~~SECRET~~

DEPTH STUDY ON THE AFSAM 109

This paper reports on the search for depths in a simulation of one year's traffic using AFSAM 109. Because the rule of motion restricts the independent motion of wheels 1, 5 and 6, the 36 distinct orientations of these wheels, in accordance with the value of $(W_5 + W_6 - W_1)$ mod 36, distribute the cycle structure into 36 mutually distinct classes. In addition the relative starting orientation of the first two wheels commits the structure to one of three mutually distinct classes associated with three cycles of the first two cycle guarantee wheels. Hence all traffic tested was restricted to lie in the same one of the 108 distinct classes. It was agreed that 50 messages in this one class would represent a generous upper bound on the maximum use of the most popular of the classes used on any one day. All of the messages were assumed to be of length 5000. The ASAF 30 compared each of the 50 messages with each of the others for depth (flush and track-in depth). The results of this traffic search appears in Appendix A.

No suitable method was devised to generate quasi-random starts which would satisfy conditions typical for 5 letter indicator systems (such as A B C D E A B C or A A B B C C D E); therefore no attempt was made to have all message starts limited in this fashion. For the depth study the indicator system was assumed to be made up of eight random letters.

~~SECRET~~

Nine notch patterns were constructed (see Appendix B). These each had 10 blocks (a stretch of notches followed by a stretch of no notches) and were calculated to be of 26 per cent saturation level in respect to propensity for producing branch points. (See "Preliminary Report on AFSAM 9 Depth Study", Robert P. Murphy).

Using these nine patterns 365 sets of eight were randomly selected and arranged and each set designated as the notch ring arrangement for the rotors taken in the fixed order of motion control and used in simulating the 50 messages involved in the depth search. (See list Appendix C, omitted in all but file copy). In order to decrease the number of changes from one day's arrangement to the next the list was sorted on the notch rings of the first wheels. This effectively recorded adjacent to one another the days with similarly placed notch rings. This order is listed in Appendix D, omitted in all but the file copy. Typical of the rest of the list is the following section.

DAY NUMBER	NOTCH RING ARRANGEMENT
334	1 2 4 7 8 3 9 5
305	1 2 4 8 5 7 9 6
222	1 2 7 6 9 5 8 3
182	1 2 7 6 3 5 6 8
243	1 2 9 3 4 8 7 6
278	1 3 8 9 2 7 6 5
228	1 3 9 4 5 6 8 2
117	1 4 3 7 8 2 6 5
191	1 4 3 9 6 8 5 7

~~SECRET~~

To aid in randomness of the generation of the staring point of the 50 messages the notch rings on the five wheels W_2, W_3, W_5, W_6. and W_7 which control the big cycle of the quasi-random generation were changed by the same method but on a less frequent basis. Appendix E shows the notch patterns and assignment to selector lines of designated wheels for this quasi-random generation.

The method used in the quasi-random setting generation is described in general in Appendix F and in detail in the above reference.

1st Lt. William H. Cornelius, Jr.
NSA-314
20 June 1955

~~SECRET~~

APPENDIX A

LIST OF DEPTHS FOUND BETWEEN MESSAGES OF LENGTH 5000

Simulated Date	Messages in Depth		
	Message Number	In Depth	Message Number
9 Jan	42	with	43
14 Feb	15	with	43
25 Feb	32	with	43
31 Mar	35	with	42
9 May	6	with	8
14 Jun	15	with	30
21 Jun	7	with	8
9 Aug	2	with	49
7 Oct	14	with	46
	20	with	23 *
11 Oct	38	with	48

LIST OF DEPTHS FOUND BETWEEN MESSAGES OF LENGTH 10,000, BUT NOT IN DEPTH DURING FIRST HALF OF ONE MESSAGE

Simulated Date	Message Number	In Depth	Message Number
3 Jan	31	with	48
6 Feb	19	with	31
7 Apr	21	with	23
18 May	10	with	50
6 Jun	5	with	35
8 Jun	26	with	33
23 Jul	4	with	18
23 Nov	30	with	50

*Note two depths of 2 were found in 7 Oct traffic

SECRET

APPENDIX B

NOTCH RINGS AVAILABLE FOR AFSAM 109 MOTION CONTROL

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
1	1	0	0	1	0	0	1	0	0	1	1	1	0	1	1	1	0	0	1	1	0	1	1	0	1	0	1	1	0	0	1	1	1	1	1	0
2	1	1	1	0	1	0	0	1	0	1	1	1	0	0	1	0	1	0	0	1	1	1	0	1	1	1	0	1	1	1	1	0	1	0	0	0
3	1	1	1	0	1	1	0	1	0	0	1	0	0	0	1	0	1	1	1	1	1	0	0	1	1	0	1	0	1	1	0	1	1	0	0	1
4	0	1	1	1	0	0	0	1	0	1	1	1	0	1	1	1	1	0	1	0	1	0	1	0	0	0	0	1	0	1	1	1	1	0	1	1
5	1	1	0	1	1	0	1	1	0	0	0	1	0	0	1	1	1	1	1	0	0	1	0	1	0	1	0	1	1	1	0	1	1	1	0	0
6	1	1	0	1	0	0	1	1	1	1	0	1	0	0	1	1	1	0	1	1	1	0	1	0	0	0	1	1	1	0	0	1	1	0	1	0
7	1	1	0	1	0	0	1	1	1	0	1	0	0	1	1	0	1	1	1	1	0	1	0	1	1	0	0	1	0	0	0	1	1	0	1	1
8	0	1	0	1	0	1	1	1	1	0	0	0	1	1	0	0	1	1	1	0	1	1	0	1	1	1	0	1	1	1	0	1	0	1	0	0
9	1	0	1	1	1	0	0	0	1	0	1	0	1	0	1	0	0	1	1	1	0	1	1	1	0	0	1	1	0	0	1	1	1	0	1	1

APPENDIX C } Included in
APPENDIX D } file copy only

SECRET

SECRET

APPENDIX E

SELECTOR LINE PATTERNS FOR "QUASI-RANDOM" MOTION CONTROL

	Ø	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	1	1	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	1	1	1	0	0	1	0	1	1	0	0	0	1	1	1
2	1	1	0	0	1	0	1	1	0	0	0	1	1	1	1	0	0	1	0	1	0	0	1	1	1	1	0	0	0	1	1	0
3	0	0	0	0	0	1	1	0	1	1	1	0	1	0	0	0	1	0	0	0	0	1	1	1	1	1	0	0	0	0	0	1
4	1	1	0	1	0	1	0	0	1	1	1	1	1	0	0	1	0	1	0	1	0	0	0	1	1	1	0	0	1	1	0	1
5	0	0	0	0	1	1	1	0	1	1	1	1	0	1	0	1	0	0	1	1	0	0	0	1	1	1	1	0	0	1	0	0
6	1	1	0	1	1	0	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	1	0	0	0	1	1	0	1	0	0	1

SECRET

APPENDIX E CONTINUED

ASSIGNMENT OF SELECTOR LINE PATTERNS FOR "QUASI-RANDOM" MOTION CONTROL

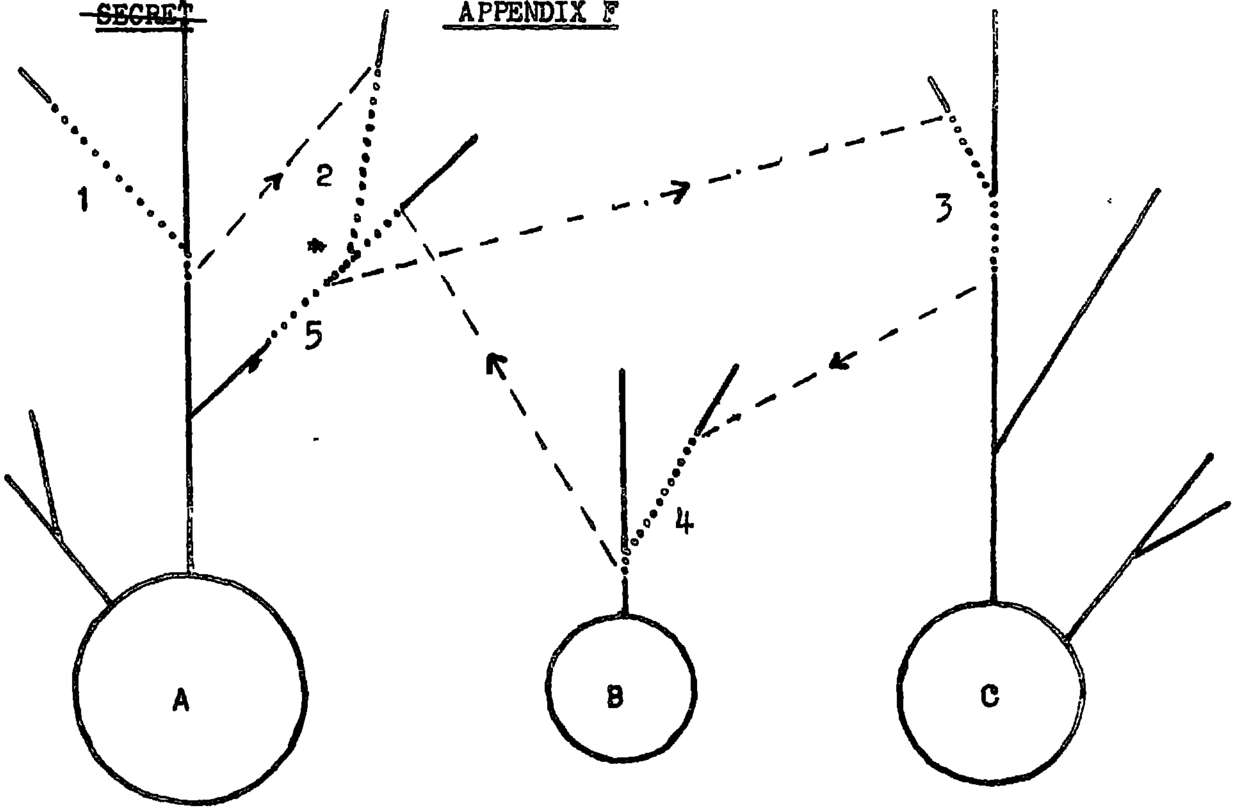
W_2	W_3	W_5	W_6	W_7	
5	3	2	1	6	.... Setting for 32 days
4	2	6	1	3	.... Setting for 34 days
6	1	3	4	5	.... Setting for 31 days
2	4	6	3	1	.... Setting for 37 days
1	2	6	3	4	.... Setting for 30 days
3	1	2	5	6	.... Setting for 37 days
4	2	3	1	5	.... Setting for 26 days
6	4	2	3	1	.... Setting for 32 days
1	4	3	6	5	.... Setting for 64 days
5	2	3	4	1	.... Setting for 52 days

SECRET

SECRET

SECRET

APPENDIX F



FUNCTIONAL DIAGRAM OF RANDOMIZER

The figure shows three cycles of the AFSAM 109. The solid lines and dotted segments show some of the branches and lead-in structure under the standard rule of motion. The dashed lines show graphically the stepping under the quasi-random motion rule from one AFSAM 109 message setting to another. An initial start is selected by a card which satisfies the condition that the setting be in the class of setting under examination. This setting is taken as the indicator of the first AFSAM 109 message see dotted line segment marked 1.

The 5000th setting of the message recorded in the memory and the quasi-random stepping rule operates for 10,000 steps to produce the initial point of the second AFSAM 109 message see digit 2. The

~~SECRET~~ APPENDIX F CONTINUED

connecting dashed lines simbolizes the qùasi-random stepping and the fact that during this rule the wheels do not obey the rules of the AFSAM 109 motion. There are shown in the Figure the first five messages generated under this complex rule. Note that message 2 and message 5 are in depth as is exhibited in the merging (see asterisk) of the segments marked 2 and 5.