

Ц840а

0-756

4892/2-76

СООБЩЕНИЯ
ОБЪЕДИНЕННОГО
ИНСТИТУТА
ЯДЕРНЫХ
ИССЛЕДОВАНИЙ

ДУБНА

6/ХИ-76



11 - 10130

Г.А.Ососков, Г.А.Погодина

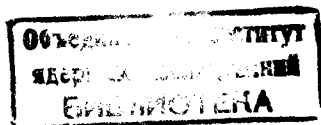
ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ
ДЛЯ МАЛОРАЗРЯДНЫХ ЭВМ

1976

11 - 10130

Г.А.Ососков, Г.А.Погодина

ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ
ДЛЯ МАЛОРАЗРЯДНЫХ ЭВМ



В работе /1/ был предложен алгоритм генерации псевдослучайных чисел, особенно удобный для применения его на малоразрядных ЭВМ.

Метод был основан на известной /2/ формуле

$$x_{n+1} \equiv x_n(2^\alpha + 1) + C \pmod{2^P},$$

применялся к числам x_n , представленным в ЭВМ с двойной точностью, и фактически состоял в замене умножения на 2^α пересылкой половины числа x_n из одной ячейки памяти в другую. Для реализации этого алгоритма необходимы две рабочие ячейки, α и β , куда до начала счёта должны быть засланы соответственно правая и левая половины 2^p -разрядного начального числа x_0 . Должна быть также записана нечётная P -разрядная константа C . Если обозначить через $\langle x \rangle$ содержимое ячейки с адресом x , а знаком \Rightarrow засылку, то генерация очередного случайного числа может быть выполнена с помощью следующих операций:

1. $\langle \alpha \rangle + \langle \beta \rangle \Rightarrow \alpha$,
 2. $\langle \beta \rangle + C \Rightarrow \beta$,
 3. При переполнении в п.2 $\langle \alpha \rangle + 1 \Rightarrow \alpha$,
 4. $\langle \alpha \rangle$ выдаётся как текущее случайное число.
- Сложение в п.п.1 и 3 выполняется по $\text{mod } 2^P$.

В данной работе приведены конкретные реализации этого алгоритма для наиболее распространенных в настоящее время малых ЭВМ "Электроника-100", ТРА-1001 (12 разрядов), М-6000 и М-400 (16 разрядов) в виде программ - генераторов случайных чисел (ГСЧ12, ГСЧ16А и ГСЧ16В).

Поскольку теория гарантирует полный период псевдослучайных последовательностей, равный 2^{24} для ГСЧ12 и 2^{32} для ГСЧ16, и достаточно хорошие их корреляционные свойства, а также из-за трудностей реализации на малых ЭВМ полной системы тестовой проверки в объёме, рекомендуем, например, в работе /3/, мы ограничились при непосредственной проверке этих генераторов на самих малых ЭВМ только вычислением величины

$$\chi^2 = \frac{32}{N} \sum_{i=1}^{32} \left(\nu_i - \frac{N}{32} \right)^2$$

при нарастающем числе испытаний N ($N = 2000, 4000, \dots, 32000$) ✓
 (здесь обозначено через ν_i количество точек, попавших в
 i -ую ячейку одномерной гистограммы, $i = \overline{1, 32}$).

Выход величины χ^2 за 1% -ное критическое значение для распределения χ^2 с 31 степенью свободы не был зафиксирован ни в одной серии испытаний.

Развитие дисплейной техники последних лет предоставило возможность весьма наглядной и оперативной оценки зависимости последовательных пар псевдослучайных чисел $(x_1, x_2), (x_3, x_4), \dots, (x_n, x_{n+1})$ путём использования их как координат точек, выводимых на экран точечного дисплея на ЭЛТ/4/.

Наличие любой связи между парами должно проявиться при росте числа высвечиваемых точек в виде полос и пятен, нарушающих равномерность засветки. На фотографиях, снятых с экрана дисплея при высвечивании 512, 2048, 65 тыс. и 131 тыс. точек после работы ГСЧ16А и ГСЧ12, только на последних можно заметить неравномерность засветки в виде неясных полос.

В Приложении даны автокодные тексты ГСЧ12, ГСЧ16А и ГСЧ16В.

В заключение авторы выражают свою искреннюю благодарность В.И.Приходько и Н.П.Алексеевой за помощь при работе с дисплеем и А.Д.Полынцева за консультации в программировании на ЭВМ М-6000.

Приложение

Автокодные тексты программ-генераторов случайных чисел ГСЧ 12, ГСЧ 16А и ГСЧ 16В.

1. ГСЧ 12 (для ЭВМ "Электроника-100", ТРА-1001, РДР-8).

```

* RNG12
1000 0000 RNG , 0000
1001 7300 CLA CLL
1002 1216 TAD A
1003 1217 TAD B
1004 3216 DCA A
1005 7100 CLL
1006 1217 TAD B
1007 1220 TAD C
1010 3217 DCA B
1011 7004 RAL
1012 1216 TAD A
1013 3216 DCA A
1014 7100 CLL
1015 5600 JMP I RNG12
1016 4344 A , 4344
1017 3361 B , 3361
1020 1131 C , 1131
    
```

2. ГСЧ 16А (для ЭВМ М-6000, НР-2116А)

```

ASMB, A, L, B
05000
05001 124357 A OCT 5000B
05002 036143 B OCT 124357
05003 117113 C OCT 36143
05004 000000 BEGIN NOP 117113
05005 000040 CLE
05006 063001 LDA A
05007 043002 ADA B
05010 073001 STA A
05011 000040 CLE
05012 063002 LDA B
05013 043003 ADA C
05014 073002 STA B
05015 002400 CLA
05016 001600 BIA
05017 043001 ADA A
05020 073001 STA A
05021 127004 JMP BEGIN, I
    
```

3. ГСЧ I6B (для ЭВМ М-400, НР-2И16А)

```
000000 A=%0
000001 B=%1
000002 C=%2
000007 PC=%7
000000 060100 GEN:ADD B,A
000002 060200 ADD C,A
000004 103001 BCC .+4
000006 005200 INC A
000010 000207 RTS PC
000000 .EOT
```

Это простейший вариант программы, использующий три индекс-регистра. До первого обращения к этому генератору в вызывающей программе должна быть выполнена следующая последовательность команд:

```
MOV # 124357,A
MOV # 36143,B
MOV # 117113,C ,
```

осуществляющая засылку константы С и начального значения x_0 в ячейки А и В.

ЛИТЕРАТУРА

1. П.Г.Акишин, Г.А.Ососков. Сообщение ОИАИ Р5-84И1, Дубна, 1974.
2. A.Rotenberg. A new pseudorandom generator. Ж.АСМ.,v.7,N1,1960.
3. Г.А.Ососков, Т.Войкова. Препринт ОИАИ Д10-7707, Дубна, 1974.
4. Х.Дорух и др. Сообщение ОИАИ Р11-8494, Дубна, 1974.

Рукопись поступила в издательский отдел
24 сентября 1976 года.