

UNIVERSITY OF ILLINOIS

DIGITAL COMPUTER

LIBRARY ROUTINE V9 - 216

TITLE Generate 40-bit Random Numbers (SADCI Only)
 TYPE Closed
 DURATION 3 milliseconds
 LENGTH 27 words plus 5 words at S3
 DESCRIPTION Upon standard entry this routine replaces the five pseudo-random numbers stored at the location specified (as an integer) by pre-set parameter S3 by five new ones. The five starting numbers (in sexadecimal form) are put in place by an interlude. The numbers are generated according to the following recursion formula

$$A_{n+5} = 7A_{n+4} + A_{n+3} - 4A_{n+2} + 3A_{n+1} + \pi(A_n)$$

where for a 40-bit number a_0, \dots, a_{39}

$$\pi(a_0, \dots, a_{39}) = a_0, a_4, a_5, \dots, a_{39}, a_1, a_2, a_3$$

The numbers have been tested and found to be random by the tests applied. Descriptions and results of the tests may be found in Internal Report No. 74, dated December 7, 1956.

The sequence has been found not to repeat within the first 10 million numbers. A list giving the five starting numbers and each succeeding 100,000 th set of five for the first 10 million numbers is given on the next page. (The first number of the first set is numbered "Q", the first number of the next set is numbered "500,000", etc.).

DATE 12/13/56 Rt: 10/29/58

PROGRAMMED BY C. Farrington

APPROVED BY D. E. Muller

lgr

LOCATION	ORDER		NOTES	PAGE 1
0	00 K(V9) K5 F 42 26L		Plant link	
1	L5 4S3 50 S3		Form A _{n+5}	
2	00 1F L4 1S3			
3	L0 2S3 00 2F			
4	L0 1S3 S4 F			
5	L4 3S3 L0 4S3			
6	40 S3 50 1S3		Form A _{n+6}	
7	00 1F L4 2S3			
8	L0 3S3 00 2F			
9	L0 2S3 L0 S3			
10	L4 4S3 S4 F			
11	40 1S3 50 2S3		Form A _{n+7}	
12	00 1F L4 3S3			
13	L0 4S3 00 2F			
14	L4 S3 L0 1S3			
15	L0 3S3 S4 F			

LOCATION	ORDER	NOTES	PAGE 2	V 9
16	40 2S3 50 3S3		Form A _{n+8}	
17	00 1F L0 S3			
18	L4 4S3 00 2F			
19	L4 1S3 L0 2S3			
20	L0 4S3 S4 F			
21	40 3S3 50 4S3		Form A _{n+9}	
22	00 1F L4 S3			
23	L0 1S3 00 2F			
24	L0 S3 L4 2S3			
25	L0 3S3 S4 F			
26	40 4S3 22 F 00 S3 02 K		Link	
0	F0 2140F 08 4011F		Starting Numbers	
1	J2 1321F 1K 1798F			
2	63 3733F 01 2535F			
3	1L 1716F 79 3747F			
4	66 584F 7S 3926F 00 (V9) 02 27K			