Records taken from
WFF's home

Cy. 46 Wm. F Friedman

SCAMP

WORKING PAPERS - 1958

NATIONAL SECURITY AGENCY
FORT GEORGE G MEADE, MARYLAND

Serial· REMP-1-201

30 October 1958

Mr William F. Friedman
310 Second Street, S. E
Washington 3, D C

Dear Mr Friedman

The inclosed folder of unclassified 1958 SCAMP Working Papers, copy number 46, is for your convenience and retention

Sincerely,

Aina V Stenson
AINA V STENSON
SCAMP Librarian

Incl
a/s

Cy 46

Wm F. Friedman

WORKING PAPERS
CONTENTS

46 953

WORKING PAPER NO. 11

THE BLANKINSHIP CONJECTURE EXAMINED

J. D. Swift
1 August 1958
11 pages

The period of $x + 1$ in $(x^p + 1)/x + 1$ is determined for all primes $p < 288$ for which p is a primitive root. This is found to be $p\left(2^{\frac{p-1}{2}} - 1\right)$ for all such primes except 37, 101, 197, 269 for which it is 1/3 of this value. The four special cases give counter-examples for the conjecture that the period is always maximal. Some arguments tending to show that the behavior is consistent with 'random expectation' are given.

WORKING PAPER NO. 11

THE BLANKINSHIP CONJECTURE EXAMINED

J. D. Swift
1 August 1958
11 pages

1. Introduction. For primes p having 2 as a primitive root, the cyclotomic polynomial

$$f(x) = \frac{x^p + 1}{x + 1} \tag{1}$$

is irreducible over GF(2). It is also evident that, with respect to this polynomial, x has order p. The question of the order of the other linear polynomial in x, $y = x + 1$, arises. By various methods, one of which is included below, it is easy to see that the order of y is pn where n is a divisor of $s = 2^m - 1$ where $m = (p - 1)/2$.

Dr. W. A. Blankinship has conjectured that $n = s$ always. This conjecture was based on certain empirical evidence concerned with $p < 100$. The chief purpose of this paper is to discuss a method by which the proposition was investigated for $p < 288$. In particular the previous evidence was found to be faulty. The final results are that $n = s$ for $p = 3, 5, 11, 13, 19, 29, 53, 59, 61, 67, 83, 107, 131, 139, 149, 163, 173, 179, 181, 211, 227$; and that $n = s/3$ for $p = 37, 101, 197, 269$.

Certain tables which were of use in the investigation and, not being readily available elsewhere, may be of some general interest, are included.

2. *Theoretical considerations*. Let the notation be as in the first paragraph of the introduction. Further, let $g(y) = f(x)$, i.e.,

$$g(y) = \frac{(y+1)^p + 1}{y} \quad . \tag{2}$$

Then define $z = x + \frac{1}{x}$ and let $h(z) = x^{-m} f(x)$. The degree of the polynomial $h(z)$ is m . Now we maintain: *The order of y with respect to $f(x)$ is p times the order of z with respect to $h(z)$.*

Proof. $y^2 = (1 + x)^2 = 1 + x^2 = xz$. The order of y^2 is the same as the order of y since both are certainly odd. The order of x is p ; the order of z is prime to p . Hence the order of y is the order of x times the order of z by the standard theorem on the orders of elements on a Galois Field. Finally if $h(z)$ divides $z^n - 1$ as a polynomial in z , it is clear that $z^n = 1$ in the $GF(2^p)$ defined by $f(x)$.

Thus the basic problem is reduced to the evaluation of the order of z with respect to $h(z)$ or, in other terms, to finding the period of $h(z)$.

Blankinship's conjecture is equivalent to the statement: $h(z)$ is primitive irreducible. Now $h(z)$ is certainly irreducible for all degrees under consideration. Indeed $h(z)$ may be irreducible when $f(x)$ is reducible. This is the case, for example, when $p = 7$. The condition for reducibility of $h(z)$ is that the corresponding $f(x)$ have a proper symmetric divisor. Thus in some vague sense $h(z)$ is 'more than irreducible' and this idea gives some credence to the conjecture. It has, however, been the generally observed fact that there is no simple characterization of primitive polynomials any more than there is a simple numerical function which always yields primes. Indeed such functions have a statistical property known as Kronecker's Hypothesis which states that the observed frequency of primes will be asymptotically equal to that expected on elementary frequency considerations.

Now how likely is a polynomial to be primitive? The number of primitive polynomials is $\phi(s)/m$ while the number of irreducible polynomials is

$$\frac{1}{m}\left(2^m - \sum 2^{\frac{m}{q_i}} + \sum 2^{\frac{m}{q_i q_j}} - \dots\right)$$

where the q_i are the prime factors of m. The ratio of these numbers for $p = 3, 5, 11, 13, 19, 29,$ and 37 is respectively, 1, 1, 1, .67, .86, .65, .54. Other figures are given in a table at the end of the paper. Hence it is quite reasonable that 37 should be the first case of imprimitivity. Again the number of polynomials belonging to e, an admissible divisor of s, is $\phi(e)/m$. Hence if $e = s/3$ the number is either $1/3$ or $1/2$ of the primitive polynomials while if $e \leq s/7$ the number is $\leq 1/6$ of the total. Further 3 is a factor of 11 of the 21 composite numbers s considered while 7 (whose presumed asymptotic frequency is also $1/2$) is a factor of only 9 of them. Five is never a factor.

Hence if $h(z)$ is imprimitive it is most likely to have a period $s/3$. These remarks suffice to suggest that the observed results are consistent with a 'purely random' or 'Kronecker' behavior of $h(z)$.

3. The computation. To test primitivity it suffices to investigate z^{s/q_i} where now the q_i are the various prime factors of s. If one of these is $1 \bmod h(z)$ then $h(z)$ is imprimitive. Further the period will divide all the s/q_i which yield 1 and will not divide those which do not give 1. This enables a brief calculation of the period. The calculation thus requires a) The polynomials $h(z)$ for the required p; b) the primes q_i; c) the numbers s/q_i; d) $z^{s/q_i} \bmod h(z)$. We now discuss the procedures used for these steps.

a) Let $f_r(x) = x^{r-1} + x^{r-2} + \cdots + x + 1$, for r an odd positive integer and $h_k(z) = x^{-k} f_r(x)$ for $z = x + x^{-1}$ and $k = (r-1)/2$. Thus f_r and h_k are generalizations of f and h

to all odd and all natural numbers respectively; $h_m(z) = h(z)$.

The important formula is:

$$h_k(z) = z\, h_{k-1}(z) + h_{k-2}(z) \quad . \tag{3}$$

This recursion was first observed in a somewhat different context by Blankinship. Its proof is trivial:

$$h_k(z) = x^{-k}(x^{2k} + x^{2k-1} + \cdots + 1) \quad \text{by definition}$$

$$= x^k + x^{k-1} + \cdots + 1 + x^{-1} + \cdot \cdot \cdot + x^{-k}$$

$$zh_{k-1}(z) + h_{k-2} = (x + x^{-1})x^{-k+1}(x^{2k-2} + x^{2k-3} + \cdots + 1)$$

$$+ x^{-k+2}(x^{2k-4} + x^{2k-5} + \cdots + 1)$$

$$= x^k + x^{k-1} + (x^{k-2} + \cdots + x^{-k+2}) + (x^{k-2} + \cdots + x^{-k+2})$$

$$+ x^{-k+1} + x^{-k} + (x^{k-2} + \cdots + x^{-k+2})$$

$$= h_k(z) \quad .$$

This formula gives a method of computing $h(z)$ which is vastly simpler than that given by Albert in SCAMP Working Paper 27 of 15 February 1956. Specifically all that is needed is to shift $h_{k-1}(z)$ left by one and add $h_{k-2}(z)$. Only the output time limits the speed. The $h_k(z)$, $k < 144$ were computed in less than two minutes on SWAC and the specific values required selected from the resulting deck.

b) The factorization of numbers $2^n - 1$ is found in several tables in Kraitchik: Introduction a la Théorie des Nombres, Paris, 1952. Since our primes p are congruent to $\pm 3 \bmod 8$ (as 2 cannot be a quadratic residue of p), $\frac{p-1}{2}$ is either odd or singly even. Hence the tables on pp. 12 and 38 sufficed. The factorizations are collected in a table appended to this paper. The prime factors were first placed on punched cards and converted to 4-precision binary by a routine written for this purpose.

c) A division routine in 4-precision exact terms was written. This took in a number s, divided it by a sequence of exact divisors and punched out the quotients. Then it accepted the next s. If a non-divisor was entered the machine halted in break-point; this feature guarded against typographical errors in Kraitchik or mis-punching in routine b).

d) This is the principal routine and was divided into two parts. In the first, the input was $h(z)$. The routine found, by successive squaring, z^{2^k}, $k = 0, 1, \cdots, m$, reducing the powers mod $h(z)$. As a check $z^{2^m} = z$. The powers were stored, as produced, on successive drum channels. The second portion accepted successively the numbers s/q_1 and computed z to these powers by multiplying consecutively the previously computed powers which appear in the binary expansion of s/q_i . As a check on this routine s itself was entered and $z^s = 1$ computed after the maximal proper divisors had been completed.

The routines listed in a), b), and c) were primarily input-output routines in the sense that the only time limitations were the cyclic rates of these devices. The routines in d) were of rather short duration. The longest were for $p = 181$ at $6\frac{1}{3}$ min. with 11 divisors and check and for $p = 211$ with 10 divisors and check, a total of 6 min. The total run takes just over an hour for all primes less than 288.

However the routine is rather hard on the machine. This seems to be due to its large number of doubling commands and repeated extracts which cause spill and the periodic drum references following violent spells of computing which produce surging. It has been necessary to choose days of specially good machine behavior to get the routine through. Three such runs have been made; on these runs the single case of inconsistency or failure to check occurred on $s/3$ for $p = 269$ which failed to give 1 on the second run. This particular exponent has been run 16 times.

As a result of these runs we can state: $h(z)$ is imprimitive for 37, 101, 197, 269. It is highly probable that the period of $h(z)$ for these primes is $s/3$. It is highly probable that $h(z)$ is primitive for all other primes $p < 288$ for which 2 is a primitive root. The difference in degrees of assertion is due to the question put: Is this polynomial 1 ? If the probability that the machine has run without error is $\rho(m)$, the probability that we should get the answer 1 by mistake is $(1 - \rho)2^{-m}$ while the probability that we should get a value not 1 when the correct answer is 1 is $(1 - \rho)(1 - 2^{-m})$. The second is much greater than the first. For the three runs, the numbers $(1 - \rho)^3 \, 2^{-3m}$ are so small they can be neglected entirely. The numbers $(1 - \rho)^3 \, (1 - 2^{-m})^3$, while small should not be totally forgotten. It must be clearly understood that in all runs mentioned the checks never failed; hence ρ is reasonably large.

All routines are on file at NAR-UCLA.

Table 1

Factors of $s = 2^{\frac{p-1}{2}} - 1$ for primes p having 2 as a primitive root

p	Factorization of s
3	1
5	3
11	31
13	$3^2 \cdot 7$
19	7 · 73
29	3 · 43 · 127
37	$3^3 \cdot 7 \cdot 19 \cdot 73$
53	3 · 2 731 · 8 191
59	233 · 1 103 · 2 089
61	$3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331$
67	7 · 23 · 89 · 599 479
83	13 367 · 164 511 353
101	3 · 11 · 31 · 251 · 601 · 1 801 · 4 051
107	6 361 · 69 431 · 20 394 401
131	31 · 8 191 · 145 295 143 558 111
139	7 · 47 · 178 481 · 10 052 678 938 039
149	3 · 223 · 1 777 · 25 781 033 · 616 318 177
163	7 · 73 · 2 593 · 71 119 · 262 657 · 97 685 839
173	3 · 431 · 9 719 · 2 099 863 · 2 932 031 007 403
179	618 970 019 642 690 137 449 562 111
181	$3^3 \cdot 7 \cdot 11 \cdot 19 \cdot 31 \cdot 73 \cdot 151 \cdot 331 \cdot 631 \cdot 23\,311 \cdot 18\,837\,001$
197	3 · 43 · 127 · 4 363 953 127 297 · 4 432 676 798 593
211	7 · 31 · 71 · 127 · 151 · 337 · 29 191 · 106 681 · 122 921 · 152 041
227	3 391 · 23 279 · 65 993 · 1 868 569 · 1 066 818 132 868 207
269	3 · 7 327 657 · 193 707 721 · 761 838 257 287 · 6 713 103 182 899

Table 2

Polynomials h(z) for primes of which 2 is a primitive root
(Notation in octal as in Marsh's Tables of irreducible polynomials)

3	3
5	7
11	67
13	163
19	1563
29	71403
37	16 33407
53	7156 00067
*59	67016 00007
61	1 63006 00003
67	15 63006 00003
83	6714 00346 01563
101	71 56034 00000 33407
107	670 16334 00000 03467
131	67 14030 00014 00000 00003
139	1560 34670 00334 00000 00067
149	71560 00670 16334 00000 03467
163	156 30060 00003 46014 00006 71403
173	7140 33460 00000 06714 00346 01563
179	67140 03460 00000 00714 03346 00163
181	1 63340 01560 00000 00334 07156 00067
197	715 60340 00160 00000 00000 67016 00007
211	1 56300 07140 33460 00000 00000 00346 01563
227	671 40300 00016 30060 00000 00000 00000 71403
269	71403 34600 16300 00000 03460 00000 00000 00000 00163

*Incorrect in SCAMP paper 26, 15 Feb. 1956, z^{17} omitted there.

Table 3

Frequencies of various classes of polynomials

p	m	Irreducible polynomials	Primitive polynomials	p_1	p_2	p_3
5	2	1	1	1	1	
11	5	6	6	.75	1	
13	6	9	6	.56	.67	.67
19	9	56	48	.44	.86	
29	14	1 161	756	.283	.65	.93
37	18	14 532	7 776	.222	.54	.38
53	26	2 580 795	1 719 900	.154	.67	.999
59	29	18 512 790	18 407 808	.138	.994	
61	30	35 790 267	17 820 000	.133	.50	.33
67	33	260 300 986	211 016 608	.121	.81	
83	41	53 647 111 550	53 630 700 752	.098	.9996	

The third column lists the number of irreducible polynomials of degree m .

The fourth column lists the number of primitive polynomials of degree m .

The fifth column gives the probability that a random polynomial of degree m lacking a linear factor is irreducible.

The sixth column gives the probability that a random irreducible polynomial of degree m is primitive.

The seventh column gives (where applicable) the probability that an imprimitive irreducible polynomial has period 1/3 the maximum.

46 g 50

UNCLASSIFIED

15

WORKING PAPER NO. 15

THE RAND CORPORATION'S RANDOM DIGIT GENERATOR

H. P. Edmundson
18 August 1958
30 pages

The theoretical and design considerations of a machine to select decimal digits at random and punch them into I.B.M. bookkeeping cards are discussed in this report. The heart of the machine is an electronic binary counter which counts pulses from a random pulse source. Periodically, the counter is stopped for observation. About 100,000 counts are expected between successive observations, so that the last digit of the total can be considered random.

Analytical studies indicate that the machine is highly random in its selection except for trivial correlation between successful selections. Experimental tests of large numbers of the digits first tabulated by the machine indicated no irregularities except a slight excess of odd over even digits. Subsequent evolution in the pulse forming and counting circuits appears to have entirely eliminated the possibility of this kind of bias.

UNCLASSIFIED

WORKING PAPER NO. 15

THE RAND CORPORATION'S RANDOM DIGIT GENERATOR

H. P. Edmundson
18 August 1958
30 pages

Introduction. Limited tables of random numbers have been published, but much larger tables -- in fact an inexhaustible supply of random numbers -- are needed to avoid using the same tables over and over again. Repetitious use of a table of random numbers is particularly undesirable within a single problem.

The generation of random digit tables by human or machine methods is not as simple as it appears. The remarks of Kendall and Smith[1,2] concerning this difficulty are pertinent:

> "It is becoming increasingly evident that sampling left to the discretion of a human individual is not random, although he may be completely unconscious of the existence of bias, or indeed actively endeavoring to avoid it. House-to-house sampling, the sampling of crop yields, even ticket drawing have been found to give results widely divergent from expectation ....
>
> "It has long been held that mechanical methods of producing random series of integers do not give satisfactory results. Dice-throwing, for example, to give a random series of the integers 1 to 6, notoriously results in bias. Nor are

[1] M. G. Kendall and B. Babington Smith, "Randomness and Random Sampling Numbers," Journal of the Royal Statistical Society, pp. 151 and 156, Vol. CI, 1938.

[2] Kendall and Smith, Loc. Cit., pp 154-156.

> roulette tables much better. Karl Pearson has shown by analysis of the gaming results at Monte Carlo that the odds against the absence of bias are exceedingly large. The source of this bias is not altogether clear, but if we exclude the possibilities of deliberate falsification, it would appear to arise from small imperfections in the roulette wheel which direct the ball into some compartments in preference to others ......"

Mr. Cecil Hastings of the RAND Corporation has proposed a scheme for accomplishing the selection of digits with a high degree of randomness, and automatically recording them at a reasonably high rate of speed. A machine based on a variation of his idea has been designed and constructed in the Development Section and put into successful operation. The following discussion describes the operation of the machine, attempts to discuss its randomness analytically, and mentions a few of the design features intended to insure conformity to the theoretical analysis.

Theoretical considerations. The two design criteria of a machine intended to produce a table of random digits are:

1) The device should be absolutely impartial.

2) There should be no correlation between successive selections; the machine should have no memory.

Almost any common device one might name falls down at one of these two criteria. A mechanical roulette wheel, for example, satisfies neither requirement. It is difficult to build a roulette wheel with such precision that one number would not be favored over another by even one percent, let alone, say, one thousandth of a percent, which would be a more nearly acceptable figure. Furthermore, if, say, one million successive 6's were thrown on a roulette wheel, a groove would be worn to the 6 compartment. Therefore, the 6 would be favored over the other numbers.

Consider, however, the following system, Figure 1, which is a modified electronic roulette wheel.

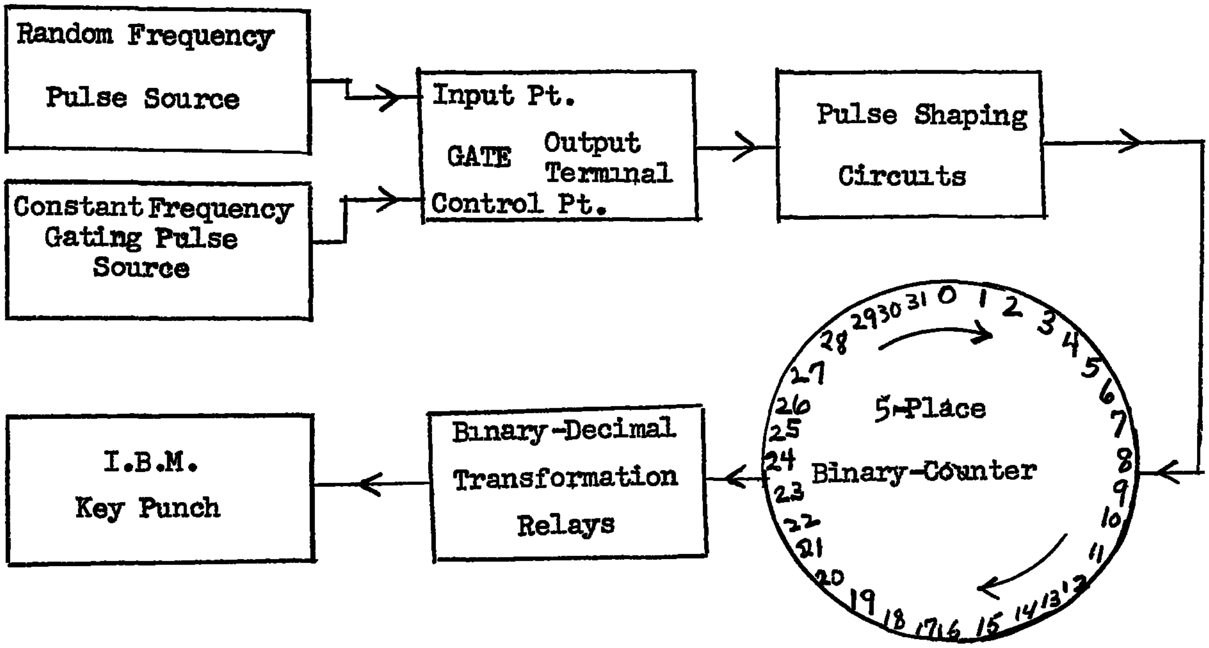

Figure 1 - Random Digit Selecting System

It is intended that sharp pulses from the random frequency pulse source should arrive at the gate at an expected frequency of about one hundred thousand per second. This gate circuit is controlled by broad constant frequency pulses from the constant frequency gating pulse source, so that the gate allows the random pulses to pass in groups of about one second time duration. Each random pulse advances the position of the counter one digit, so that each group of random pulses advances the count about one hundred thousand digits. After each group of pulses, the digit at which the counter rests is considered to be random. This system is closely analogous to a 32 compartment roulette wheel, around which the ball spins about three thousand times before stopping.

The choice of 32 numbers results, of course, from the fact that $2^5 = 32$ is the number of steps in one cycle of a five place binary counter. For a reason to be discussed later, the following transformation from binary numbers to decimal digits is now used (this transformation was not used originally).

TABLE I

TRANSFORMATION FROM BINARY TO DECIMAL DIGITS

Position in Cycle	Binary Number	Decimal Digit
0	00000	0
1	00001	1
2	00010	2
3	00011	3
4	00100	4
5	00101	5
6	00110	6
7	00111	7
8	01000	8
9	01001	9
10	01010	discard
11	01011	discard
12	01100	discard
13	01101	discard
14	01110	discard
15	01111	discard
16	10000	discard
17	10001	discard
18	10010	discard
19	10011	discard
20	10100	discard
21	10101	discard
22	10110	9
23	10111	8
24	11000	7
25	11001	6
26	11010	5
27	11011	4
28	11100	3
29	11101	2
30	11110	1
31	11111	0

The impartiality of this type machine results from the assumption that the pulse shaping circuit standarcizes the shape of all pulses it passes on to the counter, and that the level and separation of the standardized pulses driving the counter is sufficient to unerringly advance the counter one count per pulse. Even though the counter flip-flops themselves may prefer certain positions to others, the totals observed on the counter are determined entirely by the number of pulses which come from the pulse forming circuits during the measured time intervals. It was, however, the failure of the initial circuits to faithfully perform these functions that caused the initial odd-even bias in the tables created. Impartiality also depends upon complete independence of the gating pulse generator, and the random pulse generator from the position of the counter. This is accomplished easily by carefully isolating the fields and power supplies of these different components.

There is no evidence at present to indicate that the machine does not select binary numbers with complete impartiality. However, it would be necessary to sample several million numbers to detect an odd-even bias of as much as one tenth percent. As insurance against the possibility that the machine may have an undetected bias in one of its binary counters, the peculiar transformation to decimal digits given in Table I is used. Note that the two binary numbers which transform to each decimal digit are complementary. Thus, if the flip-flop controlling any one binary place is biased by a certain amount, the probability of any particular decimal digit being selected is unchanged. The excess (or shortage) in the probability of the digit being selected in the first ten positions is exactly compensated by the shortage (or excess) in the probability of that digit being selected in the last ten positions.

The effect of this complimentary combination scheme can be formulated analytically. Suppose that 0 is preferred over 1 in the last binary place by an amount 2α, in the next place by 2β, in the next place by 2δ, in the next place by 2ε, and in the first place by 2ρ. The probability of a 0 decimal digit equals the probability of a 00000 binary number plus the probability of a 11111 binary number.

$$p(0) = (1/2 + \alpha)(1/2 + \beta)(1/2 + \delta)(1/2 + \varepsilon)(1/2 + p) \\ + (1/2 - \alpha)(1/2 - \beta)(1/2 - \delta)(1/2 - \varepsilon)(1/2 - \rho) \qquad (1)$$

Neglecting terms higher than the second degree leaves

$$p(0) = 1/16 + 1/8(\alpha\beta + \alpha\delta + \alpha\varepsilon + \alpha\rho + \beta\delta + \beta\delta + \beta\varepsilon + \beta\rho + \delta\varepsilon + \delta\varepsilon + \delta\rho + \varepsilon\rho) \qquad (2)$$

Similarly

$$p(1) = 1/16 + 1/8(-\alpha\beta - \alpha\delta - \alpha\varepsilon - \alpha\rho + \beta\delta + \beta\varepsilon + \beta\rho + \delta\rho + \varepsilon\rho) \qquad (3)$$

$$p(2) = 1/16 + 1/8(-\partial\beta + \partial\delta + \partial\varepsilon + \partial\rho - \beta\delta - \beta\varepsilon - \beta\rho + \delta\varepsilon + \delta\rho - \varepsilon\rho) \qquad (4)$$

etc.

Notice that no first degree errors remain as a result of this particular type of transformation.

The second criterion, the absence of correlation between successive selections, is certainly satisfied by this system. Actually, it would be nearly impossible to intentionally control the frequency of the pulse source and the period of the gate switching pulse closely enough that a "next" selection could be predicted, since the expected number of counts per gate interval is 100,000. The following analysis indicates how small this correlation actually is assuming an ideal counter, random pulse source, and gating system.

The probability of exactly X random pulses occurring in any constant time interval group is

$$p(K) = \frac{N^K}{K!} e^{-N} , \qquad (5)$$

where N is the expected number of pulses per group.

If, therefore, the count starts from a digit d_o , the probability of its advancing just k digits to digit d_k is

$$p(k) = \frac{N^k}{k!} e^{-N} . \qquad (6)$$

The digit d_k would also be selected if the counter advanced 32 + k counts, and the probability of this happening is

$$p(k + 32) = \frac{N^{k+32}}{(k + 32)!} e^{-N} . \qquad (7)$$

Similarly, the d_k digit can be selected by the count advancing k plus any multiple of 32 counts. Thus, the entire probability of the digit d_k being selected after d_o is

$$\rho(d_k) = \frac{N^k}{k!}\, e^{-N} + \frac{N^{k+32}}{(k+32)!}\, e^{-N} + \frac{N^{k+64}}{(k+64)!}\, e^{-N} + \cdots \quad .(8)$$

Simplification of this to a finite series can be achieved by the use of the identity

$$\frac{N^k}{k!} + \frac{N^{k+32}}{(k+32)!} + \frac{N^{k+64}}{(k+64)!} + \cdots = \frac{1}{32}\sum_{m=o}^{31} e^{ik\frac{\pi m}{16}}\, e^{Ne^{i\frac{\pi m}{16}}} \quad . \qquad (9)$$

Thus,

$$p(d_k) = \frac{1}{32}\, e^{-N} \sum_{m=o}^{31} e^{-ik\frac{\pi m}{16}}\, e^{Ne^{i\frac{\pi m}{16}}} \qquad (10)$$

This equation reduces easily to the form

$$p(d_k) = \frac{1}{32}\, e^{-N} \sum_{m=o}^{31} e^{N\cos\frac{m\pi}{16}}\, e^{i(N\sin\frac{m\pi}{16} - k\frac{m\pi}{16})} \quad . \qquad (11)$$

Since N is about 100,000 , the term in the summation corresponding to $m = 0$ is by far the most important. Next are the two terms corresponding to $m = 1$ and $m = 31$, and the remaining terms are negligible in comparison with these. The three retained terms can be written

$$p(d_k) \simeq \frac{1}{32} e^{-N} \left[e^{N} + e^{N\cos\frac{\pi}{16}} e^{i(N\sin\frac{\pi}{16} - k\frac{\pi}{16})} + e^{N\cos\frac{31\pi}{16}} e^{i(N\sin\frac{31\pi}{16} - k\frac{31\pi}{16})} \right] . \qquad (12)$$

But $\cos\frac{\pi}{16} = \cos\frac{31\pi}{16}$, $\sin\frac{\pi}{16} = -\sin\frac{31\pi}{16}$; and for k an integer, $k\frac{\pi}{16}$ radians is coincident with $-k\frac{31\pi}{16}$ radians. Thus

$$p(d_k) = \frac{1}{32} \left[1 + e^{-N(1-\cos\frac{\pi}{16})} \left\{ e^{i(N\sin\frac{\pi}{16} - k\frac{\pi}{16})} + e^{-i(N\sin\frac{\pi}{16} - k\frac{\pi}{16})} \right\} \right]$$

$$= \frac{1}{32} \left[1 + 2\, e^{-N(1-\cos\frac{\pi}{16})} \cos\left(N\sin\frac{\pi}{16} - k\frac{\pi}{16}\right) \right] . \qquad (13)$$

Since the cosine function can be no greater in absolute magnitude than unity, then this probability can differ from the perfect value of 1/32 by no more than

$$\left| 1/32 - p(d_k) \right| \leq \frac{1}{16} e^{-N(1-\cos\frac{\pi}{16})} . \qquad (14)$$

For $N = 100,000$ this deviation is

$$\left| 1/32 - p(d_k) \right| \leq \frac{1}{16} e^{-100,000(1-.9807)}$$

$$= \frac{1}{16} e^{-1930} . \qquad (15)$$

Indeed, the correlation between successive selections is negligible.

The random pulse source. The circuitry used as a random pulse source is a high gain wide band noise amplifier followed by a detector biased so that only the noise peaks above a certain high level are transmitted through the detector into the output circuit. Figure 2 is a schematic of the circuits used. The source of random noise is simply shot effect in the first vacuum tube. The r-m-s value of this noise is controlled by the bias applied at the input grid. The overall bandwidth of the amplifier is about 6 megacycles.

The justification for using a highly biased random noise detector as a random pulse source may not meet the approval of the critical reader. However, all that is needed from a practical standpoint is a highly irregular and unpredictable source of pulses to drive the counter, and the biased random noise detector certainly satisfies this requirement.

As a matter of fact, it can be argued that the pulses generated by such a device are nearly truly random. The requirement of a truly random source would be that the probability of a pulse occurring between t and $t + dt$ should be some $p \ dt$, where p is the expected number of pulses per second and is a constant entirely independent of the number and distribution of pulses generated up to time t.

Figure 3 is a typical random noise voltage signal, with one detected pulse shown to aid in discussing the problem.

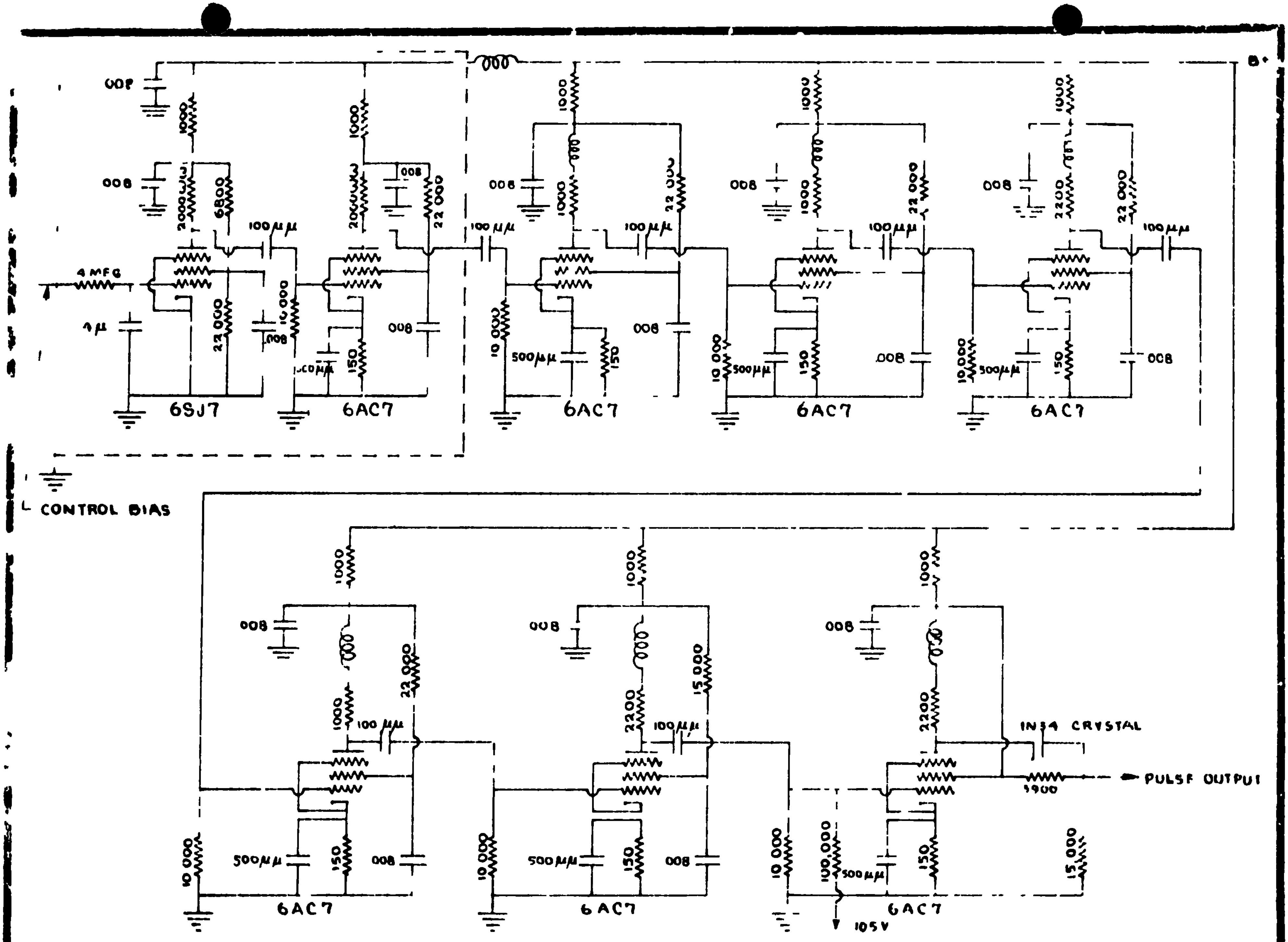

FIGURE 2 — RANDOM NOISE GENERATOR AND BIASED DETECTOR

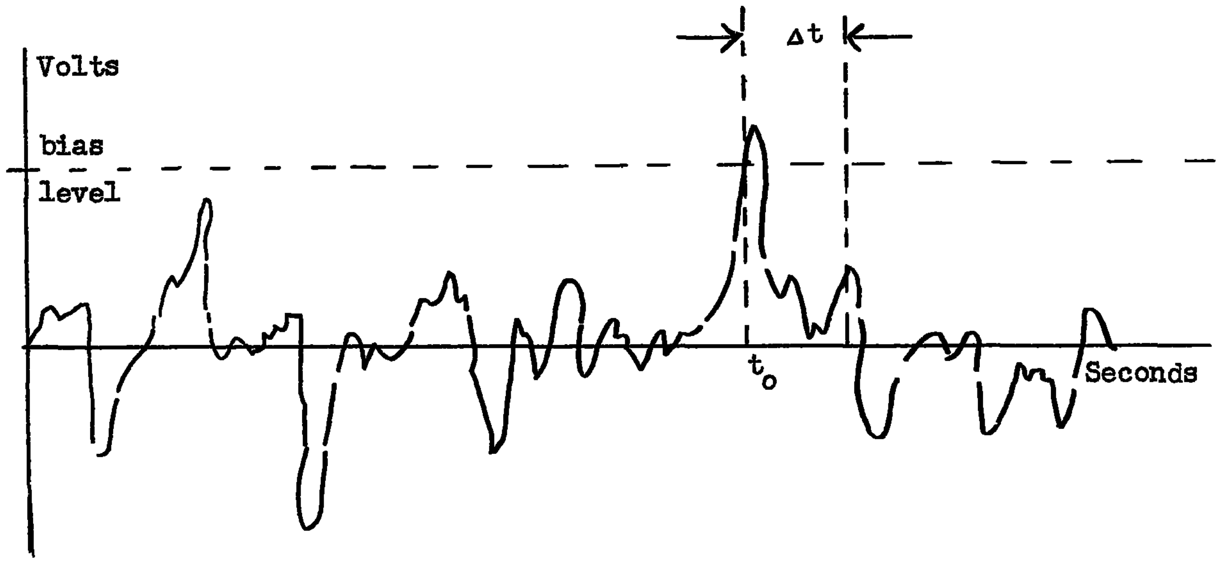

Figure 3. A Typical Random Noise Voltage Signal

Consider the following argument from the standpoint of an observer who stands at the output of the biased detector and observes only the detected pulses. Say, for example, that starting at the left end of the signal of Figure 3, a pulse has not been detected for a long time. Then proceeding with time to the right, the probability of a detectable pulse occurring between any t and $t + dt$ is $p\ dt$, where p is a constant determined by the r-m-s level of the noise voltage and the bias applied to the detector. So far as the waiting observer is concerned, a detectable pulse is just as likely to occur at one time as another.

Suppose that at time t_o a pulse is finally observed. Then, however, the observer is able to predict a trend for a short interval ahead. Knowing the intrinsic decay behavior of the amplifier in question, he knows that this decay voltage superimposed on the new random signal voltage increases (or decreases as the case may be) the probability of a detectable peak being observed. After Δt, however, the decay trend will have expended itself, and the probability of a pulse will remain constant (so far as the observer knows) until another pulse is observed.

The length of Δt can be assumed to be less than one microsecond for the amplifier in question, since one-twelfth microsecond is the conventional rule-of-thumb decay time estimate for a low-pass amplifier of six megacycles bandwidth. The fact that the amplifier is actually band-pass instead of low-pass can be neglected, since the ratio of noise power in the missing low end of the frequency range to the power in the band pass region is quite small. It will become apparent later that this divergence from pure random occurrence in an interval of one microsecond following each observed pulse is of no extra concern. The pulse forming circuits reject any pulse which falls within one microsecond of a previously observed pulse anyhow.

<u>The gate circuit and the gating pulse generator</u>. The function of the gate circuit and its controlling gating pulse generator is to measure out intervals of one second during which pulses from the random pulse generator are amplified and passed on to the pulse shaping circuits.

UNCLASSIFIED

Between each of these intervals should be a period of about one-tenth second during which the pulses from the random pulse generator are blocked, and the digit at which the counter stops is read and recorded in an I.B.M. card. This timing sequence is obtained easily by means of an unsymmetrical multivibrator.

Figure 4 is a schematic of this timing multivibrator and the gate circuit. The gate circuit is a two stage pulse amplifier with the plate of the second amplifier tube tied in common with the plate of the gating pulse isolation tube. Notice that when the multivibrator lies with its right-hand tube conducting that the isolation tube is cut off. Thus, the pulse amplifier works as a simple amplifier with no interference from the multivibrator isolation tube. When the right-hand tube is cut off, however, this isolation tube grid goes positive with respect to its -90 volt cathode, pulling its plate down to a negative value. Consequently, the voltage is removed from the plate of the second pulse amplifier tube, and no pulses from the random pulse source can pass to trip the pulse forming circuits which follow.

A second multivibrator isolation tube is shown in Figure 4. When the grid of this tube goes positive, its plate current actuates the counter reading relays and, subsequently, the I.B.M. key punch.

The pulse shaping circuits. The pulse shaping circuits have a difficult job to perform. The input pulses are of various sizes and shapes and occur at random in time. From these highly irregular input signals, the pulse shaping circuits must form output pulses of standard size and shape, no two of which can be within one microsecond of each other. Any input pulse which comes within one microsecond of a previous pulse must be rejected.

Although this would ordinarily be an easy function, it is made very difficult by the rigid requirements placed upon the dependability of the circuits. The pulse shaping circuits must be perfect, lest counter partiality bias the digit selecting system. If any pulse leaks through the pulse shaping circuits which is of such a size and shape, or is so close (less than one microsecond for the counter used) to another pulse, that the counter might or might not (according to its own preference) advance one count, then the unavoidable partiality of the counter itself is allowed to contribute partiality to the system as a whole. The circuits of Figure 5 were arrived at experimentally, and appear to be absolutely dependable.

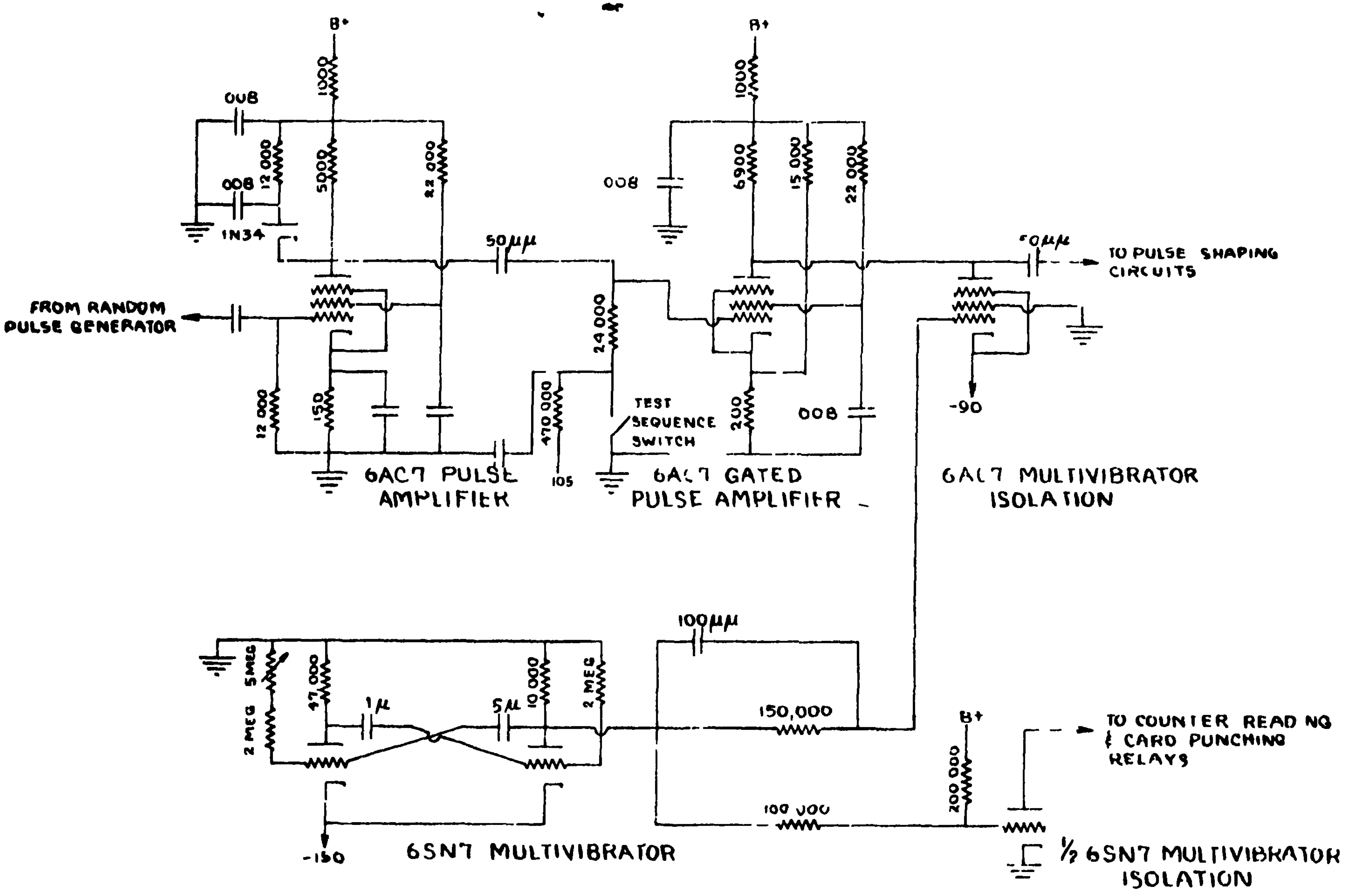

FIGURE 4 CONSTANT FREQUENCY GATING PULSE SOURCE AND GATE AMPLIFIER

First in the circuit are two cascaded one-shot multivibrator circuits (6SN7's), with a pulse width of about one microsecond. These circuits do the major portion of the work. Pulses which are too weak to trip the circuits do not get through to the output at all, and nearly every pulse strong enough to trip the circuit produces a standard one microsecond pulse. Some complications, however, occur. For example, when two strong pulses occur just about one microsecond apart, the second pulse may catch the one-shot multivibrator circuit just as it is resetting and produce something different from the standard pulse shape.

The final insurance against irregularities is a relatively fast flip-flop circuit of 6AK5's driven at the cathode of one of the 6AK5's by a 6L6 cathode follower. This circuit trips to the right if the driven cathode is made more positive than +10 volts, and resets to the left if the driven cathode is made more negative than -10 volts. Thus, the circuit can trip only once for each full pulse from the one-shot multivibrators, and any small input irregularities will fail to trip the 6AK5 flip-flop unless they go from -10 to +10 volts. There is little chance of trouble with input pulses too closely spaced in this circuit, because the flip-flop is very fast compared to the circuits which drive it. The flip-flop has a rise time at its plates of about one tenth micro-second, and stabilizes in an exchanged position at the end of about two tenths of a microsecond.

Thus, the output of this circuit is a square wave of about one microsecond duration and very steep sides. If this output is differentiated (not shown in Figure 5   ee Figure 6) the result will be sharp positive and negative pulses, and, obviously, no two positive pulses can be closer together than one microsecond. Also, these pulses will be of standard size and shape, since the relatively sluggish driving circuits ahead of the 6AK5 flip-flop cannot effect its rise time appreciably.

__The__ __counter__ __circuit__. The function of the counter circuit is to accurately count the pulses as they come from the pulse shaping circuits. The resolving time of the counter must be short compared to the one microsecond minimum spacing between successive input pulses, and the circuits must be absolutely dependable else counter partiality might contribute partiality to the system.

The counting is done in the binary number system because it is the natural system for electronic counters. All the binary places except the last five are disregarded, giving a count cycle of $2^5 = 32$ steps, the 33rd step being identical with the 1st, the 34th step being identical with the 2nd, etc., etc.

In Figure 6, the first two tubes are a cathode follower to isolate the flip-flop of Figure 5, and a driver tube for the following flip-flop. Recall that the output of the flip-flop in Figure 5 is a square wave pulse with very steep sides.

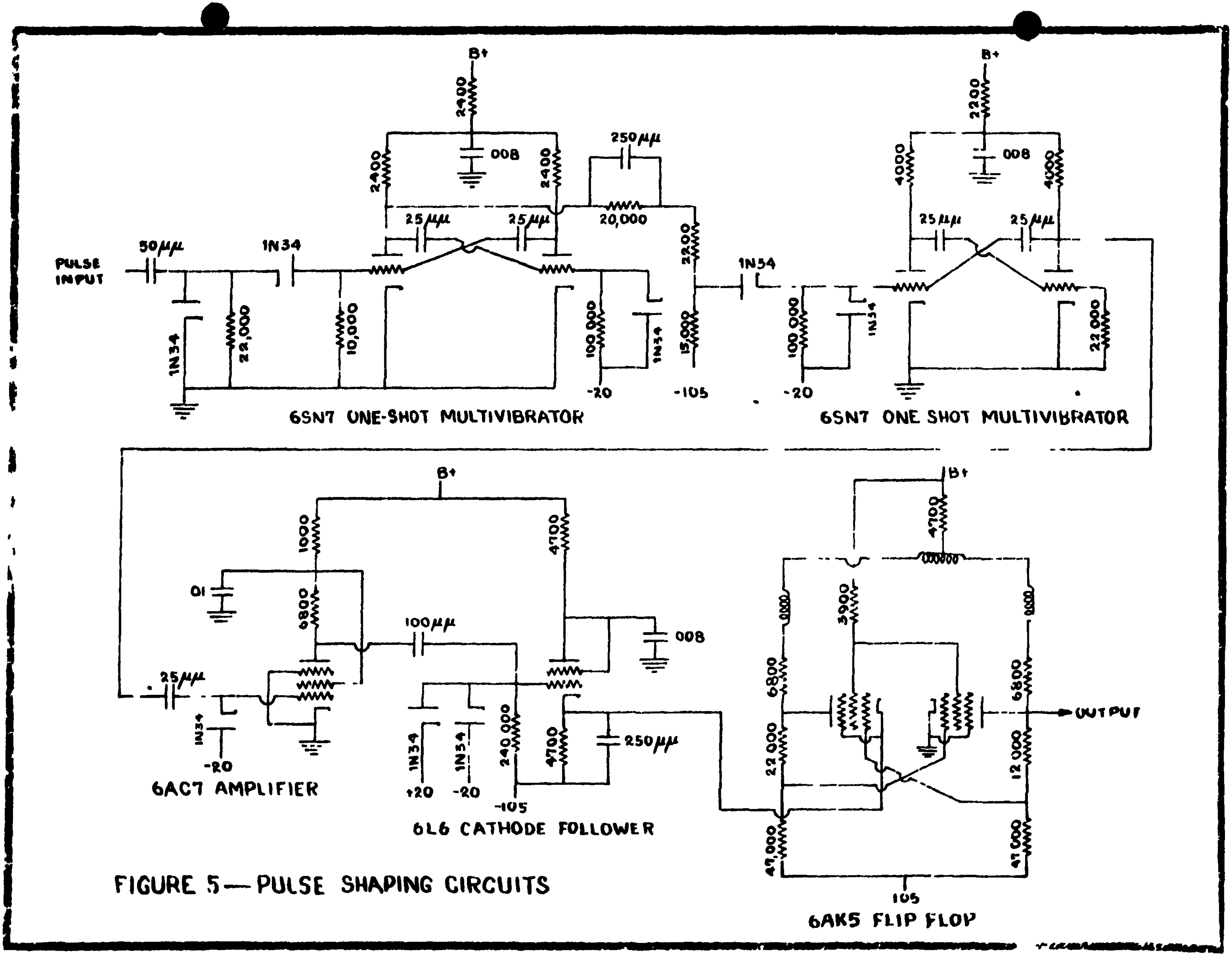

FIGURE 5—PULSE SHAPING CIRCUITS

In the output of the cathode follower circuit this voltage is differentiated by the 50 μμ condenser into the 10,000 ohm resistor, so that the input to the 6AK6 driver tube is a sharp positive pulse corresponding to the front edge of the input pulse, and a sharp negative pulse corresponding to the trailing edge of the input pulse. Of course, the positive pulse only is effective, since the tube is normally biased beyond cutoff. When this sharp positive pulse is applied to the driver tube grid, its plate conducts momentarily.

The basis of the electronic counter is a d-c flip-flop, a circuit having two stable positions. Note in Figure 6 that if no external driving pulses are supplied, the 6AK5 flip-flop would sit with either its right hand tube conducting and the left hand tube cut off, or with its left hand tube conducting and the right hand tube cut off. Note also that if the grid of the 6AK6 driving tube (which is normally cut off) is pulsed with a sharp positive peak causing its plate to conduct momentarily that both plates of the 6AK5 flip-flop will be momentarily brought to almost zero voltage, and the flip-flop circuit will then return to the state opposite the one it was resting in when the driving pulse occurred. This exchange of position is caused by the two "memory" condensers shown (20 μμ). The condenser to the formerly non-conducting plate has a greater voltage across it than the condenser to the conducting plate. Thus, if both plates are momentarily reduced to nearly zero volts, the condenser having the greater voltage across it causes the grid of the opposite tube to be the more negative. When released, then, the opposite tube becomes non-conducting, while the formerly non-conducting tube conducts. Each positive pulse from the pulse shaping circuits reverses the position of the first flip-flop.

The output of this flip-flop, then, is alternate positive and negative steps. This output is isolated by a cathode follower and differentiated by circuits similar to the differentiating circuit used ahead of the first flip-flop. The result, of course, is again very sharp positive and negative pulses, and the positive pulses are used to drive the second flip-flop. This chain -- flip-flop, cathode follower stage and driving tube -- is repeated a total of five times. The first flip-flop reverses conduction tubes for each input pulse. The second flip-flop in the chain reverses for each positive pulse from the differentiating circuit following the first flip-flop -- and this occurs only on every second input pulse. Similarly, the third flip-flop reverses on every fourth input pulse, etc., etc., and the last flip-flop reverses on every sixteenth pulse. Thus, the counter cycle consists of the following 32 steps:

TABLE II - COUNTER CYCLE

Step	Flip-Flop Position (0 for right and 1 for left)				
	No. 5	No. 4	No. 3	No. 2	No. 1
0	0	0	0	0	0
1	0	0	0	0	1
2	0	0	0	1	0
3	0	0	0	1	1
4	0	0	1	0	0
5	0	0	1	0	1
6	0	0	1	1	0
7	0	0	1	1	1
8	0	1	0	0	0
9	0	1	0	0	1
10	0	1	0	1	0
11	0	1	0	1	1
12	0	1	1	0	0
13	0	1	1	0	1
14	0	1	1	1	0
15	0	1	1	1	1
16	1	0	0	0	0
17	1	0	0	0	1
18	1	0	0	1	0
19	1	9	0	1	1
20	1	0	1	0	0
21	1	0	1	0	1
22	1	0	1	1	0
23	1	0	1	1	1
24	1	1	0	0	0
25	1	1	0	0	1
26	1	1	0	1	0
27	1	1	0	1	1
28	1	1	1	0	0
29	1	1	1	0	1
30	1	1	1	1	0
31	1	1	1	1	1

The binary to decimal transformation. Table I of the section on theoretical considerations shows the manner in which the positions of the binary cycle are to be interpreted as decimal digits. It is desirable to indicate each of the digits by a closed circuit rather than by a light, voltage, or current, so that any type of automatic device such as an electric typewriter or I.B.M. duplicating punch may be used to record the selections. Figure 7 shows how this may be accomplished by the use of multi-pole double-throw relays.

Note that, depending upon what combination in which the relays are open or closed, any one -- but only one -- path is closed to the common input point. If these relays are controlled by the position of the d-c flip-flops of the binary counter chain, then it is possible to determine by inspection the particular combination which closes the circuit to each particular output point. In Figure 7 each of the 32 output points is labeled with this binary counter combination (assuming 1 to mean upper contacts and 0 to mean lower contacts), and the decimal digit this combination should represent is copied from Table I. Then the two output points that indicate each of the decimal digits are tied to a common output terminal.

Figure 7 shows how the relays are driven by thyratrons, the grids of which are controlled by the cathode follower voltage of each of the five flip-flops. The gating pulse output tube in the lower right hand corner of Figure 4 closes the master relay - power relay in Figure 7, furnishing plate voltage to the five transformation relays. Thus, the transformation relays do not attempt to follow the progress of the electronic counter, but merely are controlled by the counter during the one-tenth second interval during which the gate is shut and no pulses are driving the counter.

The relay-power relays work in conjunction with the master transformation circuit relay to prevent the application of power to the recording circuit until all five transformation relays have been given ample time to set in the selected combination, and to open the recording circuit before the transformation relays are released. Otherwise, each time the gating pulse occurs, the transformation relays would give momentary false circuits when they were pulling in or releasing.

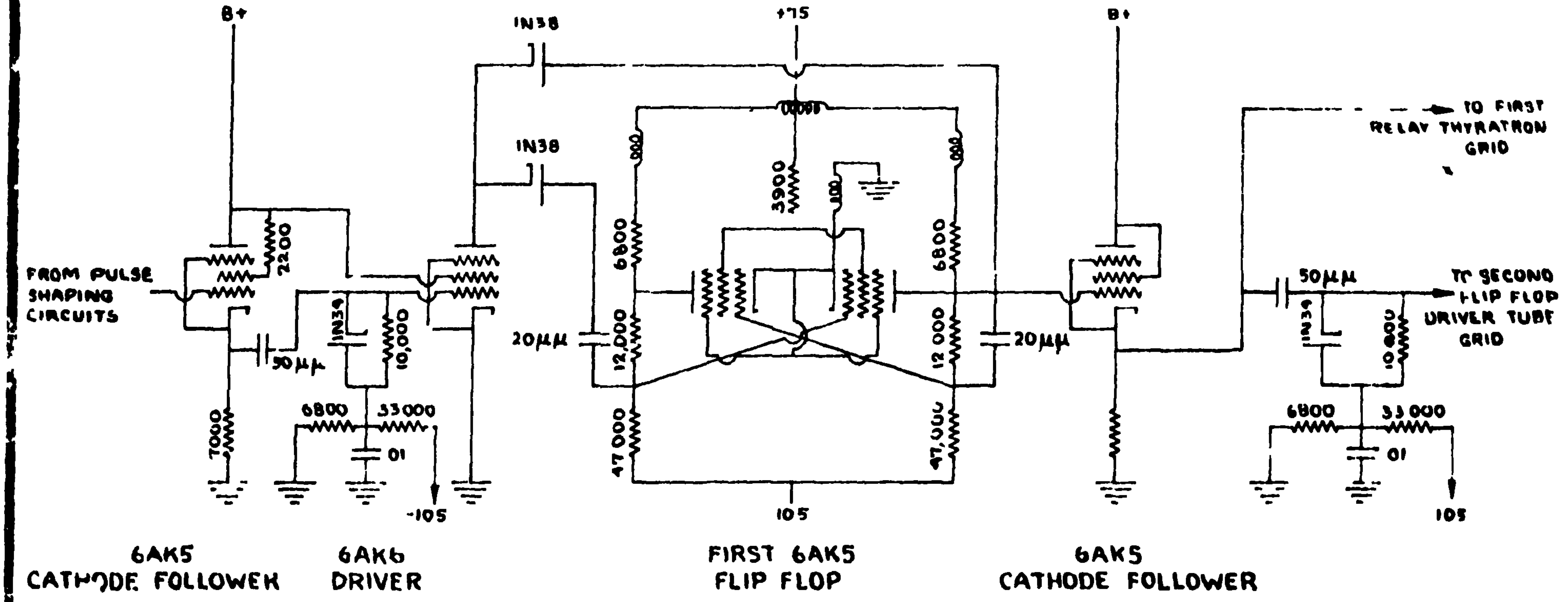

FIGURE 6 — FIRST COUNTER FLIP FLOP (CONTROLS LAST BINARY PLACE)

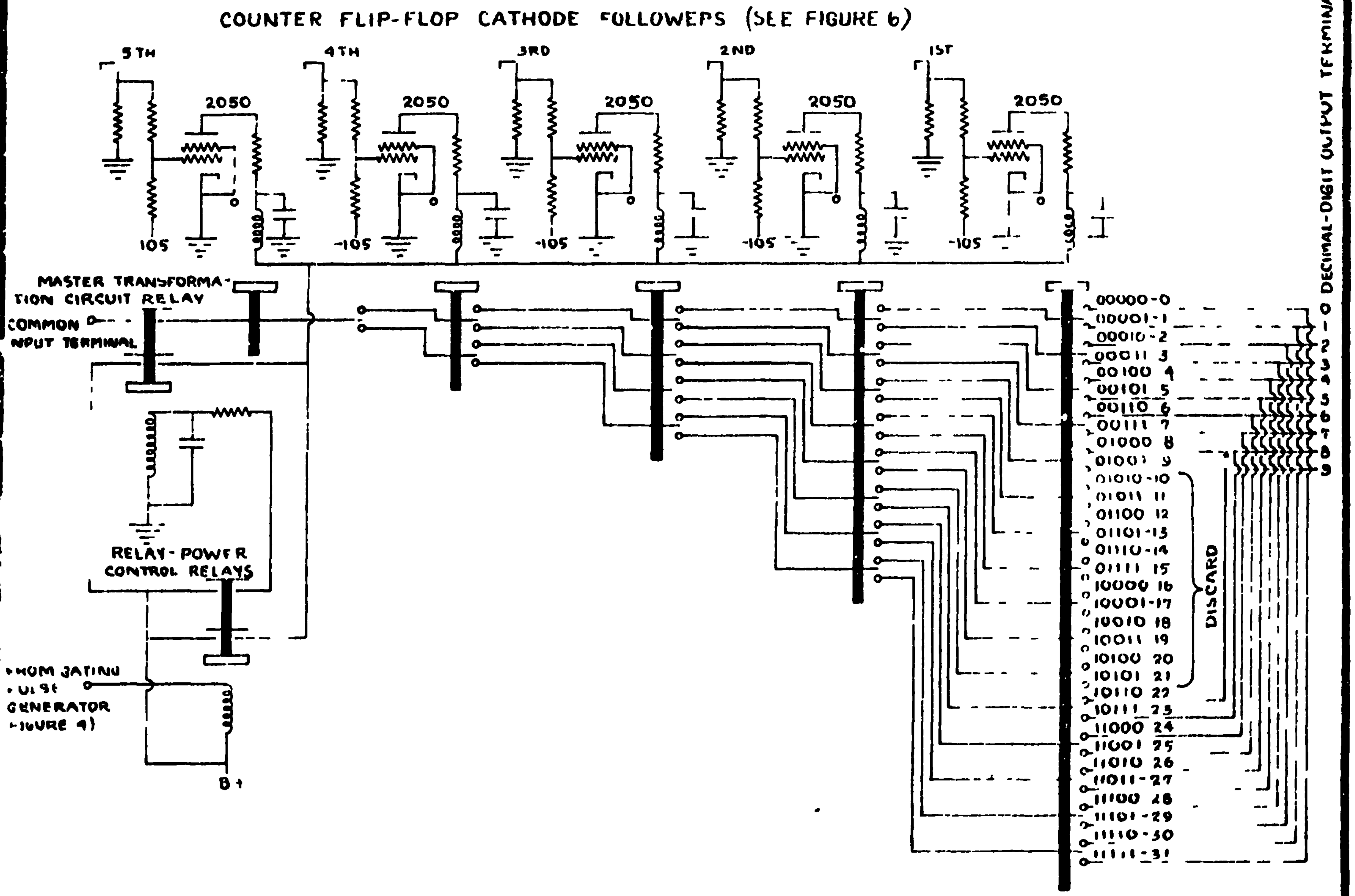

FIGURE 7-BINARY-TO-DECIMAL TRANSFORMATION CIRCUITS

Test and monitoring circuits. Unfortunately, it is impossible to devise any kind of monitoring circuit which will indicate whether or not the machine is choosing numbers without bias. There are, however, a few simple circuits which check the performance of the components of the system.

Referring to Figure 4, note the "Test Sequence Switch" in the grid circuit of the 6AC7 gated pulse amplifier. When this switch is closed, normal bias is applied to the grid of the 6AC7, and the circuit functions as a pulse amplifier. If the switch is open, however, a bias of -105 volts is applied to the 6AC7 grid, and the tube is completely cut off. Thus, no pulses from the random pulse generator can drive the counter. However, every time the gating pulse clamps this 6AC7 circuit, one pulse is formed by the pulse shaping circuits of Figure 5 (the leading edge of the gating pulse being sharp enough to trip the pulse shaping multivibrators). With this happening, the counter should advance just one count per selection. This test sequence is valuable as a check on the reliability of the system from the gate circuit through to the output device (which is an I.B.M. key punch at the present time). Before and after each running period the machine is set on "test sequence" for several minutes, and the punched cards produced are checked for errors.

A second circuit monitors the average rate at which pulses are being counted. This circuit is a simple electronic frequency meter connected to the last flip-flop in the counter chain. A voltage is generated proportional to the average frequency of the counts and is indicated by a meter on the front panel of the instrument (see Figure 8). Also, this voltage is used as an a-v-c source to regulate the average random pulse rate to the frequency desired (about 100,000 per second) by using it as a "Control Bias" on the noise source tube in Fig. 2.

Electro-mechanical counters were installed in the output circuits to indicate total counts. Ten counters were connected directly across the output terminals of the transformation relays to indicate the total number of times each decimal digit is selected. Also, two counters were installed to count the number of times the first flip-flop of the electronic binary counter indicated right and left (0 or 1) -- a measure of the impartiality of the system up to the binary selections. Recall that the binary-to-decimal digit transformation used, Table I, yields decimal digits of improved impartiality. Thus, it is advisable to look for partiality in the binary selections since partiality would be more evident there.

Conclusions.

1. A machine which takes as random the last digit of the total random pulses in a fixed period has been constructed and put into successful operation. Initially, an improbable excess of even over odd

UNCLASSIFIED

selections occurred. But, since revisions were made in the original circuits, no indication of partiality has occurred.

2. A complimentary type of transformation from binary to decimal digits is used. If partiality should exist in the binary numbers selected, this particular type of transformation would yield decimal digits with considerably less partiality.

3. The machine is completely automatic. The unit built was connected to an I.B.M. key punch to compile a table of several million random digits.

References

A Million Random Digits with 100,000 Normal Deviates, The RAND Corporation, 1955.

WORKING PAPER No. 20

A CLASS OF MAPPINGS AND SOME EXAMPLES

G. A. Hedlund
28 August 1958

This note concerns a class of mappings defined and studied by Rothaus (SCAMP Working Paper No. 25, August 30, 1957) and Blackwell (Ibid and SCAMP Working Paper No. 3, July 9, 1957). The first part of the paper develops some of the general theory. Most of the theorems proved are not new, though it appears that the proofs are. The second part of the paper gives some examples which seem to have been unknown previously.

Let S_n denote the set of all sequences of 0's and 1's of length n, n a positive integer. Any member of S_n will be called an n-block.

Let S denote the set of all unending sequences of 0's and 1's. Any member of S is a function with domain the set I of all integers (positive, negative or zero) and range in S_1. Let

$$s = \quad \ldots. \quad s_{-1}\, s_o\, s_1 \ldots$$

and

$$t = \quad \ldots. \quad t_{-1}\, t_o\, t_1 \ldots$$

be members of S. We define a distance in S as follows:

$$d(s,s) = 0 .$$

If $t \neq s$, there exists a least non-negative integer k such that $s_k \neq t_k$ or $s_{-k} \neq t_{-k}$, and we define

$$d(s,t) = \frac{1}{k+1} .$$

It is easily verified that S, with this metric, is a Cantor discontinuum.

Let f be a function with domain S_n and range in S_1, i.e., $f \cdot S_n \rightarrow S_1$. Then f defines a mapping g_m of S_{m+n-1} into S_m, as follows: Let $B \epsilon S_{m+n-1}$ and let

$$B = s_1 s_2 \ldots . s_{m+n-1} .$$

Define

$$t_i = f(s_i, s_{i+1}, \ldots, s_{i+n-1}) , \quad i = 1, 2, \ldots, m,$$

and let $C = t_1 t_2 \ldots t_m$. Then $g_m (B) = C$. Similarly, f defines a mapping g of S into S, as follows Let $s \epsilon S$ and let $s = \ldots s_{-1} s_o s_1 s_2 \ldots$.

Define

$$t_i = f (s_i, s_{i+1}, \ldots, s_{i+n-1}) , \quad i \epsilon I ,$$

and let

$$t = \ldots t_{-1} t_o t_1 \ldots .$$

We define $g (s) = t$. Clearly g is continuous.

A basic problem is to determine conditions on the function of f which will assure that the mapping g is an onto mapping, i. e., $g (S) = S$.

Remark. g is an onto mapping if, and only if, $g_m(S_{m+n-1}) = S_m$ for all m, or, equivalently, if, and only if, B being any m-block, there exists an (m+n-1)-block C such that $g_m(C) = B$.

The stated condition is obviously necessary.

To prove the sufficiency, suppose that, B being any m-block, there exists an (m+n-1)-block C such that $g_m(C) = B$. But then $g(S)$ is clearly dense in S. Since S is compact and g is continuous, $g(S)$ is compact, thus closed, and, being dense in S, $g(S) = S$.

Let $s = \ldots s_{-1} s_0 s_1 \ldots$ belong to S. Then s is said to be periodic if there exists a positive integer p such that

$$s_{i+p} = s_i , \; i \in I .$$

The least such positive integer is the period of s.

Remark. If $s \in S$ is periodic, then $g(s)$ is periodic. If s has period ω then the period of $g(s)$ divides ω.

In the following if A is a set, crd (A) denotes the number of members of A. If $B \in S_m$, $g_m^{-1}(B)$ denotes the collection of all members C of S_{m+n-1} such that $g_m(C) = B$. In general, if D is a subset of S_m, $g_m^{-1}(D)$ denotes the collection of all members E of S_{m+n-1} such that $g_m(C) \in D$.

<u>Lemma.</u> Let the mapping g defined by f be an onto mapping and let there exist a positive integer k such that $\mathrm{crd}\ g_m^{-1}(B) = k$ for some m-block B and $\mathrm{crd}\ g_p^{-1}(A) \geq k$ for all p-blocks A and all positive integers p. Then $\mathrm{crd}\ g_{p+m}^{-1}(BA) = k$ for all p-blocks A and all positive integers p.

<u>Proof.</u> It is sufficient to prove that

$$\mathrm{crd}\ g_{m+1}^{-1}(B0) = k = \mathrm{crd}\ g_{m+1}^{-1}(B1) .$$

Let

$$g_m^{-1}(B) = [C_1 , C_2 , \ldots , C_k] .$$

A member of $g_{m+1}^{-1}(B0)$ cannot be identical with a member of $g_{m+1}^{-1}(B1)$. Thus $\mathrm{crd}\ g_{m+1}^{-1}[B0 , B1] \geq 2k$.

But

$$g_{m+1}^{-1}[B0, B1] \subset [C_1 0, C_2 0, \ldots, C_k 0, C_1 1, C_2 1, \ldots, C_k 1]$$

and thus

$$g_{m+1}^{-1}[B0, B1] = [C_1 0, C_2 0, \ldots, C_k 0, C_1 1, C_2 1, \ldots, C_k 1]$$

and $\mathrm{crd}\ g_{m+1}^{-1}[B0, B1] = 2k$.

Since $\mathrm{crd}\ g_{m+1}^{-1}(B0) \geq k$, $\mathrm{crd}\ g_{m+1}^{-1}(B1) \geq k$, it follows that

$$\mathrm{crd}\ g_{m+1}^{-1}(B0) = k = \mathrm{crd}\ g_{m+1}^{-1}(B1).$$

The conclusion of the lemma now follows by induction.

Theorem Let the mapping g be an onto mapping. Then crd g_p^{-1} (A) $\leq 2^{n-1}$ for all p-blocks A and all positive integers p.

Proof. Let I^+ denote the set of positive integers and let

$$k = \min_{m \in I^+,\ B_m \in S_m} \operatorname{crd} g_{m.}^{-1}(B_m) \quad .$$

Since g is an onto mapping, $k \geq 1$. Let B be an m-block such that crd g_m^{-1} (B) = k. It follows from the preceding lemma that crd g_{p+m}^{-1} (BA) = k for all p-blocks A and all positive integers p.

Let

$$g_m^{-1}(B) = [C_1, C_2, \ldots, C_k] \quad .$$

Then

$$g_{m+q}^{-1}(BS_q) \subset [C_1S_q, \ldots, C_k S_q] , \quad q \in I^+ \quad .$$

We recall that S_q denotes the set of all q-blocks and BS_q denotes the set of all (m+q)-blocks with initial block B. Let the collection $[C_1S_q, \ldots, C_k S_q]$ be donoted by C_q^* .

The set C_q^* has $k \cdot 2^q$ members.

Now different members of BS_q cannot have the same inverses under g_{m+q}^{-1} and each member of BS_q has exactly k inverses under g_{m+q}^{-1} . Thus crd g_{m+q}^{-1} $(BS_q) = k \cdot 2^q$, g_{m+q}^{-1} $(BS_q) = C_q^*$ and the mapping g_{m+q} $(C_q^*) = BS_q$ is exactly k to 1 .

Let A be an arbitrary p-block and let crd $g_p^{-1}(A) = w$. Let $q = p+n-1$. Now S_q contains exactly w members, the image of each of which under g_p is A. Thus in C_q^* there are exactly kw members whose images under g_{m+q} are blocks ending in A. Now BS_q contains exactly 2^{n-1} blocks ending in A. Since the mapping $g_{m+q} \cdot C_q^* \to BS_q$ is exactly k to 1, the image set under g_{m+q} of kw members of C_q^* must contain at least w members. It follows that $2^{n-1} \geq w$ and the proof is completed.

<u>Theorem.</u> Let the mapping g be an onto mapping. Then crd $g_p^{-1}(A) = 2^{n-1}$ for all p-blocks A and all positive integers p.

<u>Proof.</u> Let A be a p-block and suppose

$$\text{crd } g_p^{-1}(A) \neq 2^{n-1} .$$

From the preceding theorem we infer that crd $g_p^{-1}(A) < 2^{n-1}$ and crd $g_q^{-1}(B) \leq 2^{n-1}$ for all q-blocks B and all positive integers q. Now $g_p(S_{p+n-1}) = S_p$, crd $S_{p+n-1} = 2^{p+n-1}$ and crd $S_p = 2^p$. Also crd $[S_{p+n-1} - g_p^{-1}(A)] > 2^{p+n-1} - 2^{n-1}(2^p-1)$, and

$$g_p[S_{p+n-1} - g_p^{-1}(A)] = S_p - A .$$

Not more than 2^{n-1} members of $S_{p+n-1} - g_p^{-1}(A)$ can map, under g_p, into the same element of $S_p - A$.

$$N(B, qi) \leq 2^{qi} - 2^{qi} \cdot 2^{-n+1} .$$

Thus

$$2^p - 1 = \text{crd}\,[S_p - A] \geq 2^{-n+1}\ \text{crd}\ [S_{p+n-1} - g_p^{-1}(A)] > 2^p - 1.$$

From this contradiction, we infer the truth of the theorem.

Remark. The preceding theorem shows that the property that g be an onto mapping is equivalent to the property that g be noisy in the sense that it transforms a random sequence (all blocks equidistributed) into a random sequence.

Theorem. Let g be an onto mapping and let $s \epsilon S$. Then $\text{crd}\ g^{-1}(s) \leq 2^{n-1}$.

Proof. Suppose that $\text{crd}\ g^{-1}(s) > 2^{n-1}$. Let $g^{-1}(s) = t_1, t_2, \dots, t_k$. Consider any pair t_i, t_j, $i \neq j$. There exists an integer p_{ij} such that the central $(2p_{ij} + 1)$-blocks of t_i and t_j are not identical. But then the central $(2p+1)$-blocks of t_i, t_j differ for all $p > p_{ij}$. Let p be an integer such that

$$p > \max\,[p_{ij} \mid 1 \leq i \leq j \leq k]$$

Then no two of the central $(2p+1)$-blocks of $t_1, t_2, \dots, t_k$ are alike. But the images under g_{2p-n+2} of these k blocks are identical. If $k > 2^{n-1}$, this contradicts a preceding theorem.

The proof of the theorem is completed.

Remark. It appears that the multiplicities of the mapping g at different points may be different. It would be of interest to investigate the various possibilities and characterize them.

<u>Theorem.</u> If g is an onto mapping and

$$s = \quad .. \; s_{-1} \, s_o \, s_1 \, s_2 \; \ldots$$

is a periodic sequence, then each member of $g^{-1}(s)$ is periodic. Let s have period ω , let $t \in g^{-1}(s)$ and let μ be the period of t . Then $\mu = p\omega$, and $1 \leq p \leq 2^{n-1}$.

<u>Proof.</u> Let g be an onto mapping, let

$$s = \quad \ldots \; s_{-1} \, s_o \, s_1 \, s_2 \ldots$$

be periodic with period ω and let $t \in g^{-1}(s)$. Let $p_s(k)$ be the number of different k-blocks in s . Then $p_s(k) \leq \omega$ for all k By a preceding theorem we infer that t contains at most $2^{n-1}\omega$ different $(k+n-1)$-blocks for each positive integer k. Thus, if $p_t(m)$ denotes the number of different m-blocks in t , we have $p_t(m) \leq 2^{n-1}\omega$ for all m .

Suppose t has no period less than $2^{n-1}\omega + 1$ From lemma 7.2 (Morse and Hedlund, American Journal of Mathematics, Vol. <u>60</u>, 1938, pp 815-866) $p_t(m) \geq m + 1$ for all values of m for which $p_t(m) < 2^{n-1}\omega + 1$. But this is true for all m and thus $p_t(m) \geq m + 1$ for all m Let $m = 2^{n-1}\omega$. Then $p_t(2^{n-1}\omega) \geq 2^{n-1}\omega + 1$, contradictory to $p_t(m) \leq 2^{n-1}\omega$ for all m . We infer that t has a period less than $2^{n-1}\omega + 1$ and t is periodic.

Let μ be the period of t . Then $\mu \leq 2^{n-1}\omega$ From a preceding theorem, there exists a positive integer p such that $\mu = p\,\omega$, and we have $\omega \leq p\omega \leq 2^{n-1}\omega$ and $1 \leq p \leq 2^{n-1}$.

Lemma Let m be a positive integer and let B be an m-block. For $q \geq m$, let $N(B,q)$ be the number of q-blocks which contain B . Then

$$\lim_{q \to \infty} \frac{N(B,q)}{2^q} = 1 .$$

Proof. We first observe that $N(B,q)/2^q$ is a montonic increasing function of q. For if C is a q-block which contains B, then $C0$ and $C1$ are different (q+1)-blocks each of which contains B . Thus

$$N(B,q+1) \geq 2\,N(B,q)$$

and consequently

$$\frac{N(B,q+1)}{2^{q+1}} \geq \frac{N(B,q)}{2^q} .$$

Thus we can assume that $q = pm$ and it is sufficient to prove that

$$\lim_{p \to \infty} \frac{N(B,pm)}{2^{pm}} = 1 ,$$

Let $B = B_1$, and let $B_1, B_2, \ldots, B_k$, $k = 2^m$, be the set of all m-blocks. Any block of length, pm can be written as a p-block of B_i's. There are k^p such blocks. Of these there are $(k-1)^p$ which do not contain $B \equiv B_1$, and thus $k^p - (k-1)^p$ which do contain B. Thus

$$N(B, pm) \geq k^p - (k-1)^p = 2^{mp} - (2^m - 1)^p$$

and

$$\frac{N(B, pm)}{2^{pm}} \geq 1 - (1 - \frac{1}{2^m})^p \quad .$$

But

$$\lim_{p \longrightarrow \infty} (1 - \frac{1}{2^m})^p = 0$$

and hence

$$\lim_{p \longrightarrow \infty} \frac{N(B, pm)}{2^{pm}} = 1 \quad .$$

The proof is completed.

Lemma. Let B be a block. For $q \geq n$, let D_q denote a partition of the set S_q of all q-blocks into sets of q-blocks each containing 2^{n-1} members. For q sufficiently large, all members of some element of the partition D_q must contain B as a sub-block.

Proof. We suppose the theorem false. That is, there exists a sequence of integers $q_1 < q_2 < \ldots$, D_{q_1}, D_{q_2} , ... , and partitions such that some member of each element of D_{q_1} fails to contain B as a sub-block. But then the number of members of D_{q_1} which do not contain B is at least equal to the number of elements of D_{q_1} , or $2^{q_1}/2^{n-1}$. Thus, using the notation of the preceding lemma, we have

But then

$$\limsup_{i \longrightarrow \infty} \quad \frac{N(B, qi)}{2^{qi}} \leq 1 - \frac{1}{2^{n-1}} \quad .$$

This contradicts the preceding lemma.

<u>Definition:</u> The sequence

$$s = \quad \ldots \; s_{-1} \, s_o \, s_1 \, s_2 \ldots$$

is said to be transitive provided every finite block appears in s .

<u>Theorem.</u> Let g be an onto mapping and let s be transitive. Then each member of $g^{-1}(s)$ is transitive.

<u>Proof.</u> Let B be an arbitrary k-block. The collection $g^{-1}(A) \mid A \epsilon S_m$ defines a partition D_{m+n-1} of all (m+n-1)-blocks into sets each containing 2^{n-1} blocks . From the preceding lemma we infer that for m sufficiently large there exists an m-block A such that each member of $g_m^{-1}(A)$ contains B . Now A appears in s and each member of $g^{-1}(s)$ must contain an element of $g_m^{-1}(A)$. It follows that each member of $g^{-1}(s)$ contains B and thus is transitive.

Let f_n be a function with domain S_n and range in S_1 , and let $g_m^{(n)}$, $g^{(n)}$ be corresponding mappings of S_{m+n-1} into S_m and S into S , respectively. Let f_p be a function with domain S_p and range in S_1 , and let $g_m^{(p)}$, $g^{(p)}$ be the corresponding mappings.

The mappings $g^{(n)}_{m+p-1}$ and $g^{(p)}_m$ can be composed in an obvious fashion to define mappings $g^{(p)}_m \cdot g^{(n)}_{m+p-1}$ of $S_{m+n+p-2}$ into S_m and thus a mapping $g^{(p)} \cdot g^{(n)}$ of S into S . Similarly there is defined a mapping $g^{(n)} \cdot g^{(p)}$ of S into S . It is not necessarily true that $g^{(p)} \cdot g^{(n)} = g^{(n)} \cdot g^{(p)}$.

Let $s \in S$

$$s = \quad \dots s_{-1} s_o s_1 \dots$$

and let

$$t = \quad \dots t_{-1} t_o t_1 \dots$$

be defined by

$$t_i = \quad s_{i+1} \ , \ i \in I \ .$$

The transformation $\phi : s \longrightarrow t$ is called the shift transformation. It is a homeomorphism of S onto S whose properties have been studied extensively (see Gottschalk and Hedlund, Topological Dynamics, Am. Math. Soc. Colloquium Publications, vol. 36, 1955, Ch. 12). A subset Y of S is invariant if $\phi(Y) = Y$.

It is easily shown that the transformation g of S into S, defined by f , commutes with ϕ, i.e., $g\phi = \phi g$.

Theorem. Let f define an onto mapping g of S onto S and and let X be a proper closed invariant subset of S . Then g (X) is a proper closed invariant subset of S.

Proof . Suppose g is an onto mapping and X is a proper closed invariant subset of S. Then X is compact, g (X) is compact and g (X) is closed. Since $g\phi = \phi g$, g (X) is invariant.

Suppose $g(X) = S$. Let s be a transitive point and let $x \epsilon X$ such that $g(x) = s$. According to a preceding theorem, x must be transitive and thus $X = S$, contrary to hypothesis. The theorem is proved.

Corollary. $g^{(p)}. g^{(n)}$ is an onto mapping if and only if both $g^{(p)}$ and $g^{(n)}$ are onto mappings.

Proof. Clearly, if $g^{(p)}$ and $g^{(n)}$ are both onto mappings, the $g^{(p)}. g^{(n)}$ is an onto mapping.

Suppose $g^{(p)} g^{(n)}(S) \subset g^{(p)}(S) \neq$ contrary to the supposition. Thus, in any case, $g^{(p)}$ is onto. Now if $g^{(n)}$ is not onto, then $g^{(n)}(S)$ is a proper closed invariant subset. Hence, by the last theorem $g^{(p)}$ $g^{(n)}(S)$ is a proper closed subset of S, again contradicting the assumption that $g^{(p)}. g^{(n)}$ is onto. Thus $g^{(n)}$ must also be onto and the second part of the corollary is proved.

The remainder of this paper is devoted to the determination of all functions f_n which determine onto mappings $g^{(n)}$ for $n \leq 4$.

The totality of functions f which define onto mappings in the cases $n = 2$ or 3 are easily compiled and are as follows. For $n = 2$ there are 6 such functions of which three are

$$f(x_1, x_2,) = x_1$$

$$'' = x_2$$

$$'' = x_1 + x_2$$

and the other three are the duals of these, that is, the functions obtained by adding 1 to each of the function values.

For $n = 3$ there are 30 such functions of which 15 are as follows:

	$f(x_1, x_2, x_3)$
1	x_1
2	x_2
3	x_3
4	$x_1 + x_2$
5	$x_1 + x_3$
6	$x_2 + x_3$
7	$x_1 + x_2 + x_3$
8	$x_1 + x_2x_3$
9	$x_3 + x_1x_2$
10	$x_1 + x_2 + x_2x_3$
11	$x_1 + x_3 + x_1x_2$
12	$x_1 + x_3 + x_2x_3$
13	$x_2 + x_3 + x_1x_2$
14	$x_1 + x_2 + x_3 + x_1x_2$
15	$x_1 + x_2 + x_3 + x_2x_3$

and the other 15 are the duals of these.

Remark. Of the fifteen listed, the first six are compositions of mappings for which $n = 2$.

For the case $n = 4$, it is considerably more difficult to determine which functions determine onto mappings. It is known that if f is linear in either x_1 or x_4, that is, f is defined by

$$f(x_1, x_2, x_3, x_4) = x_1 + f_1(x_2, x_3, x_4)$$

or

$$f(x_1, x_2, x_3, x_4) = x_4 + f_4(x_1, x_2, x_3) ,$$

then the corresponding mapping is onto. There are 496 such functions

It is also known that if f is defined by composing a pair of mappings of lower order (in this case a 3 and a 2) then f defines an onto mapping if and only if each of the composing mappings is onto. It is easily verified that there are 22 such composed functions which are not linear in x_1 or x_4 and which define onto mappings Of these 11 are given in the following table

	$f(x_1, x_2, x_3, x_4)$
1	x_2
2	x_3
3	$x_2 + x_3$
4	$x_2 + x_3x_4$
5	$x_3 + x_1x_2$
6	$x_1 + x_3 + x_1x_2$
7	$x_2 + x_3 + x_1x_2$
8	$x_2 + x_3 + x_3x_4$
9	$x_2 + x_4 + x_3x_4$
10	$x_1 + x_2 + x_3 + x_1x_2$
11	$x_2 + x_3 + x_4 + x_3x_4$

and the remaining 11 are the duals of these.

Now a necessary and sufficient condition that the mapping g defined by the function f be an onto mapping is that crd g_m^{-1} (B) = 2^{n-1} for each m-block B, and each positive integer m . But it is sufficient (theorem due to Blackwell, see Rothaus, loc. cit.) that crd g_m^{-1} (B) = 2^{n-1} for m = 2^{n-1} and each 2^{n-1}-block B.

This criterion is not as difficult to apply as first appears if use is made of the following device, illustrated for the case n = 4.

Let the set of all possible 3-blocks be denoted as follows:

(1)

000	0
001	1
010	2
011	3
100	4
101	5
110	6
111	7

Then the 4-blocks can be denoted

(2)

0000	00
0001	01
0010	12
0011	13
0100	24
0101	25
0110	36
0111	37
1000	40
1001	41
1010	52
1011	53
1100	64
1101	65
1110	76
1111	77

where

$x_i x_j$ $(i, j = 0, 1, 2, \ldots, 7, \quad j \equiv 2i \text{ or } 2i + 1, \bmod 8)$

denotes the 4-block of which the initial 3-block is x_i and the terminal 3-block is x_j .

Now for any specified function f (on the 4-blocks) we list under 0 , those blocks B for which f (B) = 0, and under 1, the complementary set. For example:

(3)

0	1
00	12
01	24
13	37
25	41
36	52
40	64
53	65
76	77

.

Any 5-block B can be written in the form abc , where a, b and c are integers from 0 to 7 , a is the integer corresponding by (1) to the initial 3-block of B , b is the integer corresponding by (1) to the middle 3-block of B and c is the integer corresponding by (1) to the terminal 3-block of B . Thus 01011 can be written as 253 .

Now if the 5-block B = abc is to map (under g_2) into 00 , then ab and bc must appear under 0 in (3) and this condition is clearly sufficient. It is thus possible to obtain the 5-blocks which map into 00 by taking any element ab under 0 in (3) for which the second term b appears as a first term and following ab by the second term of all elements for which b is the first term. As an illustration we determine the 5-blocks which map into 00 and 01 respectively

00	01
000	012
001	137
013	252
136	364
253	365
400	537
401	764
536	765

The process can be continued in an obvious fashion. The 7-blocks which map into 0000 are

0000
00000
00001
00013
00136
40000
40001
40013
40136 .

But it should be noted that in continuing this process, it is only the digits (representing 3-blocks) which appear at the ends which are of concern to us and the intermediate ones can be suppressed. We list, in terms of their terminal 3-blocks only, the blocks which map into 0, 00, 0000, 00000000 , respectively.

0	00	0000	00000000
00	00	00	00
01	01	01	01
13	03	03	03
25	16	06	06
36	23	40	40
40	40	41	41
53	41	43	43
76	56	46	46

When it was found (by hand computation) that there existed a function (n=4) which defined an onto mapping, which was not linear in any variable and which was not obtained by composition of onto mappings of lower order, it appeared that it might be worthwhile to determine all such functions.

This determination was carried through on SWAC. The non-restrictive assumption was made that $f(0,0,0,0) = 0$. Then of all such functions, those were rejected which did not produce an equal number of 0's and 1's (eight of each). The remainder were then successively subjected to tests as to whether crd $g_2^{-1}(B_2) = 8$ for each 2-blocks B_2, crd $g_4^{-1}(B_4) = 8$ for each 4-block B_4, crd $g_8^{-1}(B_8) = 8$ for each 8-block B_8 . There were 291 such successful matriculants. The following data concerning these was recorded on punch cards.

1) A tabulation of the function f .

2) The eight 4-blocks constituting $f^{-1}(0)$ in terms of their terminal 3-blocks.

3) The coefficients of the polynomial defining f .

The machine time in carrying through this program was 80 minutes.

Of the 291 functions defining onto maps, the 248 linear in the first or last variable were sorted out, leaving a residue of 43. Of these 11 were known to be obtainable by compositions of lower order onto mappings, leaving a residue of 32 . These 32 functions are tabulated in the following two tables:

Table I Functions on 4-blocks which determine onto mappings, which are not linear in either the first or last variables and which are not obtainable by compositions of lower order ($n \leq 3$) onto mappings

	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
0 0 0 0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0 0 0 1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0 0 1 0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	1	1	0	1	0	1
0 0 1 1	0	0	1	1	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	1	0	1	1	0
0 1 0 0	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1	0	0	1	1	1	0	1	0	1	1	1	1	1	1	1	1
0 1 0 1	1	1	1	1	0	1	0	0	1	1	0	0	0	1	1	1	0	1	0	1	1	0	0	1	0	0	1	1	0	0	0	0
0 1 1 0	1	1	0	1	0	0	1	1	0	1	0	0	1	0	0	1	1	0	0	0	0	1	1	1	1	1	0	0	0	0	1	1
0 1 1 1	1	1	0	0	1	1	1	1	1	0	0	1	0	0	0	0	1	1	1	0	0	1	0	0	1	0	1	0	1	0	0	1
1 0 0 0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
1 0 0 1	0	1	0	1	1	0	1	1	0	0	1	0	0	1	1	0	0	1	1	0	0	0	1	1	0	0	0	0	1	1	1	1
1 0 1 0	1	0	1	0	1	0	1	1	1	1	1	1	1	0	0	0	0	0	0	1	1	0	0	0	0	0	1	1	1	0	1	1
1 0 1 1	0	0	1	1	0	0	0	0	1	1	1	1	1	1	1	1	1	0	0	0	0	1	0	0	0	1	0	1	0	1	1	0
1 1 0 0	1	1	1	1	1	1	0	1	1	0	1	0	1	0	1	1	0	0	1	1	0	1	0	1	1	1	1	1	1	1	1	1
1 1 0 1	1	0	1	0	1	1	0	1	1	0	1	0	1	0	1	1	0	0	1	1	0	1	0	1	1	1	0	0	0	0	0	0
1 1 1 0	0	1	1	1	0	1	1	0	0	1	0	1	0	1	0	0	1	1	0	0	1	0	1	0	1	1	0	0	1	1	0	0
1 1 1 1	1	1	0	0	1	1	1	0	0	1	0	1	0	1	0	0	1	1	0	0	1	0	1	0	1	0	1	0	1	0	0	1

Table II. Non-zero coefficients of the polynomials defining the functions listed in Table I.

$$f(x_1, x_2, x_3, x_4) = \sum_{1\le i\le 4} a_i x_i + \sum_{1\le i<j\le 4} b_{ij} x_i x_j + \sum_{1\le i<j<k\le 4} c_{ijk} x_i x_j x_k$$

f	A_1	A_2	A_3	A_4	B_{12}	B_{13}	B_{14}	B_{23}	B_{24}	B_{34}	C_{123}	C_{124}	C_{134}	C_{234}
1		1				1							1	
2		1					1						1	
3		1				1		1		1			1	1
4		1					1			1			1	
5		1	1				1		1	1			1	1
6		1	1			1				1			1	
7			1				1					1		
8			1		1		1					1		
9			1		1			1	1		1	1		
10			1						1			1		
11		1	1				1		1				1	1
12		1	1		1				1			1		
13		1	1					1	1		1	1		
14		1	1		1	1	1				1	1		
15		1	1			1	1				1	1		
16		1	1			1		1					1	1
17	1		1		1		1					1		
18	1		1		1			1	1		1	1		
19	1	1	1		1				1			1		
20	1	1	1		1	1	1				1	1		
21	1	1	1			1	1				1	1		
22	1		1				1					1		
23	1	1	1					1	1		1	1		
24	1		1						1			1		
25		1		1			1			1			1	
26		1		1			1						1	
27		1	1	1			1		1				1	1
28		1	1	1			1		1	1			1	1
29		1		1		1		1		1			1	1
30		1	1	1		1				1			1	
31		1		1		1							1	
32		1	1	1		1		1					1	1

It was pointed out by R A Dean and R. C Lyndon that the set of 32 polynomials listed in Table II, can be generated from a set of eight by application of two simple processes One of these is the substitution $(x_1x_4)(x_2x_3)$, i e., interchange of x_1 and x_4 and interchange x_2 and x_3 The other is complementation, i e., substitution of $1+x_i$ for x_i , $i=1, 2, 3, 4$ The following is a generating set

7	$x_3 + x_1 x_4 + x_1 x_2 x_4$
10	$x_3 + x_2 x_4 + x_1 x_2 x_4$
24	$x_1 + x_3 + x_2 x_4 + x_1 x_2 x_4$
22.	$x_1 + x_3 + x_1 x_4 + x_1 x_2 x_4$
9	$x_3 + x_1 x_2 + x_2 x_3 + x_2 x_4 + x_1 x_2 x_3 + x_1 x_2 x_4$
13.	$x_2 + x_3 + x_2 x_3 + x_2 x_4 + x_1 x_2 x_3 + x_1 x_2 x_4$
14	$x_2 + x_3 + x_1x_2 + x_1 x_3 + x_1 x_4 + x_1 x_2 x_3 + x_1x_2x_4$
23	$x_1 + x_2 + x_3 + x_2 x_3 + x_2 x_4 + x_1 x_2 x_3 + x_1 x_2 x_4$

46 of 50
edman

UNCLASSIFIED

WORKING PAPER No. 22

A NUMERICAL SIMULATION TO STUDY THE READINGS OF A FIXED ANTENNA ADCOCK RADIO DIRECTION FINDER UNDER CONDITIONS OF FADING

Joseph F. Mount
C. Tompkins
25 Feb 1958
10 pages

22

In this paper we shall describe a numerical simulation from which we try to draw some conclusions concerning the behavior of a perfectly balanced fixed antenna Adcock direction finder [1, 2, 3] under conditions of fading. It is assumed that fading is caused by random cancellation of signals arriving on different transmission paths. Normally these paths might differ either in the number of reflections from the ionosphere or in the layer from which they are reflected, or both. Minor variations in directions of the transmission path from any jump pattern may occur at the receiving site because of variations in ionospheric tilt, variations in penetration, local reflections, and other causes.

will be centered about two sets of direction cosines, which may be specified independently of each other and of other simulations at the start of each calculation; an approximate intensity is specified precisely for each transmission, independently of all other inputs. We allow for the following random variations in transmissions, each variation to occur slowly enough to justify treatment through use of variables which are piecewise constant:

(a) The relative phase between the two arrivals varies randomly and uniformly between 0 and 2π ;

(b) The intensity of each arrival will vary from the approximate value set by a factor $1 + h$, where h is a sample from an approximately normal distribution with mean zero and standard deviation which is set as part of the input of the problem;

(c) The six direction cosines of the arriving signals will be modified to direction numbers by the addition of independent samples from normal distributions each with mean zero and with standard deviations which are set as part of the input to the calculation.

UNCLASSIFIED

These eight standard deviations are set independently of each other and independently of other parts of the calculations.

At least for the time being the calculation will consist of the determination of two functions and the recording of relations between them. For each choice of the random variates the signal strength received at one of the collectors will be computed and for each choice the reading of a fixed antenna Adcock direction finder will be estimated. The signal strength will be calculated straightforwardly. The reading of the radio direction finder will be estimated either by computing the points of maximum deflection of a Watson Watt [2] type display under the stimulus of the two signals, or by computing angles of minimum deflection for a rotating goniometer [1] type display. In each case, it will be assumed that the equipment receiving the signals is in perfect adjustment, so that none of the calibrating complexities of [1] and [2] will be introduced except to the extent that the angle of arrival influences the octantal error.

It is proposed that relations between these two functions be exhibited by means of tallies in one hundred positions, giving a kind of scatter diagram. Thus, if the functions are denoted by f and F , we propose that the range of possible values of each be divided into ten parts, arbitrarily as part of the input routine, and that the number of examples found in which the functions fall into each possible pair of cells be recorded and presented as output.

2. The functions to be computed -- the two-channel case.

For the two-channel case, we examine equations (8) of [1] (these equations will be repeated below), and try to compute the response of a two-channel direction finder under the influence of a pair of signals of the type indicated above.

Explicitly, we assume that signals with frequency $\omega/2\pi$ are being received over two paths. The quantities pertinent to the two signals will be distinguished by subscripts, the subscript 1 for the first signal and the subscript 2 for the second. The first signal will arrive with direction cosines α_1 , β_1 and γ_1 , the second will have direction cosines α_2 , β_2 , and γ_2 . The signals will have amplitudes (weighted by the effectiveness of the collectors) A_1 and A_2 respectively. The first signal will be taken to set the standard in phase, so that the responses of the two antenna pairs to it will be given by direct analogues of equations (8) in [1] ,

$$(1)\quad \left\{\begin{aligned} E_{NS1} &= 2A_1 \sin \frac{\omega\beta_1 d}{2c} \sin \omega t ,\\ E_{EW1} &= 2A_1 \sin \frac{\omega\alpha_1 d}{2c} \sin \omega t , \end{aligned}\right.$$

where, as before, d is the distance between collectors of the pair and c is the velocity of radio wave propogation. For the second arrival the phase is displaced a constant amount ξ_2 sampled from a uniform distribution over the range $[0, 2\pi]$. (Here ξ_2 plays a role somewhat different from the role of ξ in [2].) The responses to the second signal are respectively

$$(2)\quad \left\{\begin{aligned} E_{NS2} &= 2A_2 \sin \frac{\omega\beta_2 d}{2c} \sin (\omega t - \xi_2) ,\\ E_{EW2} &= 2A_2 \sin \frac{\omega\alpha_2 d}{2c} \sin (\omega t - \xi_2) . \end{aligned}\right.$$

The analysis here follows that of [2].

The total NS signal is the algebraic sum of the two signals received:

$$E_{NS} = 2[A_1 \sin \frac{\omega\beta_1 d}{2c} \sin \omega t + A_2 \sin \frac{\omega\beta_2 d}{2c} \sin (\omega t - \xi_2)] ,$$

or

$$(3) \quad E_{NS} = 2[(A_1 \sin \frac{\omega\beta_1 d}{2c} + A_2 \cos \xi_2 \sin \frac{\omega\beta_2 d}{2c}) \sin \omega t$$

$$- A_2 \sin \xi_2 \sin \frac{\omega\beta_2 d}{2c} \cos \omega t] .$$

Similarly,

$$(4) \quad E_{EW} = 2[(A_1 \sin \frac{\omega\alpha_1 d}{2c} + A_2 \cos \xi_2 \sin \frac{\omega\beta_2 d}{2c}) \sin \omega t$$

$$- A_2 \sin \xi_2 \sin \frac{\omega\beta_2 d}{2c} \cos \omega t] .$$

The development of the functions to be tallied follows the general development in [2] .

A heterodyning signal $E_L \cos (\omega + \omega_o)t$ is mixed with E_{NS} and E_{EW} , the difference frequency is extracted, and the signals amplified to be presented respectively as horizontal and vertical deflections. Using (3) and (4) and the relations

$$(5) \quad \begin{aligned} \cos (\omega + \omega_o)t \sin \omega t &= \tfrac{1}{2}[\sin (2\omega + \omega_o)t - \sin \omega_o t] , \\ \cos (\omega + \omega_o)t \cos \omega t &= \tfrac{1}{2}[\cos (2\omega + \omega_o)t + \cos \omega_o t] \end{aligned}$$

the retained signals are proportional to

$$(6)\quad \begin{cases} E_V = -(A_1 \sin\frac{\omega\ \beta_1 d}{2c} + A_2 \cos\ \xi_2\ \sin\frac{\omega\beta_2 d}{2c}) \sin\omega_o t \\ \qquad - A_2 \sin\xi_2\ \sin\frac{\omega\beta_2 d}{2c}\ \cos\omega_o t\quad , \\ E_H = -(A_1 \sin\frac{\omega\alpha_1 d}{2c} + A_2 \cos\ \xi_2\ \sin\frac{\omega\alpha_2 a}{2c}) \sin\omega_o t \\ \qquad - A_2 \sin\ \xi_2\ \sin\frac{\omega\beta_2 d}{2c}\ \cos\omega_o t\quad . \end{cases}$$

The deflection may now be calculated as a function of t. formally,

$$r^2 = E_V{}^2 + E_H^2 \quad .$$

The maximum deflection (and the minimum) occurs when $dr/dt = 0$, hence when

$$(7)\qquad E_V\ \mathring{E}_V + E_H\ \mathring{E}_H = 0\quad ,$$

where the dot denotes differentiation with respect to time.

Since we propose a computational, and not an analytic, attack on the problem, we propose to simplify the notation at this point. To that end write the computable functions

$$(8)\quad \begin{cases} V_S = -\ (A_1 \sin\frac{\omega\beta_1 d}{2c} + A_2 \cos\ \xi_2\ \ \sin\frac{\omega\beta_2 d}{2c})\ , \\ V_C = -\ A_2 \sin\xi_2\ \sin\frac{\omega\beta_2 d}{2c}\quad , \\ H_S = -\ (A_1 \sin\frac{\omega\alpha_1 d}{2c} + A_2 \cos\ \xi_2\ \ \sin\frac{\omega\alpha_2 d}{2c})\quad , \\ H_C = -\ A_2 \sin\ \xi_2\ \sin\frac{\omega\alpha_2 d}{2c}\quad , \end{cases}$$

so that

$$(9)\quad \left\{\begin{aligned} E_V &= V_S \sin \omega_o t + V_C \cos \omega_o t \\ E_H &= H_S \sin \omega_o t + H_C \cos \omega_o t \ . \end{aligned}\right.$$

Then the condition (7) for maximum or minimum deflection gives

$$(10)\qquad \tan 2\omega_o t_o = \frac{2(V_C V_S + H_C H_S)}{V_C^2 - V_S^2 + H_C^2 - H_S^2} \ .$$

In a complete cycle of 2π radians, this equation (10) is satisfied by four angles $\omega_o t_o$ separated by $\pi/2$ radians.

Values for E_V and E_H at these points may be found by writing

$$\tan \omega_o t_o = \frac{-1 \pm \sqrt{\tan^2 2\omega_o t_o + 1}}{\tan 2\omega_o t_o} ,$$

using a similar formula to find tan $\omega_o t_o/2$ (choosing the ambiguous sign carefully each time) and writing

$$(11)\quad \left\{\begin{aligned} \sin \omega_o t_o &= \frac{2 \tan \omega_o t_o/2}{1 + \tan^2 \omega_o t_o/2} , \\ \cos \omega_o t_o &= \frac{1 - \tan^2 \omega_o t_o/2}{1 + \tan^2 \omega_o t_o/2} \ . \end{aligned}\right.$$

Independently of the choice of sign, the four displacements may be computed easily. If the computed values of (11) are written

$$S_o = \sin \omega_o t_o \quad \text{and} \quad C_o = \cos \omega_o t_o \quad ,$$

then at the four extreme deflections the components are

$$(12) \quad \left\{ \begin{aligned} E_V{}^1 &= S_o V_S + C_o V_C \quad \text{and} \quad E_H{}^1 = S_o H_S + C_o H_C \quad , \\ E_V{}^2 &= C_o V_S - S_o V_C \quad \text{and} \quad E_H{}^2 = C_o H_S - S_o H_C \quad , \\ E_V{}^3 &= -S_o V_S - C_o V_C \quad \text{and} \quad E_H{}^3 = -S_o H_S - C_o H_C \quad , \\ E_V{}^4 &= -C_o V_S + S_o V_C \quad \text{and} \quad E_H{}^4 = -C_o H_S + S_o H_C \quad . \end{aligned} \right.$$

$E_V{}^3$ and $E_V{}^4$ above are obtainable from $E_V{}^1$ and $E_V{}^2$ by multiplying by -1 , and a similar remark applies to the horizontal components, only the first and second of these deflections will be considered. Write

$$(E^\alpha)^2 = (E_V{}^\alpha)^2 + (E_H{}^\alpha)^2 \quad , \quad \alpha = 1, 2 \ ,$$

the first or the second of the deflections will be retained depending on whether $(E^1)^2$ or $(E^2)^2$ is larger. We choose the first function to be tallied as

$$F_1 = \max_\alpha \left[(E_V{}^\alpha)^2 + (E_H{}^\alpha)^2 \right] \quad .$$

F_1 is a measure of the received signal strength.

Finally note that for the deflection retained the displacement is at an angle ϕ_o where

(13) $$\tan \phi = \frac{E_H^{\alpha}}{E_V^{\alpha}}$$

for the chosen displacement index α. This is the tangent of the angle read on the direction finding equipment

For some α, β write $\tan \phi_o = \beta/\alpha$. Choose α, β to be horizontal direction cosines accepted as correct--say the mean from which α_1 and β_1 deviate. Then the tangent of the "error" in reading (including octantal error) is

(14) $$F_2 = \tan(\phi - \phi_o) = \frac{\tan \phi - \tan \phi_o}{1 + \tan \phi \tan \phi_o} .$$

This function F_2 is the second function to be tallied.

BIBLIOGRAPHY

1. C. Tompkins. Elementary Calibration of Direction Finding Equipment from Target Transmitter Tests, and Graphical Plotting of Bearings under Idealized Conditions. Memorandum with some considerable circulation, 10 August 1957.

2. C. Tompkins. Calibration of 2-Channel Adcock Direction Finders. Memorandum with some considerable circulation, 22 August 1957.

3. R. Keen. Wireless Direction Finding, 4th Edition, Iliffe, London, 1947, especially p.283-285.

University of California, Los Angeles