(2)

PSEUDO-RANDOM NUMBERS

by

Dr. John W. Mauchly

The increasing application of random digits in the solution of problems in physics, engineering, genetics and many other sciences has made desirable a study of the feasibility of generating such numbers as they are needed in the problem at hand.

Accordingly, a routine for generating pseudo-random digits was prepared for the Binac and several hundred thousand such digits were generated. Their randomness was tested in several ways, the results of which will be described later.

The Binac routine generated a 6-digit "random" number by extracting an interior group of six digits from the 12-digit product of two "random" numbers previously obtained. The process was initiated by a group of ten 6-digit numbers arbitrarily assumed. The first product was formed by the first and sixth such input constants, the extracted "random" number replacing the fifth input constant. The instructions were then each augmented by one unit to multiply the second by the seventh constant and replace the sixth constant by the extracted "random" product. The process was continued cyclically for as many as 21,504 "random" numbers.

The right-hand two of the six digits in the "random" number were isolated and employed in a statistical study then under way. In addition, the frequency of occurrence of each possible combination of the two octal digits was tallied, X^2 computed for every 512 tallies against a random-distribution frequency, and the X^2 graded into class intervals of eight. Further, row and column sums of the 64-digit square array of tallies were compiled. Finally, a gap test was run on each digit value of the left digit of the octal pair, a tally being made for each digit value and each gap size.

The equivalent routine for generating such numbers on UNIVAC is shown on pages 4-6. The computation time per number is approximately ten milliseconds. The coding and its explanation is given on page 4; the flow chart on page 5, and a list of the codes used and their meanings on page 6. Following the routine is a page of simple block diagrams indicating the manner in which the UNIVAC carries out its operations.

The distribution of X^2 tallies (for octal class intervals) obtained from all runs combined is shown below:

X^2 for 63 degrees of freedom

Range	0	32	40	48	56	64	72	80	88	96	104	∞
Tallies	0	2	16	28	76	57	23	9	1	2	0	

Since the distribution of $(X^2/\nu)^{1/3}$ is approximately normal, the ranges above have been subjected to a cube-root transformation and the data corresponding to the above table plotted on the same chart (Figure I) with the appropriate normal curve.

As a matter of curiosity, a test was made to see what effect a very small change in the starting constants would have in the resulting sequence. Table I lists the first 256 "random" numbers generated from the ten input constants listed at the head of the table. Table II compares the first 32 such numbers with the corresponding set produced from a second group of input constants, identical with the first group except for an increase of one unit in the second constant. Identical numbers in the two sets are underlined. Those number not underlined have no recognizable resemblance to each other.

Table III lists the row and column sums of the octal-pair tallies made during six distinct runs of the routine, using different input constants. The row sums are actually frequency counts of the first digit of the pair, and the column sums are similarly counts of the second digit. The X^2 for each run, for the total of all runs, and for the ΣX^2 are given below the tallies, together with the probability that the corresponding X^2 for random digits would equal or exceed the realized values. It is obvious that the <u>second</u> digit is not sufficientl random. This is probably because the digit in question came from a position too far from the center of the product. It is likely that much better results would have been obtained by taking the octal pair from the <u>center</u> of the 12-digit span, as evidenced by the more satisfactory test results on the <u>first</u> digit of the octal pair, which was closer to the center of the product.

Table IV gives the tallies obtained in three runs of the gap test together with X^2 and probability values of such gaps as of random origin. This test was performed on the <u>fourth</u> digit from the right end of the product and appears to give satisfactory evidence of randomness. The theoretical

gap frequencies with which the observed gap frequencies were matched were calculated from the relation:

$$p_n(j) = (n-1-j)p_i^2 (1-p_i)^j$$

where $p_n(j)$ is the probability of occurrence of a gap of length j in the digit i for a group of n random digits, and p_i is the probability of occurrence of the digit i.

It should be evident from this study that it is practicable to generate "random" numbers as required in the problem, using the method outlined or a modification thereof. Such numbers may be quickly and cheaply obtained, and may be selected for the number of degrees of freedom required by the problem.

Any desired test of randomness may be incorporated in the computer routines so that, in effect, the numbers used are subject to "quality control". One of the advantages of such pseudo random sequences is that one may reproduce such a sequence at any later time in order to apply further tests, or if a sequence is known to pass all tests deemed necessary, it may be used repeatedly in independent problems.

The author is greatly indebted to a number of other persons in the Application Department of Eckert-Mauchly Computer Corporation for aid in the coding and BINAC operation.

The analysis of results was efficiently carried out by Dr. Herbert F. Mitchell, Jr.

TABLE I

PSEUDO-RANDOM OCTAL DIGITS

As generated by Binac Routine A-510-2B, using following constants:

123456 111111 222222 765432 555555
345345 456456 567567 357357 135135

	0	1	2	3	4	5	6	7
0	406554	206204	525006	376131	527002	040060	244331	215100
1	037275	015410	354567	765073	224667	107514	332414	011110
2	076007	436146	765730	717416	563767	317405	747530	256265
3	440466	365612	555172	777277	102065	167620	076024	471005
4	155412	046060	025175	120460	355260	230413	702462	537657
5	767512	330246	563642	312234	072317	644634	543753	750044
6	130225	127726	222144	362145	246575	647114	656541	721127
7	633353	220644	311274	226513	730755	533602	060657	427320
10	104343	005700	471106	355001	617003	266501	142043	332317
11	746730	516321	164466	231475	445573	317250	275151	544552
12	454410	542313	372727	417754	137635	546015	073016	001437
13	607470	314712	660252	642224	151637	271015	653301	571760
14	224372	422553	424632	327772	054061	660334	724541	545516
15	647141	762755	100641	161625	303663	404364	772614	522460
16	164223	407570	420435	047046	155555	461061	326357	237065
17	160312	626624	711042	436702	566723	530010	037771	530000
20	273255	045714	376601	273300	675120	002252	532470	245601
21	267000	037405	477641	702422	706400	427047	443211	776653
22	425032	773604	547057	054273	014357	717550	177666	704474
23	431665	515201	136347	740364	215772	346254	431155	736162
24	101261	617763	106765	136605	224241	566650	357471	112527
25	761247	761502	225624	637656	106027	652171	364472	337577
26	000775	105731	012435	654024	165471	307170	116375	310121
27	461160	430211	152342	217774	626141	002443	573113	252130
30	620465	077512	455674	645253	537066	306746	621155	015144
31	621065	343015	724015	254732	232126	567331	261111	250153
32	711133	337211	053347	030232	737210	722654	342327	666637
33	767105	033770	674722	117250	766213	657627	240146	251676
34	634062	214113	054231	245377	003571	662251	204022	256503
35	416615	251502	331032	723612	777142	337120	376566	300057
36	327133	044704	446464	566545	442264	230552	770560	603173
37	570472	130471	335623	232237	163673	461600	475633	355551

TABLE II

COMPARISON OF PSEUDO-RANDOM OCTAL NUMBERS

The first 32 pseudo-random numbers from Table I are repeated in columns 2 and 5 of the following table. The corresponding numbers generated from a second group of ten constants, identical except for the change of one unit in the second constant, are listed in columns 3 and 6 of the table. Identical numbers are underlined.

(1) No.	(2) c_2=111111	(3) c_2=111112	(4) No.	(5) c_2=111111	(6) c_2=111112
0	-436115	-436115	20	-726744	-726744
1	453545	732507	21	-144355	154034
2	336701	-030315	22	-304300	546615
3	-434360	-434360	23	164552	425741
4	252226	252226	24	273514	-635622
5	-304720	-534304	25	-022327	-154312
6	627426	-223011	26	-071324	-275204
7	-026617	-026617	27	-430512	-631455
10	-507761	-507761	30	640732	630454
11	-757147	543505	31	237064	347453
12	156033	464722	32	-433734	-430614
13	117727	-477227	33	366217	744161
14	-101523	-101523	34	120534	170067
15	-515070	763201	35	-170506	-124037
16	-054221	-103751	36	-356663	-061160
17	353152	-367272	37	-264450	-046150

TABLE III

ROW AND COLUMN SUMS OF OCTAL-PAIR TALLIES

Tally		Run No. 1	Run No. 2	Run No. 3	Run No. 4	Run No. 5	Run No. 6	Total
Row Sum: First Digit	0	2787	1810	1789	2734	1123	1725	11968
	1	2700	1842	1830	2623	1074	1647	11716
	2	2658	1761	1848	2657	1111	1680	11715
	3	2704	1818	1769	2718	1090	1676	11775
	4	2500	1679	1743	2671	1056	1651	11300
	5	2768	1837	1826	2700	1107	1653	11891
	6	2694	1769	1751	2699	1065	1650	11628
	7	2693	1820	1780	2702	1078	1630	11703
Column Sum, Second Digit	0	2736	1861	1915	2769	1146	1764	12191
	1	2752	1789	1748	2661	1036	1574	11560
	2	2669	1792	1742	2727	1146	1741	11817
	3	2581	1692	1776	2637	1096	1663	11445
	4	2760	1845	1783	2662	1156	1718	11924
	5	2676	1776	1772	2569	1041	1657	11491
	6	2697	1825	1788	2755	1085	1645	11795
	7	2633	1756	1812	2724	998	1550	11473
Total, row or column		21504	14336	14336	21504	8704	13312	93,696
First Digit :								
X^2		19.64	11.44	4.82	3.29	3.62	3.60	23.5
P		0.007	0.13	0.68	0.85	0.82	0.82	0.002
Second Digit:								
X^2		9.87	11.25	11.53	11.89	22.43	24.21	41.5
P		0.20	0.13	0.12	0.11	0.003	0.001	0.0000

Overall ΣX^2

	ΣX^2	P
First Digit---	46.41	0.2954
Second Digit--	91.18	0.0000
Both Digits--	137.59	0.0002

TABLE IV

GAP TESTS

$N_1 = 512$

Gap \ Digit	0	1	2	3	4	5	6	7	Theor. Freq.
0	10	14	13	4	9	5	6	4	8.0
1	9	4	7	17	6	7	10	3	7.0
2	7	3	3	5	6	6	6	3	6.1
3	5	10	7	8	4	5	4	7	5.3
4	4	3	6	5	8	5	7	3	4.6
5	2	6	3	3	3	4	3	3	4.1
6	0	9	2	5	5	2	7	4	3.5
7	2	2	1	3	5	2	2	1	3.1
8	5	4	3	2	1	3	1	2	2.7
9	2	1	6	1	2	5	2	3	2.4
10	3	3	2	5	0	4	3	0	2.1
11	2	2	2	4	1	2	2	1	1.8
12	2	2	2	0	0	0	3	0	1.6
13	2	2	0	1	1	1	1	1	1.4
14	0	1	2	0	1	2	3	2	1.2
15 or over	8	6	8	8	10	8	6	13	9.3
Total	63	72	67	71	62	61	66	50	64.0

$\Sigma X^2 = 130.6281$; $\nu = 127$; $P = 0.394$

$N_2 = 4096$

Gap \ Digit	0	1	2	3	4	5	6	7	Theor. Freq.
0	60	67	71	55	60	68	58	63	63.98
1	52	47	46	61	67	71	57	47	55.97
2	55	50	41	53	48	57	35	47	48.96
3	50	49	43	47	30	44	34	48	42.83
4	34	38	30	47	41	36	42	41	37.47
5	24	28	40	37	24	39	22	29	32.78
6	35	34	30	33	31	34	23	37	28.67
7	30	28	25	28	25	26	20	30	25.08
8	19	25	27	16	22	25	15	18	21.94
9	16	17	19	16	30	23	20	25	19.20
10	16	20	12	26	13	20	18	17	16.79
11	15	17	14	16	16	15	15	15	14.69
12	6	11	18	13	8	9	13	12	12.85
13	10	13	14	11	15	8	13	15	11.24
14	9	8	13	11	9	11	9	13	9.83
15 or over	71	60	65	59	69	62	78	60	69.72
Total	502	512	508	529	508	548	472	517	512.00

$\Sigma X^2 = 110.304$; $\nu = 127$; $P = 0.847$

Excerpts from UNIVAC INSTRUCTION CODE C-10

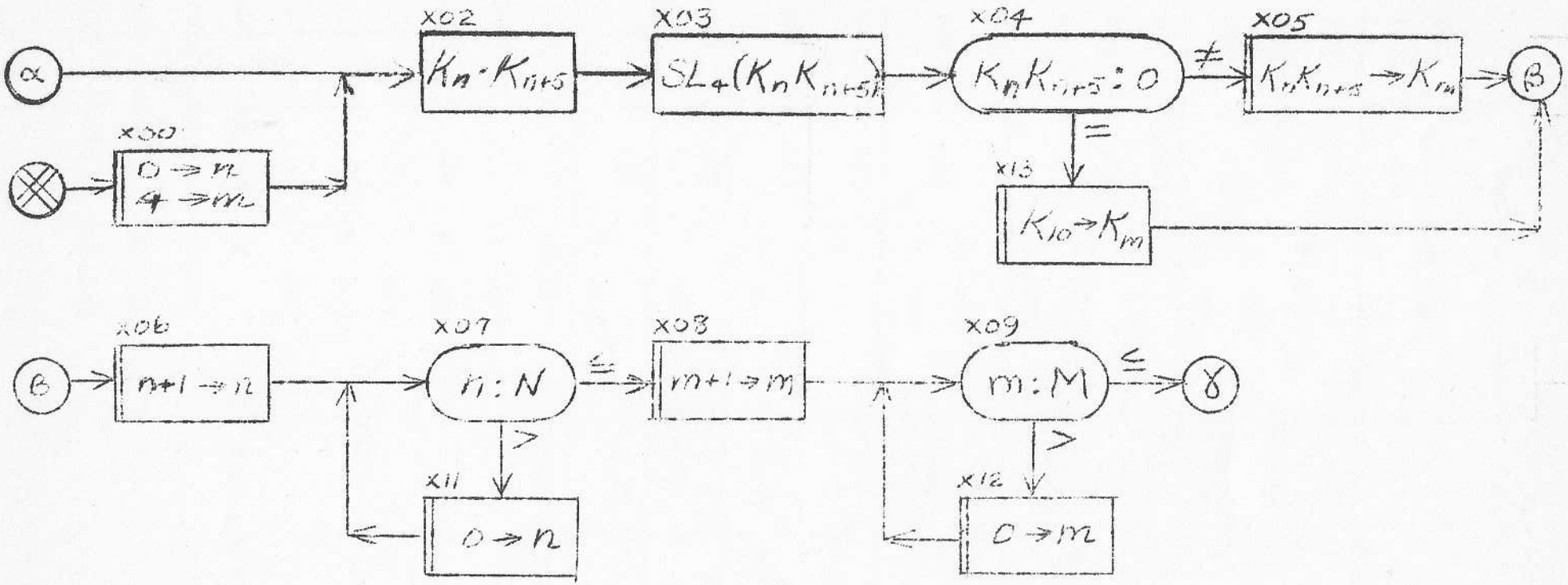
(An operation symbol, such as A,E,Q, etc., is followed by a memory location denoted here by "m". In use, m is a 4-digit number in the range from 0000 to 0999. Parentheses indicate "contents of"; for example, the symbol (rA) means "contents of register A". Approximate time is given in milliseconds.

Time	Symbol	Interpretation
0.6	Am	Add (m) to (rA); result in rA.
0.5	Bm	Clear rA to zero. Put (m) in rA.
0.5	Cm	Put (rA) in m. Clear rA to zero.
0.5	Em	Extract from (m) the digits specified by (rF Clear only those digits of (rA) which are replaced by extracted digits. When a digit in (rF) is zero (or even) leave the corresponding digit in (rA) unaltered. When a digit in (rF) is "1" (or odd) the corresponding digit of (m) is inserted in (rA).
0.5	Fm	Put (m) in rF.
0.5	Hm	Put (rA) in m. Leave (rA) unaltered; i.e., do not clear rA to zero.
0.5	Lm	Put (m) in rL.
2.2	Mm	Multiply (m) and (rL), rounding off the product to 11 digits; result in rA.
0.4	Qm	If (rA) = (rL), start instruction routine beginning at location m. If not, continue normal sequence of instructions.
0.4	Tm	If (rA) > (rL), start instruction routine beginning at location m. If not, continue normal sequence of instructions.
0.3	Um	Unconditional change of instruction routine to one beginning at location m.
0.3-0.6	On m	Shift all digits of (rA) except sign digit, n digits to the left (equivalent to multiplying (rA) by 10^n). Disregard m.

NOTE: There are also instructions for transferring from (rA) to rL, (rX) to m, (rX) to rA, (rF) to m; for dividing (rA) by (rL); for multiplying -(m) by (rL), for multiplying without round-off to double precision; for transferring two words or ten words at a time from one memory region to another; for shifting right or left, with or without the sign digit; for rewinding, reading forward or backward, and writing on magnetic tapes; for stopping; and for transferring to and from the memor and the Supervisory Control Typewriter.

Routine to Generate Pseudo-random Numbers

x00	B x15		0 → n; [L (x200 M (x25)]
		C x02	→ x02
x01	B x18		4 → m; [C (x24) B x02]
		C x05	→ x05
x02	[L(x20+n)		K_n → rL
		M(x25+n)]	$K_n \cdot K_{n+5}$
x03	04 000		$SL_4(K_nK_{n+5})$
		H x14	→ x14
x04	L x31		zero → rL
		Q x13	if $K_nK_{n+5} = 0$ go to x13
x05	[C(x24+m)		if $K_nK_{n+5} \neq 0$; K_nK_{n+5} → K_m
		B x02]	[L(x20+n) M(x25+n)]
x06	A x32		+1 +1 ; n+1 → n
		L x16	[L (x24) M (x29)] → rL; N → rL
x07	H x02		[L(x20+n) M(x25+n)] → x02
		T x11	if n ≥ N go to x11
x08	B x05		if n ≤ N; [C(x20+m) B x02]
		A x33	+1; m+1 → m
x09	L x19		[C (x29) B x02] → rL; M → rL
		T x12	if m ≥ M, go to x12
x10	C x05		if m ≤ M,
		U	exit to routine using numbers
x11	B x15		if n ≥ N; 0 → n
		U x07	[L (x20) M (x25)] → x02
x12	B x17		if m ≥ M; 0 → m
		U x10	[C(x20) B x02] → x05
x13	B x30		if $K_nK_{n+5}=0$, K_{10} → K_m
		U x05	
x14	+00000	000000	temporary storage for K_nK_{n+5}
x15	L x20	M x25	
x16	C x24	M x29	
x17	C x20	B x02	
x18	C x24	B x02	
x19	C x29	B x02	
x20	through x30		K_o through K_{10} in form +xxxxx xx0000
x31	+00000	000000	
x32	+00001	000001	
x33	+00001	000000	



LEGEND

$K_m = K_n \cdot K_{n+5}$ or K_{10}

n = running index of factors; N=4

m = running index of product; M=9

SL_4 = shift left 4 positions

α = point of entry to routine

γ = point of exit from routine

X^2 DISTRIBUTION FOR TWO-DIGIT OCTAL PSEUDO-RANDOM NUMBERS

Compared with the approximately normal distribution of $(\frac{X^2}{\nu})^{1/3}$, where $\nu = 63$ and $s = 0,0594 = (\frac{2}{9\nu})^{1/2}$. 183 groups of 512 octal pairs each, for a total of 187, 392 octal digits.

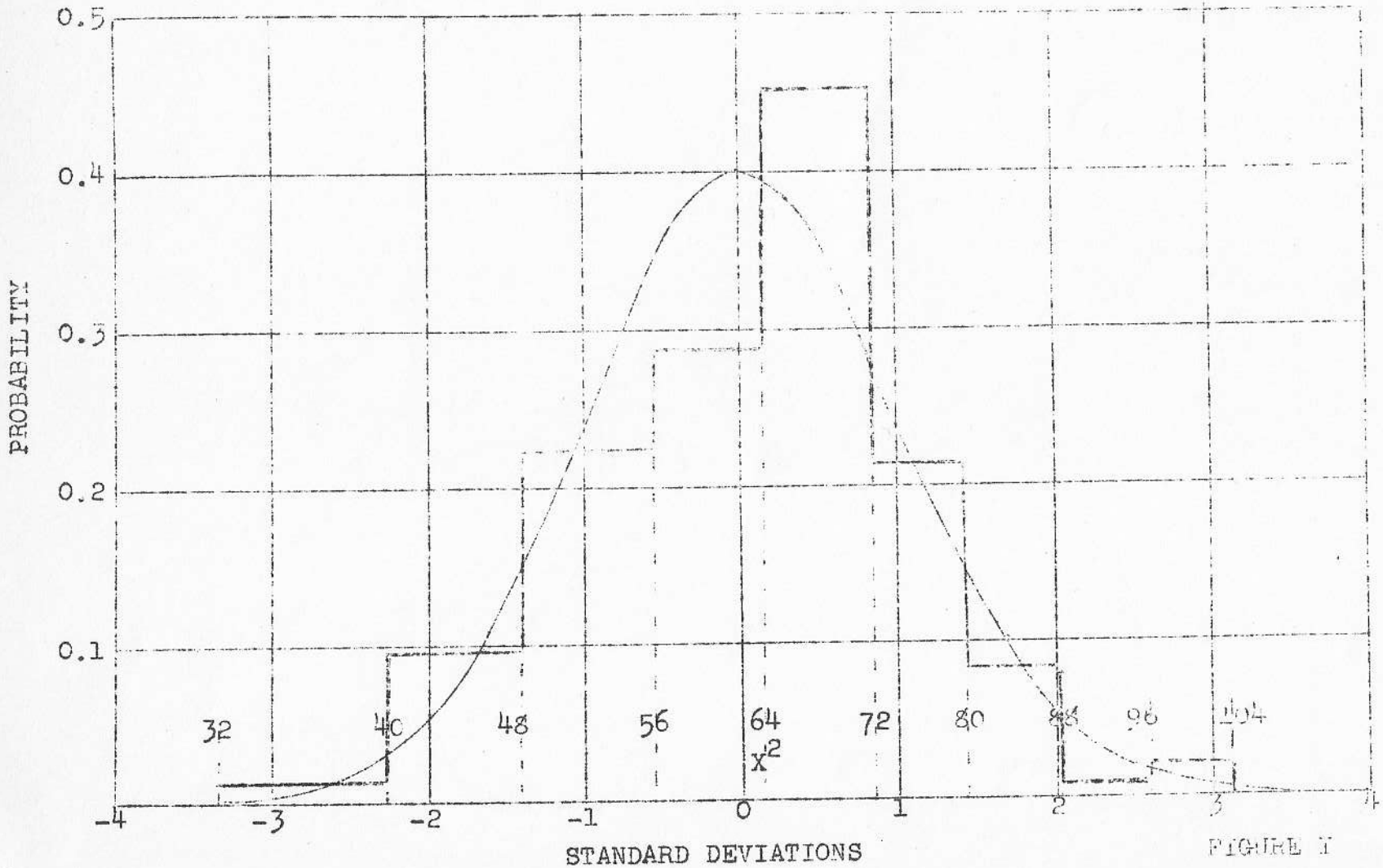


FIGURE I

Fig. 1
BLOCK DIAGRAM OF
UNIVAC SYSTEM

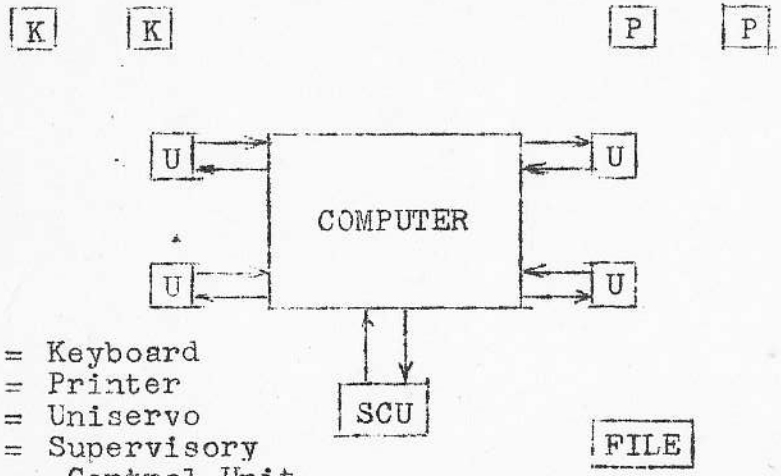


Fig. 2
CAPACITIES AND RATES FOR UNIVAC

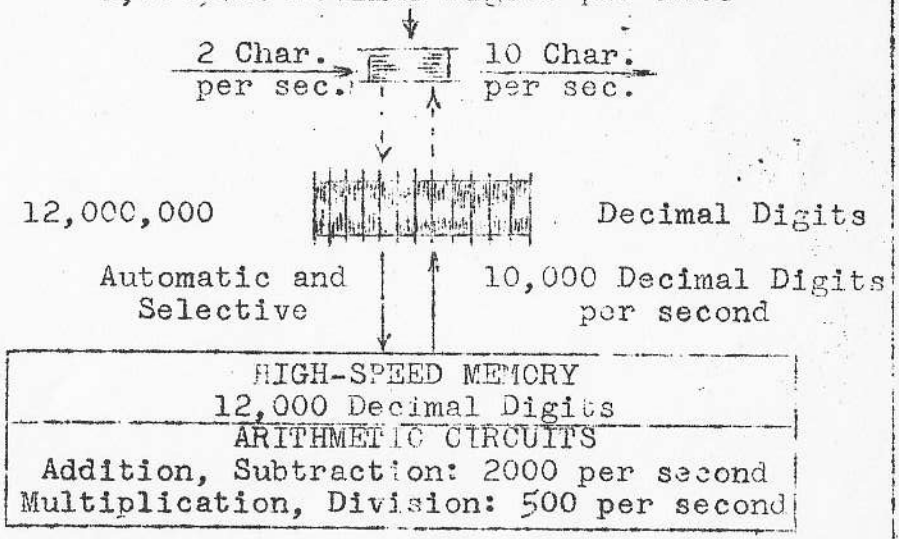


Fig. 3
BLOCK DIAGRAM OF
UNIVAC COMPUTER

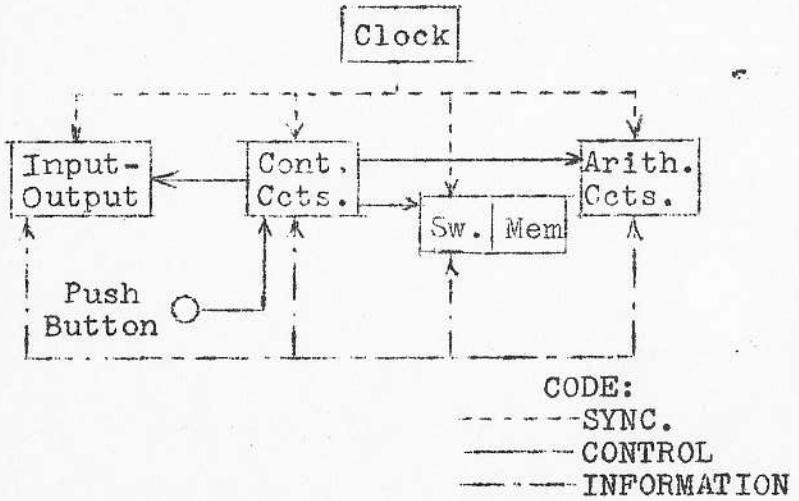


Fig. 4
PRINCIPAL ONE-WORD REGISTERS
OF ARITHMETIC CIRCUITS