 7.9076 4.6294 6.969 |
31935 4.2757 4.1656 3.7530 7.1859 7.9211 4.2060 6.5287 4.5190 4.7373 5.3100 5.7198 7.7673 6.2806 7.3326 4.0659 5.9126 7.9076 4.6294 6.960 |
314 3.9366 4.9783 3.7263 4.0059 5.3184 4.8522 5.1530 4.5627 8.2461 6.4964 4.0089 4.3929 5.7336 5.2806 3.9306 4.0443 7.1919 7.9211 4.5906 4.2280 3.9392 4. |
315 4.2578 4.4801 8.2179 6.6656 5.5630 6.3378 7.8487 9.193 4.6527 8.2461 6.4964 4.0089 4.3929 5.7336 5.2806 3.9306 4.0443 7.1919 7.9211 4.5906 4.2280 3.9392 4. |
316 5.6667 4.5801 8.0232 3.7530 6.5396 7.5848 7.9143 4.2029 4.3501 3.8266 7.9482 4.5280 4.5040 5.7941 3.8739 5.9088 3.9398 5.7988 7.9685 8.0369 8.
317 5.1243 4.6526 6.5975 5.0331 8.0095 5.6330 6.3337 8.6365 6.3373 5.8485 9.3976 7.5168 4.4666 4.0039 5.5257 6.8567 7.9754 4.5906 5.7746 3.7990 5.8270 3.8515 18 6.5667 4.5801 8.0232 3.7530 6.5396 7.5848 7.9143 4.2029 4.3501 3.8266 7.9482 4.5280 4.5040 5.7941 3.8739 5.0494 4.2280 7.3506 6.4007 4.2438 6.7828 4.6368 8.4528 6.2365 7.9754 3.8938 7.9368 5.7868 5.7868 5.7868 5.7868 5.7868 5.7868 5.7868 5.7868 5.7868 5.7868 5.7868 5.7868 5.7868 5.78

7. Логистическое распределение

Описание алгоритма:

Случайное число Y, подчиняющееся логистическому распределению, определяют по формуле:

$$Y = a + b * ln(\frac{U}{1-U}).$$

Параметры запуска программы:

/d:ls /p1:1 /p2:2 /f:out.txt

Исходный текст алгоритма:

import math

```
### distr-E.dat — Борожног

#
```

8. Биномиальное распределение

Описание алгоритма:

Преобразование:

```
y = binominal(x, a, b, m): u = U(x) s = 0 k = 0 loopstart:
```

```
s = s + Cbk ak (1 - a)b - k if s > u: y = k
Завершить
  if k < b - 1: k = k + 1 перейти к loopstart
  y = b
    Коэффициент C_b^k = \frac{b!}{k!(b-k)!}
    Параметры запуска программы:
    /d:bi /p1:0.2 /p2:10 /f:out.txt
    Исходный текст алгоритма:
    def bi(p1, p2, file name):
        x = []
         with open(file name) as f:
             for line in f:
                 for a in line.split():
                     x.append(int(a))
         res = []
         left border = 0
         right border = len(x)
         for i in range(left border, right border):
             u = x[i] / 1024
             y = 0
             s = 0
             k = 0
             while (True):
                              s = s + (math.factorial(p2)) /
(math.factorial(k) * math.factorial(p2 - k))) * (p1 ** k) *
                      ((1 - p1) ** (p2 - k))
                 if s > u:
                     y = k
                     break
                 if k < p2 - 1:
                     k = k + 1
                     continue
```

```
y = p2
break
res.append(y)
return res
```