REF ID: A56994

MEMO ROUTING SLIP

NEVER USE FOR APPROVALS, DISAPPROVALS, CONCURRENCES, OR SIMILAR ACTIONS

	NAME OR TITLE / ORGANIZATION AND LOCATION	INITIALS / DATE		
1	Mr Friedman Sheet		✓	CIRCULATE
				COORDINATION
2			✓	FILE
				INFORMATION
3				NECESSARY ACTION
				NOTE AND RETURN
4				SEE ME
				SIGNATURE

REMARKS

FROM NAME OR TITLE	NSA-314	DATE	July
ORGANIZATION AND LOCATION	12 117	TELEPHONE	60891

DD FORM 1 FEB 50 94 REPLACES NME FORM 94, 1 FEB 49, WHICH MAY BE USED. 16—66269-2 GPO

SECRET

"ENCIPHERED MOTION" Branching Structure

Introduction:

There has been considerable interest in observational data concerning the proportion of origins, single points, and branch points of a device employing wheels stepped by enciphered motion. To this end a program was written for ATLAS II to compare the empirical results with the expectations under purely random stepping.

The probability P(i) of a branch point of multiplicity "i" for the case where there are n random stepping wheels (each of the "random" wheels steps with probability 1/2, each wheel steps independently of each other, and therefore each of the 2^n motion assumptions is equally likely) can be given by the following formula:

$$P(i) = \binom{2^n}{i}\left(\frac{1}{2^n}\right)^i\left(1 - \frac{1}{2^n}\right)^{2^n - i} \qquad (1)$$

As n increases, (1) approaches $\frac{1}{e(i!)}$ as a limit.

$$\therefore P(i) \sim \frac{1}{e(i!)} \qquad (2)$$

Note the expected number of origins and single points approaches the same value.

In the ATLAS program, rotor maze wirings were simulated and the motion determined for each setting of the rotors, and after stepping the rotors in accordance with the motion (the maze encipherment of the stepping

SECRET

pulses was carried out, etc.) a listing of the initial setting, the next four successive settings, and the 10th setting was recorded. This was done for all settings composed of core settings A, B, or C in each of the rotors stepped by the output of the maze. Examination of these runs and recognition of confluences provided additional information in that for some settings (those composed of B or C on each of the rotors stepped by the output of the maze) all possible predecessors and their immediate sucessors were present in the print out. For these settings actual enumeration would provide the number of them that were origins, single points, branch points of order 2, branch points of order 3, etc.

For example when n = 5 there are 2^5 settings which are either origins, single points, or branch points of degree two or more. We know for a certainty the character of these 32 settings since all their possible predecessors have been examined among the 3^5 initial settings.

A. The first device to be examined was a 10 wheel machine with four metric or cycle guarantee wheels and six wheels stepped by enciphered motion. Each of the latter six wheels has probability 1/2 of stepping. The following is a listing of four samples made on ATLAS. The samples differed in that the metric rotors were set to a new position before each set of runs was made. Shown also is the expected number E(i) of each kind of point for the sample observed.

~~SECRET~~

SAMPLES

	A	B	C	D	E(i)
Origins	24	22	25	27	23.4
Single points	25	22	20	16	23.7
Double points	11	16	14	15	11.8
Triple points	3	2	2	5	3.9
Quadruple points	1	1	3	1	1.0
Quintuple points	-	1	-	-	.2
	64	64	64	64	64.0

SECRET

B. The second device to be examined was a 10 wheel machine with five metric or cycle guarantee wheels and five wheels stepped by enciphered motion. Each of these five latter wheels has probability 1/2 of stepping. The following is a listing of nine samples made on ATLAS. E(i) is the expected number of branch points of multiplicity (i).

SAMPLES

	A	B	C	D	E	F	G	H	I	E(i)
Origins	9	14	13	11	12	12	15	13	11	11.6
Single points	14	8	6	11	12	14	11	6	12	12.0
Double points	7	7	11	9	4	2	4	11	5	6.0
Triple points	2	2	1	-	4	2	2	2	2	1.9
Quadruple points	-	1	1	1	-	2	-	-	1	.4
Quintuple points	-	-	-	-	-	-	-	-	1	.1
	32	32	32	32	32	32	32	32	32	32.0

Robert Sengpiehl
NSA-314
28 June 1955