CHAPTER III

RANDOM SEQUENCES

<u>Definition</u> Let S_n denote a string of n binary digits that may be 0 or 1.

For example S_1 can be 0 or 1 ,

S_2 can be 00, 01, 10, 11,

S_3 can be 000,001,010,011,100,101,110,111,

and so on.

In general, S_n may be one of 2^n different strings, for all n in N.

<u>Definition</u> Let H be a sequence of binary digits with finite period P, let h_i be a digit in one period of the sequence, and let S_n be one of the possible strings of n digits as defined above. Then we shall denote by p (S_n) the number of values of i for which $h_i h_{i+1} \ldots h_{i+n-1} = S_n$ divided by P.

Thus p (S_n) is the probability that $h_i h_{i+1} \ldots h_{i+n-1} = S_n$ if h_i is selected at random.

Let $N(S_n)$ be the number of values of i in one period such that $h_i h_{i+1} \ldots h_{i+n-1} = S_n$.

Then $p(S_n) = N(S_n)/P$.

<u>Definition</u> If $p(S_n) = 1/2^n$ for all possible string S_n, the sequence H is said to be perfectly random to order n.

__Definition__ If $p(S_n)$ does not differ from $1/2^n$ by more than ten percent for all possible strings S_n, then the sequence H is said to be nearly random to order n.

We shall now examine $N(S_n)$ for all possible string S_n of the sums of basic sequences, and find sequences that are nearly or perfectly random to order n.

Table 3 The sequences $H_{i,j,\ldots,k}$ for $i,j,\ldots,k \leq 6$, and the values of $N(S_n)$ for $n = 1,2,3$.

Sequence	P	N(0)	N(1)	N(00)	N(01)	N(10)	N(11)	N(000)	N(001)	N(010)	N(011)	N(100)	N(101)	N(110)	N(111)	nearly random to order	perfectly random to order
$H_{1,2}$	4	2	2	1	1	1	1	0	1	0	1	1	0	1	0	-	2
$H_{1,3}$	3	2	1	1	1	1	0									-	-
$H_{1,4}$	8	4	4	1	3	3	1									-	1
$H_{1,5}$	5	3	2	1	2	2	0									-	-
$H_{1,6}$	12	6	6	1	5	5	1									-	1
$H_{2,3}$	12	6	6	3	3	3	3	2	1	2	1	1	2	1	2	-	2
$H_{2,4}$	8	4	4	3	1	1	3									-	1
$H_{2,5}$	20	10	10	5	5	5	5	2	3	2	3	3	2	3	2	-	2
$H_{2,6}$	6	4	2	3	1	1	1									-	-
$H_{3,4}$	24	12	12	7	5	5	7									-	1
$H_{3,5}$	15	8	7	6	3	3	3									1	-
$H_{3,6}$	12	6	6	5	1	1	5									-	1
$H_{4,5}$	40	20	20	13	7	7	13									-	1
$H_{4,6}$	24	12	12	9	3	3	9									-	1
$H_{5,6}$	60	30	30	21	9	9	21									-	1
$H_{1,2,3}$	12	6	6	3	3	3	3	2	1	2	1	1	2	1	2	-	2
$H_{1,2,4}$	8	4	4	1	3	3	1									-	1

Sequence	P	N(0)	N(1)	N(00)	N(01)	N(10)	N(11)	N(000)	N(001)	N(010)	N(011)	N(100)	N(101)	N(110)	N(111)	nearly random to order	perfectly random to order
$H_{1,2,5}$	20	10	10	5	5	5	5	2	3	2	3	3	2	3	2	-	2
$H_{1,2,6}$	6	3	3	1	2	2	1									-	1
$H_{1,3,4}$	24	12	12	5	7	7	5									-	1
$H_{1,3,5}$	30	15	15	6	9	9	6									-	1
$H_{1,3,6}$	12	6	6	1	5	5	1									-	1
$H_{1,4,5}$	40	20	20	7	13	13	7									-	1
$H_{1,4,6}$	24	12	12	3	9	9	3									-	1
$H_{1,5,6}$	60	30	30	9	21	21	9									-	1
$H_{2,3,4}$	24	12	12	7	5	5	7									-	1
$H_{2,3,5}$	60	30	30	15	15	15	15	8	7	8	7	7	8	7	8	3	2
$H_{2,3,6}$	6	3	3	1	2	2	1									-	1
$H_{2,4,5}$	40	20	20	13	7	7	13									-	1
$H_{2,4,6}$	24	12	12	9	3	3	9									-	1
$H_{2,5,6}$	30	15	15	9	6	6	9									-	1
$H_{3,4,5}$	120	60	60	33	27	27	33	18	15	12	15	15	12	15	18	2	1
$H_{3,4,6}$	24	12	12	7	5	5	7									-	1

Sequence	P	N(0)	N(1)	N(00)	N(01)	N(10)	N(11)	N(000)	N(001)	N(010)	N(011)	N(100)	N(101)	N(110)	N(111)	nearly random to order	perfectly random to order
$H_{3,5,6}$	60	30	30	21	9	9	21									-	1
$H_{4,5,6}$	120	60	60	39	21	21	39									-	1
$H_{1,2,3,4}$	24	12	12	5	7	7	5									-	1
$H_{1,2,3,5}$	60	30	30	15	15	15	15	8	7	8	7	7	8	7	8	3	2
$H_{1,2,3,6}$	6	2	4	1	1	1	3									-	-
$H_{1,2,4,5}$	40	20	20	7	13	13	7									-	1
$H_{1,2,4,6}$	24	12	12	3	9	9	3									-	1
$H_{1,2,5,6}$	30	16	14	7	9	9	5									1	-
$H_{1,3,4,5}$	120	60	60	33	27	27	33	12	15	18	15	15	18	15	12	2	1
$H_{1,3,4,6}$	24	12	12	7	5	5	7									-	1
$H_{1,3,5,6}$	60	30	30	9	21	21	9									-	1
$H_{1,4,5,6}$	120	60	60	21	39	39	21									-	1
$H_{2,3,4,5}$	120	60	60	33	27	27	33	12	15	18	15	15	18	15	12	2	1
$H_{2,3,4,6}$	24	12	12	7	5	5	7									-	1
$H_{2,3,5,6}$	30	14	16	5	9	9	7									1	-
$H_{2,4,5,6}$	120	60	60	39	21	21	39									-	1
$H_{3,4,5,6}$	120	60	60	33	27	27	33	18	15	12	15	15	12	15	18	2	1

Sequence	P	N(0)	N(1)	N(00)	N(01)	N(10)	N(11)	N(000)	N(001)	N(010)	N(011)	N(100)	N(101)	N(110)	N(111)	nearly random to order	perfectly random to order
$H_{1,2,4,5}$	120	60	60	27	33	33	27	12	15	18	15	15	18	15	12	2	1
$H_{1,2,3,4,6}$	24	12	12	5	7	7	5									-	1
$H_{1,2,3,5,6}$	30	15	15	9	6	6	9									-	1
$H_{1,2,4,5,6}$	120	60	60	21	39	39	21									-	1
$H_{1,3,4,5,6}$	120	60	60	27	33	33	27	12	15	18	15	15	18	15	12	2	1
$H_{2,3,4,5,6}$	120	60	60	33	27	27	33	18	15	12	15	15	12	15	18	2	1
$H_{1,2,3,4,5,6}$	120	60	60	27	33	33	27	12	15	18	15	15	18	15	12	2	1

For each of the sequences $H_{i,j,\ldots,k}$ in table 3 we see that one of the following conditions must be satisfied :

(1) The sequence is not random to any order.

(2) The sequence is nearly random to order 1.

(3) The sequence is perfectly random to order 1.

(4) The sequence is perfectly random to order 1 and nearly random to order 2 or more.

(5) The sequence is perfectly random to order 2 and nearly random to order 3 or more.

We see that if the sequence $H_{i,j,\ldots,k}$ satisfies condition (5) , then $i,j,\ldots,k$ are primes and one of them is 2.

We see that each of the sequences $H_{2,i,j,\ldots,k}$, where $2,i,j,\ldots,k$ are primes satisfies condition (2) of theorem 8. Therefore each sequence $H_{2,i,j,\ldots,k}$ has period $P_{2ij\ldots k} = 2 \times 2 \times i \times j \times \ldots \times k$. It is perfectly random to order 2 but not to any order greater than 2, because $P_{2ij\ldots k}$ is not divisible by 2^n, where $n \geqslant 3$ and n is in N. But it is nearly random to order 3 or more.

From now on we shall consider only sequences $H_{2,i,j,\ldots,k}$, where $2,i,\ldots,k$ are primes, and find the value of $N(S_n)$ for all possible strings S_n of each of the sequences.

Table 4 The sequences $H_{2,i,\ldots,k}$ and their periods, where $i,\ldots,k$ are primes, and $i,\ldots,k \leq 13$,

	Sequence	Period
$H_{2,3}$	= 001011110100,001011110100 ...	12
$H_{2,5}$	= 00110100111100101100,001101001111.....	20
$H_{2,7}$	= 0011001011001111001101001100,001100...	28
$H_{2,11}$	= 00110011001011001100111100110011010011001100,00110011...	44
$H_{2,13}$	= 0011001100110100110011001111001100110010110011001100.00110011...	52
$H_{2,3,5}$	= 001010001000001100000100010100110101110111110011111011101011,00101000...	60
$H_{2,3,7}$	= 001011101011111011110011110111110101110100110100010100000001000011000010000001010001011,00101000101...	84
$H_{2,3,11}$	= 001011101011101000010000010111100111101000001000010111010111101001101000010100010111101111101 00001100001011111011110100010100001011,0010...	132
$H_{2,3,13}$	= 0010111101000101000010111110111101000011000010111101111101000010100010111101001101000010111010 1111010000010000101111001111010000100000101111010111010000101l,0010...	156
$H_{2,5,7}$	= 0011010100001110110001001011111100110011111101001000110111000010101100110010101111000100111 0110100000011001100000010110111001000111101010011,0011...	140
$H_{2,5,11}$	= 0011010011101101001111110100111101010011110001001111001100111100100011110010101111001011111 0010110111001011001100101100010010110000001011000010101100001110110000110011000011011100001l 0101000011010000001101001000110100ll,001101...	220

Sequence	Period
$H_{2,5,13}$ = 0011010011110101001111001000111100101101110010110000001011000011001100001101000000110100111011 0100111100010011110010101111001011001100101100001010110000110111000011010010001101001111101 00 111100110011110010111111001011000100101100001110110000110101000011010011,001101...	260
$H_{2,7,11}$ = 00110010110100001100100011000011010100110000001101001101110011010000 111100110011001111000010 11001110110010110000001100101011000011000100110000101101001100110011010010111100110111001111 00101011001111110010110010001100101111000011001100110000111101001100010011010011111100110101 00111100111011001111010010110011,0011001...	308
$H_{2,7,13}$ = 0011001011001000110010110000001100101101000011001011110000110010101100001100100011000011001100 1100001100010011000011010100110000111101001100001011010011000000110100110001001101001100110011 0100110111001101001111110011010010111100110100001111001101010011110011011100111100110011001111 0011101100111100101011001111000010110011110100101100111111001011001110110010110011,0011001...	364
$H_{2,3,5,7}$ = 0010100101111111100000001110100011010000100011001110010001101100110111010000110111110110101001010 1000011111010000011110101011010100100001001111010001001100100111011000110011101111010011101000 11111100000001011010111101011010000000111111000101110010111101110011000110111001001100100010 111100100001001010110101011110000001011111100001010100101011011110110000101110110011011000100 11100110001000001011000101110000001111111010010100,00101...	420

Table 5 The sequences $H_{2,i,\ldots,k}$ for $i,\ldots,k$ are primes and $i,\ldots,k \leq 13$ and the values of $N(S_n)$ for $n=1,2,3,4$.

Sequence	P	N(0)	N(1)	N(00)	N(01)	N(10)	N(11)	N(000)	N(001)	N(010)	N(011)	N(100)	N(101)	N(110)	N(111)	N(0000)	N(0001)	N(0010)	N(0011)	N(0100)	N(0101)	N(0110)	N(0111)	N(1000)	N(1001)	N(1010)	N(1011)	N(1100)	N(1011)	N(1100)	N(1111)
$H_{2,3}$	12	6	6	3	3	3	3	2	1	2	1	1	2	1	2	1	1	1	0	1	1	0	1	1	0	1	1	0	1	1	1
$H_{2,5}$	20	10	10	5	5	5	5	2	3	2	3	3	2	3	2	1	1	1	2	1	1	2	1	1	2	1	1	2	1	1	1
$H_{2,7}$	28	14	14	7	7	7	7	2	5	2	5	5	2	5	2	1	1	1	4	1	1	4	1	1	4	1	1	4	1	1	1
$H_{2,11}$	44	22	22	11	11	11	11	2	9	2	9	9	2	9	2	1	1	1	8	1	1	8	1	1	8	1	1	8	1	1	1
$H_{2,13}$	52	26	26	13	13	13	13	2	11	2	11	11	2	11	2	1	1	1	10	1	1	10	1	1	10	1	1	10	1	1	1
$H_{2,3,5}$	60	30	30	15	15	15	15	8	7	8	7	7	8	7	8	4	4	4	3	4	4	3	4	4	3	4	4	3	4	4	4
$H_{2,3,7}$	84	42	42	21	21	21	21	12	9	12	9	9	12	9	12	6	6	6	3	6	6	3	6	6	3	6	6	3	6	6	6
$H_{2,3,11}$	132	66	66	33	33	33	33	20	13	20	13	13	20	13	20	10	10	10	3	10	10	3	10	10	3	10	10	3	10	10	10
$H_{2,3,13}$	156	78	78	39	39	39	39	24	15	24	15	15	24	15	24	12	12	12	3	12	12	3	12	12	3	12	12	3	12	12	12
$H_{2,5,7}$	140	70	70	35	35	35	35	16	19	16	19	19	16	19	16	8	8	8	11	8	8	11	8	8	11	8	8	11	8	8	8
$H_{2,5,11}$	220	110	110	55	55	55	55	24	31	24	31	31	24	31	24	12	12	12	19	12	12	19	12	12	19	12	12	19	12	12	12
$H_{2,5,13}$	260	130	130	65	65	65	65	28	37	28	37	37	28	37	28	14	14	14	23	14	14	23	14	14	23	14	14	23	14	14	14
$H_{2,7,11}$	308	154	154	77	77	77	77	28	49	28	49	49	28	49	28	14	14	14	35	14	14	35	14	14	35	14	14	35	14	14	14
$H_{2,7,13}$	364	182	182	91	91	91	91	32	59	32	59	59	32	59	32	16	16	16	43	16	16	43	16	16	43	16	16	43	16	16	16
$H_{2,3,5,7}$	420	210	210	105	105	105	105	54	51	54	51	51	54	51	54	27	27	27	24	27	27	24	27	27	24	27	27	24	27	27	27

<u>Conjecture 1</u> In each of the sequences $H_{2,i,\dots,k}$, where $2,i,\dots,k$ are primes, with period $P = 2 \times 2 \times i \times j \times \dots \times k$, there exists a unique positive integer m such that :

(1) $N(S_1) = P/2$, for each possible string S_1.

(2) $N(S_2) = P/4$, for each possible string S_2.

(3) $N(S_3) = (P+4m)/8$ or $(P-4m)/8$, for each possible string S_3.

(4) 4.1) If $(P+4m)/8$ is even, and $(P-4m)/8$ is odd and greater than m, then

$N(S_4) = (P+4m)/16$ or $(P-12m)/16$, for each possible string S_4.

4.2) If $(P+4m)/8$ is odd and greater than m, and $(P-4m)/8$ is even, then

$N(S_4) = (P+12m)/16$ or $(P-4m)/16$, for each possible string S_4.

(5) 5.1) If $(P+4m)/16$ is even, and $(P-12m)/16$ is odd and greater than m, then

$N(S_5) = (P+4m)/32$ or $(P-28m)/32$, for each possible string S_5.

5.2) If $(P+4m)/16$ is odd and greater than m, and $(P-12m)/16$ is even, then

$N(S_5) = (P+20m)/32$ or $(P-12m)/32$, for each possible string S_5.

5.3) If $(P+12m)/16$ is even, and $(P-4m)/16$ is odd and greater than m, then

$N(S_5) = (P+12m)/32$ or $(P-20m)/32$, for each possible string S_5.

5.4) If $(P+12m)/16$ is odd and greater than m, and $(P-4m)/16$ is even, then

$N(S_5) = (P+28m)/32$ or $(P-4m)/32$, for each possible string S_5.

And so on.

From the table 5 we see that :

(1) Each of the sequences $H_{2,3}$, $H_{2,5}$, $H_{2,3,5}$ has m = 1.

(2) Each of the sequences $H_{2,7}$, $H_{2,3,7}$, $H_{2,5,7}$, $H_{2,3,5,7}$ has m = 3.

(3) Each of the sequence $H_{2,11}$, $H_{2,3,11}$, $H_{2,5,11}$ has m = 7. Each of these sequences (except the first) is a sequence from (1) plus A_{11}. Also $H_{2,3,5,11}$ is a sequence from (1) plus A_{11} therefore we expect it to have m = 7 too.

(4) Each of the sequences $H_{2,13}$, $H_{2,3,13}$, $H_{2,5,13}$ has m = 9, and we expect that $H_{2,3,5,13}$ has m = 9 too (for the same reason as in case (3)).

(5) The sequence $H_{2,7,11}$ has m = 21, where the number 21 comes from 3 × 7 . Hence we expect that each of the sequences $H_{2,3,7,11}$, $H_{2,5,7,11}$, $H_{2,3,5,7,11}$ has m = 21 too.

(6) The sequence $H_{2,7,13}$ has m = 27 , where the number 27 comes from 3 × 9 . Hence we expect that each of the sequences $H_{2,3,7,13}$, $H_{2,5,7,13}$, $H_{2,3,5,7,13}$ has m = 27 too.

Since each of the sequences $H_{2,3}$, $H_{2,5}$, $H_{2,3,5}$ has m = 1, we make the following conjectures.

<u>Conjecture 2</u>. Each of the sequences $H_{2,i}$, $H_{2,3,i}$, $H_{2,5,i}$, $H_{2,3,5,i}$, where i is prime and greater than 5, has m = i - 4.

Conjecture 3. Each of the sequences $H_{2,i,j,\ldots,k}$, $H_{2,3,i,j,\ldots,k}$, $H_{2,5,i,j,\ldots,k}$, $H_{2,3,5,i,j,l\ldots,k}$, where $i, j, \ldots, k$ are primes and greater than 5, has

$$m = (i - 4) \times (j - 4) \times \ldots \times (k - 4)$$

Define

$D(N(S_n)) = (\max. N(S_n) - \min. N(S_n)) / P$ to be the deviation from randomness for a given oder.

This parameter is suitable only for comparisons between sequences for the same n. It is not suitable for comparisons involving different values of n.

We wish to make this parameter as small as possible.

Table 6 The sequences $H_{2,i,\ldots,k}$ where $i,\ldots,k$ are primes and $i,\ldots,k \leq 13$, and the values of $D(N(S_n))$ for n=1,2,3,4.

Sequence	P	m	$D(N(S_1))$	$D(N(S_2))$	$D(N(S_3))$	$D(N(S_4))$
$H_{2,3}$	12	1	0	0	.0833	.0833
$H_{2,5}$	20	1	0	0	.0500	.0500
$H_{2,7}$	28	3	0	0	0.1071	0.1071
$H_{2,11}$	44	7	0	0	0.1591	.1591
$H_{2,13}$	52	9	0	0	0.1731	.1731
$H_{2,3,5}$	60	1	0	0	.0167	.0167
$H_{2,3,7}$	84	3	0	0	.0357	.0357
$H_{2,3,11}$	132	7	0	0	.0530	.0530
$H_{2,3,13}$	156	9	0	0	.0523	.0523
$H_{2,5,7}$	140	3	0	0	.0214	.0214
$H_{2,5,11}$	220	7	0	0	.0318	.0318
$H_{2,5,13}$	260	9	0	0	.0385	.0385
$H_{2,7,11}$	308	21	0	0	.0682	.0682
$H_{2,7,13}$	364	27	0	0	.0742	.0742
$H_{2,3,5,7}$	420	3	0	0	.0071	.0071

Conjecture 4. Among the sequences which have the same m, the sequence that contains A_2, A_3, A_5 is more random than the other sequences.

Conjecture 5. If in the sequence $H_{2,i,\ldots,k}$, $i,\ldots,k$ are primes, then

$$D(N(S_1)) = D(N(S_2)) = 0,$$

and $$D(N(S_n)) = m/P \text{ , for some } n \geq 3.$$

Conjecture 6. For each of the sequences $H_{i,j}$, where i, j are primes, the sequence $H_{2,5}$ is more random than the other sequences.

Conjecture 7. For each of the sequences $H_{i_1,i_2,\ldots,i_n}$, where $i_1,i_2,\ldots,i_n$ are primes and $n \geq 3$, the sequence $H_{j_1,j_2,\ldots,j_n}$, where $j_1,j_2,\ldots,j_n$ are n consecutive primes beginning with 2, is more random than the other sequences.

Conjecture 8. Let $j_1,j_2,\ldots,j_n$ be n consecutive primes beginning with 2, then in the infinite sequence of sequences $H_{2,3}$, $H_{2,3,5}$, ... $H_{j_1,j_2,\ldots,j_n}$, the first one is less random than the second, and the second is less random than the third, and so on.